

SERVIZI ALLE IMPRESE (quattro seggi)**CONFCOMMERCIO - CONFESERCENTI -
CNA - CONFARTIGIANATO****Paladini Ennio**

C.F. PLDNNE57A06E563U nato a Leverano (LE) il 06.01.1957 ed ivi residente alla Via Consolazione, 84, CAP 73045. Esperto.

Mazzotta Roberta

C.F. MZZRRT74C66F970J nata a Novoli (LE) il 26.03.1974 e residente in Lecce - Villa Convento - Via Pio XII n. 6, CAP 73100. Imprenditore.

Petrelli Roberto

C.F. PTRRRT60A03E506Z nato a Lecce il 03.01.1960 e residente in San Donato di Lecce alla Via Case Sparse Contrada Macchitelle CAP 73010. Esperto.

CONFINDUSTRIA LE**Benisi Vincenzo**

C.F. BNSVCN53P21H811I nato a San Damiano d'Asti (AT) il 21.09.1953 e residente in Racale (LE) alla Via Ospina snc, CAP 73055. Imprenditore.

PESCA (un seggio)**Sansò Luigi**

C.F. SNSLGU44E06E506W nato a Lecce il 06.05.1944 ed ivi residente alla Via Ventimiglia 33 CAP 73100. Esperto

**ORGANIZZAZIONI SINDACALI
LAVORATORI (un seggio)****CGIL-CISL-UIL****Giannetto Salvatore**

C.F. GNNSVT48A22C297X nato a Castiglione di Sicilia (CT) il 22.01.1948 e residente in Lecce alla Via Mario di Lecce n. 14, CAP 73110. Segretario Provinciale UIL

**TUTELA CONSUMATORI
E UTENTI (un seggio)****ADICONSUM - ADOC
FEDERCONSUMATORI****Moscagiuri Antonio**

C.F. MSCNTN47H23E815E nato a Maglie il 23.06.1947 ed ivi residente in Via Unità d'Italia n. 129, CAP 73024. Funzionario CGIL

Il competente Ufficio del Servizio Attività economiche consumatori provvederà alla notifica del presente atto ai nominati ed alla convocazione della prima seduta del Consiglio Camerale.

Il presente decreto sarà inserito nella raccolta ufficiale dei decreti del Presidente della Regione Puglia e sarà pubblicato sul Bollettino Ufficiale.

Bari, lì 31 dicembre 2009

VENDOLA

DETERMINAZIONE DEL DIRETTORE DELL'AREA POLITICHE PER LO SVILUPPO, IL LAVORO E L'INNOVAZIONE 23 dicembre 2009, n. 31

PO FESR 2007-2013 - Asse I - Delibera n. 749 del 07/05/2009 "Programma Pluriennale di Attuazione (PPA)" - Linea 1.3, Azione 1.3.6, Linea 1.5, Azione 1.5.2 - Presa d'atto e adozione del documento CRIPAL "Linee Guida Tecniche standard e specifiche tecniche Azione 1.5.2 PO FESR 2007-2013, Versione del 23/10/2009".

Il giorno 23 dicembre 2009, in Bari, nella sede

- Visti gli artt. 4,5 e 6 della L.R. 4/02/1997 n.7;
- Vista la DGR n. 3261 del 28/07/1998;
- Visti gli artt. 4 e 16 del D.lgs 165 del 30/03/2001;
- Vista la DGR n. 20 del 21/01/2008 e la successiva DGR n. 180 del 20/02/2008;

- Visto il Decreto del Presidente della Giunta Regionale n. 161 del 22/02/2008;
- Vista la DGR n. 1444 del 30/07/2008;
- Visto il PO FESR 2007-2013 della Regione Puglia, come approvato dalla Commissione Europea con C(2007) 5726 del 20/11/2007;
- Vista la DGR n. 146 del 12/2/2008 con la quale la Giunta Regionale ha preso atto di detta decisione comunitaria;
- Visto il Decreto del Presidente della Giunta Regionale n. 886 del 24/9/2008 con cui è stato emanato l'Atto di Organizzazione per l'Attuazione del PO FESR 2007-2013;
- Vista la DGR n. 1849 del 30/9/2008 con la quale sono stati nominati l'Autorità di Gestione del PO FESR 2007-2013, nonché i Responsabili degli Assi di cui al medesimo programma;
- Vista la DGR n. 165 del 17/02/09 con la quale la Giunta Regionale ha approvato le "Direttive concernenti le procedure di gestione del PO FESR 2007-2013";
- Vista la DGR n. 185 del 17/02/09 con la quale la Giunta Regionale ha nominato i Responsabili delle Linee di Intervento del PO FESR 2007-2013 e ha autorizzato gli stessi ad operare sui capitoli di bilancio che finanziano il Programma, ciascuno per la Linea di propria responsabilità;
- Vista la DGR n. 748 del 07/05/09, "PO 2007-2013. Strategia regionale per la Società dell'Informazione";
- Vista la DGR n. 749 del 07/05/09 con la quale la Giunta Regionale ha approvato il Programma Pluriennale di Attuazione dell'Asse I del PO FESR 2007-2013;
- Vista l'azione 1.3.6, "Sviluppo ed evoluzione del Centro Tecnico Regionale e dei servizi centrali dell'Amministrazione Regionale", Linea di intervento 1.3, "Interventi per il potenziamento di infrastrutture digitali", Programma Pluriennale di Attuazione dell'Asse I del PO FESR 2007-2013, come approvato dalla DGR n. 749 del 07/05/09;
- Vista l'azione 1.5.2, "Sviluppo dei servizi di e-government nella Pubblica Amministrazione Regionale e Locale", Linea di intervento 1.5, "Interventi per lo sviluppo dei servizi pubblici digitali", Programma Pluriennale di Attuazione dell'Asse I del PO FESR 2007-2013, come approvato dalla DGR n. 749 del 07/05/09;
- Vista la determinazione del Direttore dell'Area Politiche per lo Sviluppo, il Lavoro e l'Innovazione n.5 dell'11/06/2009, con la quale viene formalmente istituito il Centro Regionale per l'Innovazione della PA Locale (CRIPAL);
- Vista la determinazione del Direttore dell'Area Politiche per lo Sviluppo, il Lavoro e l'Innovazione n.6 del 30/06/2009, con la quale si prende atto e si adotta il documento CRIPAL "Servizi pubblici della PAL prioritariamente informatizzabili";
- Vista la determinazione del Direttore dell'Area Politiche per lo Sviluppo, il Lavoro e l'Innovazione n.7 del 01/07/2009, con la quale si adottano le linee di indirizzo per la individuazione e la gestione degli interventi ammissibili a finanziamento nell'attuazione della Linea di Intervento 1.5;
- Vista la DGR n. 2001 del 27/11/2007, "Deliberazione di Giunta regionale n. 1610 del 23/10/2006 - PO 2007-2013, Asse I, Linea di intervento 1.5 Interventi per lo sviluppo dei servizi digitali per la Pubblica Amministrazione ed i cittadini. Azione: Interventi di supporto alla diffusione dell'utilizzo dei servizi della RUPAR da parte degli enti pubblici rimuovendo gli ostacoli che ne impediscono la fruizione". Prosecuzione attività avviate con il Por 2000-2006";
- Vista la DGR n. 1880 del 07/10/2008; "PO 2007-2013, Asse I - RUPAR - Azioni per garantire la continuità tra i Programmi Operativi 2000-2006 e 2007-2013";
- Vista la Determinazione del dirigente Servizio e-

government, e-democracy e cittadinanza attiva n. 34 del 05/08/2009, sulla continuità d'uso e modalità rendicontative della RUPAR;

- Vista la Determinazione del dirigente Settore Programmazione, n. 199 del 30/06/2006, "Approvazione elenco delle proposte ammesse a finanziamento ai sensi della Delibera di Giunta Regionale n. 262 del 07/03/2005 e successiva n. 685 del 09.05.2005";
- Vista la DGR n. 72 dell'8 febbraio 2007, Delibera CIPE n. 35/2005, "Ripartizione risorse Fondo Aree Sottoutilizzate (FAS) Aree Urbane";
- Vista la DGR n. 1072 del 4/07/2007 "Approvazione delle Linee Guida per la pianificazione strategica territoriale di Area Vasta";
- Vista DGR n. 917 del 26/05/2009, "Pianificazione strategica di Area Vasta. Adempimenti per la definizione del Programma Stralcio di Interventi di Area Vasta";
- Vista la Legge regionale n. 4 del 08/03/2007, "Nuova disciplina in materia di Nucleo di valutazione e verifica degli investimenti pubblici della Regione Puglia (NVVIP)";

CONSIDERATO CHE:

- L'azione 1.3.6 prevede che il Centro Regionale per l'Innovazione della PA Locale (CRIPAL): definisca attraverso la concertazione con il sistema delle autonomie locali i servizi di e-government nella pubblica amministrazione locale; definisca e rilasci gli standard territoriali e le linee guida relativi ai servizi di e-gov con particolare riferimento alle soluzioni Open Source e al riuso di soluzioni esistenti; gestisca l'Albo delle soluzioni; certifichi i servizi di e-government degli Enti Locali; supporti l'Ente regionale per l'innovazione tecnico-organizzativa del sistema delle PAL;
- L'azione 1.5.2, avente l'obiettivo di costituire una rete regionale di servizi finalizzata allo sviluppo del sistema di e-government e della Società dell'Informazione nell'Amministrazione regionale e nelle Amministrazioni locali, prevede che il CRIPAL fornisca indicazioni, rilasci standard e

certifichi l'aderenza a questi ultimi al fine di realizzare e far evolvere un insieme di servizi e un insieme di modalità avanzate per la fruizione degli stessi;

- In sede di riunione del CRIPAL del 26/06/2009 è stato approvato il documento "Servizi pubblici della PAL prioritariamente informatizzabili" adottato con determinazione del Direttore dell'Area Politiche per lo Sviluppo, il Lavoro e l'Innovazione n.6 del 30/06/2009;
- Lo stesso documento riporta nel capitolo 6 "Definizione degli standard: il ruolo del CRIPAL" che il CRIPAL procederà "...alla stesura e al rilascio presso gli Enti locali dei documenti (Linee Guida Tecniche) relativi agli standard nazionali e regionali da seguire nello sviluppo e erogazione dei servizi individuati";
- In sede di riunione del CRIPAL del 27/10/2009 è stato approvato il documento "Linee Guida Tecniche standard e specifiche tecniche Azione 1.5.2 PO FESR 2007-2013, Versione del 23/10/2009";

RITENUTO CHE:

- Al fine di adempiere a quanto stabilito in sede di riunione CRIPAL del 27/10/2009, sia necessario prendere atto del documento "Linee Guida Tecniche standard e specifiche tecniche Azione 1.5.2 PO FESR 2007-2013, Versione del 23/10/2009" e procedere alla sua adozione per le attività conseguenti;

ADEMPIMENTI CONTABILI AI SENSI DELLA L.R. N. 28/01 e s.m.i.

Si dichiara che il presente provvedimento non comporta alcun mutamento qualitativo e quantitativo di entrata o di spesa né a carico del bilancio regionale né a carico degli enti per cui debiti i creditori potrebbero rivalersi sulla Regione e che è escluso ogni ulteriore onere aggiuntivo rispetto a quelli già autorizzati a valere sullo stanziamento previsto dal bilancio regionale.

Ritenuto di dover provvedere in merito, in qualità di Responsabile dell'Asse I,

DETERMINA

per le motivazioni innanzi espresse, che qui si intendono integralmente riportate ed in attuazione del PPA approvato con DGR n. 749/2009, di:

- prendere atto dell'allegato documento "Linee Guida Tecniche standard e specifiche tecniche Azione 1.5.2 PO FESR 2007-2013, Versione del 23/10/2009", così come approvato in sede di riunione del CRIPAL del 27/10/2009;
- adottare l'allegato documento "Linee Guida Tecniche standard e specifiche tecniche Azione 1.5.2 PO FESR 2007-2013, Versione del 23/10/2009", così come approvato in sede di riunione del CRIPAL del 27/10/2009;
- notificare il presente Atto all'Autorità di Gestione

FESR 2007-2013, e al Nucleo di Valutazione e Verifica degli Investimenti Pubblici della Regione Puglia per gli adempimenti conseguenti ai sensi della DGR 917/2009;

- notificare il presente Atto ai responsabili delle Linee 1.3 e 1.5 dell'Asse I - PO FESR 2007-2013 ai fini della attuazione delle rispettive Linee di intervento;
- pubblicare il presente atto sul Bollettino Ufficiale della Regione Puglia.

il presente provvedimento, redatto in un unico esemplare è immediatamente esecutivo.

Davide F. Pellegrino

C.R.I.P.A.L.

Versione del 23 ottobre 2009

**Linee Guida Tecniche
standard e specifiche tecniche
Azione 1.5.2 PO FESR 2007-2013**

INDICE

1	Introduzione	634
2	Normativa, Standard e Specifiche tecniche	636
2.1	Servizi con Priorità 1	636
2.1.1	Protocollo Informatico	636
2.1.2	Posta Elettronica Certificata (PEC).....	636
2.1.3	Gestione informatizzata degli atti amministrativi.....	637
2.1.4	Firma Digitale	637
2.1.5	Componente intrinseca: Cooperazione Applicativa.....	638
2.2	Servizi con Priorità 2.....	638
2.2.1	Sistema Informativo Territoriale (SIT).....	638
2.2.2	Identificazione in rete del cittadino.....	647
2.2.3	Sportello Unico per l'Edilizia (SUE).....	648
2.3	Servizi con Priorità 3.....	650
2.3.1	Circolarità Anagrafica.....	650
2.4	Servizi con Priorità 4.....	650
2.4.1	Piani Urbanistici Generali (PUG)	650
3	Componenti rese disponibili dal Centro Tecnico Regionale	652
3.1	Protocollo Informatico	652
3.2	Gestione informatizzata degli atti amministrativi	652
3.3	PEC.....	652
3.4	Cooperazione Applicativa	653
3.5	Circolarità anagrafica	653
3.6	Identificazione in rete del cittadino.....	653
3.7	Sistema Informativo Territoriale (SIT Regionale).....	653

ALLEGATI

Allegato 1: Ontologia dell'Indice della Pubblica Amministrazione (IPA) e Servizi Documentali

Allegato 2: Accordi di Servizio per l'Indice della Pubblica Amministrazione (IPA) e Servizi Documentali

Allegato 3: Servizi del SIT Regionale

Allegato 4: Istruzioni Tecniche per la informatizzazione dei Piani Urbanistici Generali (PUG) nell'ambito del SIT Regionale

Allegato 5: Identificazione in rete del cittadino

1 Introduzione

Le presenti Linee Guida intendono fornire gli standard e le specifiche tecniche per la realizzazione dei progetti per la Società dell'Informazione nell'ambito dell'Azione 1.5.2 del PO FESR 2007-2013 in conformità al Programma Pluriennale di Attuazione (PPA 2007-2010) approvato con Delibera di Giunta n. 749 del 7/5/2009.

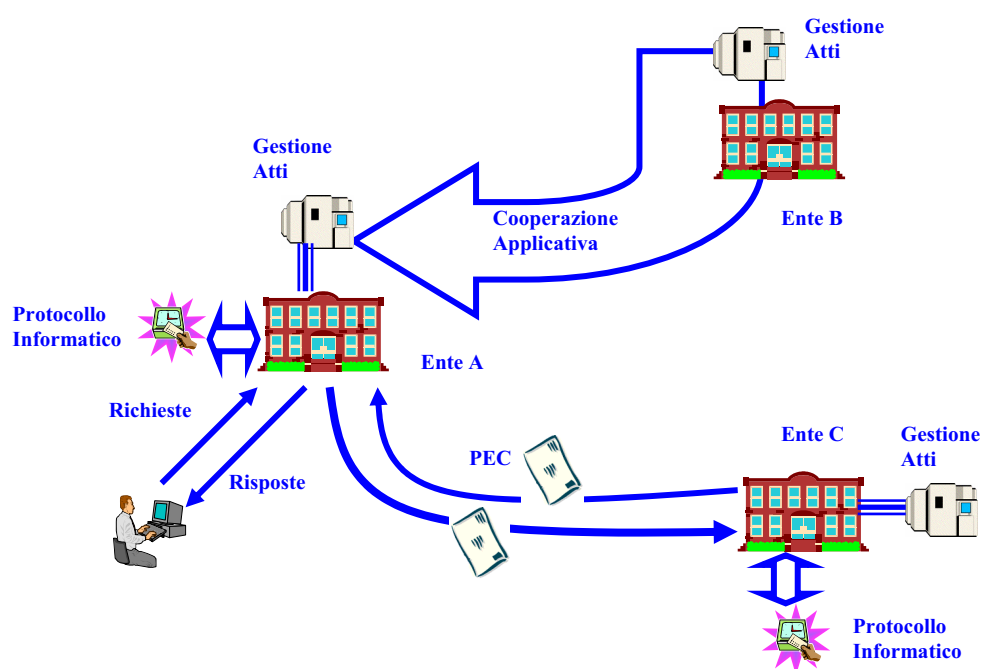
Questa versione è relativa ai servizi classificati nei primi quattro livelli di priorità nel documento del CRIPAL "Servizi pubblici della PAL prioritariamente informatizzabili", con riguardo ai servizi per l'efficienza interna, ai servizi interni per il governo del territorio (SIT), a cui si associano i servizi strettamente connessi PUG e SUE, ed ai servizi interni abilitanti, con la focalizzazione sui servizi di collaborazione tra le pubbliche amministrazioni.. Si rinvia ad una prossima edizione del presente documento l'emanazione degli standard e specifiche tecniche dei servizi per l'interazione con cittadini e imprese

Lo scopo dei progetti dell'Azione 1.5.2 è di attuare l' e-government nella regione Puglia in modo omogeneo e standardizzato, nonché il più possibile esteso, per innovare profondamente il modo di operare della Pubblica Amministrazione Locale ed il suo rapporto con i cittadini e le imprese utenti dei suoi servizi.

Gli obiettivi funzionali che si intende raggiungere sono i seguenti:

- dematerializzazione del procedimento amministrativo, con la minimizzazione dell'uso della carta, e gestione interamente informatica e telematica del procedimento stesso al fine di velocizzarlo
- interazione telematica tra diversi Enti Pubblici al fine di reperire e/o trasferire informazioni attinenti al procedimento, evitando di chiedere al cittadino/impresa di fornire informazioni già in possesso di altre Amministrazioni
- possibilità per il cittadino/impresa di iniziare e concludere il procedimento in modalità telematica, senza doversi necessariamente recare presso lo sportello dell'Ente pubblico
- accesso telematico del cittadino/impresa alle informazioni del proprio procedimento (trasparenza) per poterne conoscere lo stato di avanzamento

La seguente figura illustra in modo sintetico le componenti principali dei sistemi che, se attivati in un contesto di riorganizzazione dei processi lavorativi dell'Amministrazione, consentono di raggiungere gli obiettivi precedentemente indicati.



I principali servizi interni abilitanti, comuni a tutte le Amministrazioni, di cui è richiesta l'adozione sono i seguenti.

- Protocollo informatico
- Posta Elettronica Certificata (PEC)
- Firma Digitale
- Gestione informatizzata degli Atti Amministrativi
- Sistema Informativo Territoriale
- Identificazione in rete del cittadino
- Circolarità anagrafica
- Endoprocedimenti SUE

Una componente intrinseca necessaria a molti di questi servizi è la Cooperazione Applicativa.

2 Normativa, Standard e Specifiche tecniche

2.1 Servizi con Priorità 1

Le presenti specifiche tecniche sono nel seguito dettagliate per ognuno dei moduli funzionali ma, per la comprensione delle scelte che sottendono alla specifica, si deve tener presente che i servizi abilitanti descritti devono essere necessariamente interfacciati tra di loro. Per questo motivo il Protocollo Informatico richiesto non è un nucleo minimo di protocollo ma un protocollo interfacciato al Gestore Documentale ed alla PEC. Inoltre lo stesso Protocollo Informatico ed il Gestore Documentale devono essere dotati di Servizi di Cooperazione Applicativa per l'accesso allo stato delle pratiche amministrative. Infine la firma digitale è una componente fondamentale di tutti i processi.

Analogamente le specifiche che riguardano i dati e servizi territoriali sono strettamente correlate e quindi vanno tenute presente in modo unitario per poter produrre i risultati attesi di conformità, oltre che di efficacia.

2.1.1 Protocollo Informatico

L'Ente deve aver definito almeno una AOO ed aver completato l'iter dell'accreditamento ed iscrizione della struttura organizzativa all'IPA (Indice nazionale della Pubbliche Amministrazioni).

Il sistema di Protocollo deve essere conforme alla vigente normativa e in particolare a:

- circolare 7 maggio 2001, n. AIPA/CR/28
- circolare 21 giugno 2001, n. AIPA/CR/31
- DPCM 31 ottobre 2000
- DPR 28 dicembre 2000, n. 445, capo IV
- Decreto Legislativo 7 marzo 2005, n.82 (Codice dell'amministrazione digitale)

La conformità richiesta rispetto alla Circolare AIPA CR/28 è relativa a tutte le funzionalità, nessuna esclusa. Si evidenzia l'importanza del supporto della interoperabilità di protocollo con la corretta gestione della segnatura al fine di consentire l'automazione delle operazioni di protocollazione di ingresso/uscita tra diverse AOO.

La specifica tecnica concernente l'integrazione nei confronti della Cooperazione Applicativa è riportata nello specifico paragrafo.

2.1.2 Posta Elettronica Certificata (PEC)

La Posta Elettronica Certificata ed il suo utilizzo da parte delle Pubbliche Amministrazioni è regolamentata dalle seguenti disposizioni legislative:

- DLGS n. 82 del 7 marzo 2005 (Codice dell'Amministrazione Digitale) e s.m.i., in particolare gli artt. 1, 6 e 48.

- DPR 11 febbraio 2005, n.68, Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata
- Decreto Legge n. 185 del 29 novembre 2008 convertito, con modificazioni, nella Legge n. 2 del 28 gennaio 2009 che, all'art. 16bis prevede che ogni amministrazione pubblica utilizzi unicamente la posta elettronica certificata con effetto equivalente, ove necessario, alla notificazione per mezzo della posta, per le comunicazioni e le notificazioni aventi come destinatari dipendenti della stessa o di altra amministrazione pubblica.
- Decreto del Presidente del Consiglio dei Ministri del 6 maggio 2009, pubblicato sulla Gazzetta Ufficiale del 25 maggio 2009 n. 119, che definisce sia le modalità di rilascio di caselle PEC ai cittadini sia, all'art. 4, le modalità di attivazione della PEC per le Pubbliche Amministrazioni

E' richiesto che ad ogni AOO definita nell'IPA sia associata almeno una casella di PEC attivata presso uno dei gestori iscritti nell'Albo tenuto dal CNIPA.

2.1.3 Gestione informatizzata degli atti amministrativi

Il sistema di Gestione degli atti amministrativi deve essere conforme alla vigente normativa e in particolare a:

- Codice dell'Amministrazione digitale (d.lgs. 7 marzo 2005, n. 82)
- Decreto Legislativo 4 aprile 2006, n.159 "Disposizioni integrative e correttive al decreto legislativo 7 marzo 2005, n. 82"
- Deliberazione Cnipa 19 febbraio 2004, n. 11 recante le regole tecniche per la riproduzione e conservazione di documenti su supporto ottico idoneo a garantire la conformità dei documenti agli originali;
- Codice dei beni culturali e del paesaggio (D. lgs. 22 gennaio 2004, n. 42)

La specifica tecnica concernente l'integrazione nei confronti della Cooperazione Applicativa è riportata nello specifico paragrafo.

2.1.4 Firma Digitale

E' richiesto che almeno il responsabile della AOO sia dotato di firma digitale rilasciata da una della Autorità di Certificazione iscritte nell'Albo del CNIPA.

La normativa che concerne la firma digitale è la seguente:

- Decreto legislativo 7 marzo 2005, n. 82 (Codice dell'Amministrazione Digitale)
- DPCM del 13 gennaio 2004
- Deliberazione CNIPA n.4 del 17 febbraio 2005
- Deliberazione CNIPA n.34 del 18 maggio 2006 con relativo allegato
- Circolare CNIPA n.48 del 6 settembre 2005

2.1.5 Componente intrinseca: Cooperazione Applicativa

L'Ente deve installare la Porta di Dominio presso il proprio accesso RUPAR-SPC ed accreditare e qualificare la propria porta presso il CNIPA.

La Cooperazione Applicativa è uno standard tecnico (SPCoop) previsto dall'art. 76 comma 1 del Decreto legislativo 7 marzo 2005, n. 82 (Codice dell'Amministrazione Digitale) e definito in dettaglio negli artt. 19 e 20 del Decreto del Presidente del Consiglio dei Ministri 1 aprile 2008 "Regole tecniche e di sicurezza per il funzionamento del Sistema pubblico di connettività previste dall'articolo 71, comma 1-bis del decreto legislativo 7 marzo 2005, n. 82, recante il «Codice dell'amministrazione digitale»." G.U. 21 giugno 2008, n. 144.

E' richiesto che i sistemi di protocollo informatico e di gestione documentale, nel rispetto dell'art. 76 comma 1. del Codice dell'Amministrazione digitale, esponano i seguenti servizi di cooperazione:

- interrogazione del contenuto di un fascicolo (a partire da una protocollazione)
- estrazione di un documento di un fascicolo
- ricerca generalizzata sulle protocollazioni di propria pertinenza.

Questi servizi sono resi disponibili da un'Amministrazione alle altre Amministrazioni con cui essa ha rapporti e sono funzionali a permettere ad ogni Amministrazione di tracciare la gestione delle pratiche di proprio interesse presso le altre Amministrazioni a cui le ha inoltrate.

In futuro, una volta avviati i servizi di FrontEnd di cui ai punti successivi dell'Azione 1.5.2, la disponibilità di questi servizi di cooperazione consentirà alle Amministrazioni, per tramite del proprio portale, di rendere disponibile ai cittadini l'accesso per via telematica alle informazioni sullo stato delle loro pratiche: trasparenza dell'azione amministrativa, art. 41 comma 2 del Codice dell'Amministrazione digitale.

La specifica tecnica dettagliata è riportata in Allegato 1 (Ontologia) e Allegato 2 (Accordi di servizio).

2.2 Servizi con Priorità 2

2.2.1 Sistema Informativo Territoriale (SIT)

Obiettivo

La costruzione di una infrastruttura di dati e servizi territoriali a livello regionale (IDT-Puglia) nella logica della Direttiva Europea INSPIRE passa attraverso l'adozione a tutti i livelli amministrativi di regole e standard tecnici per l'interoperabilità e l'armonizzazione sia dei dati che dei servizi stessi. La Regione intende sostenere e adottare tali principi per tutti i dati territoriali di pubblico interesse a qualunque livello istituzionale siano essi costruiti, a partire dai dati di base quali cartografie tecniche e cartografie tematiche sino agli strumenti della Pianificazione territoriale e urbanistica.

L'armonizzazione dei dati presuppone l'adozione di regole che si applicano nella fase di costruzione del dato, l'interoperabilità presuppone l'adozione di regole che si applicano nella fase di

pubblicazione (condivisione). Le prime riguardano il contenuto e sono pertanto strettamente correlate alla specificità del dato, le seconde attengono al formato di pubblicazione e ai servizi minimi che ne consentono l'accesso e sono pertanto valide per qualsiasi tipologia di dato territoriale.

Di seguito si riportano sinteticamente:

- 1) le specifiche tecniche di riferimento per la pubblicazione del dato distinte su tre aspetti:
 - il **formato di pubblicazione**, regole e standard essenziali ai fini dell'interoperabilità tra sistemi informativi;
 - i **metadati**, ne permettono la identificazione e la ricerca;
 - i **servizi per l'accesso al dato**, ne consentono la disponibilità effettiva;
- 2) le specifiche di riferimento per la costruzione dei dati, distinte in funzione del settore applicativo di riferimento.

1- Specifiche tecniche per la pubblicazione di dati territoriali

Formato di pubblicazione

Per quanto riguarda la pubblicazione di archivi territoriali in maniera aperta e standard, quindi senza vincoli proprietari di formati di rappresentazione, rivestono notevole importanza gli standard tecnologici dell'Open Gis Consortium (OGC), un'organizzazione internazionale senza fini di lucro impegnata nella definizione di specifiche tecniche per i servizi geospaziali e di localizzazione.

Attività preponderante dell'OGC è lo sviluppo e l'implementazione di standard per il contenuto, i servizi e l'interscambio di dati geografici in ottica di apertura ed estensibilità; tutte le specifiche OGC sono disponibili sul sito www.opengis.org.

Gli standard OGC più utilizzati per la pubblicazione via Internet di dati geografici sono i seguenti:

- Web Map Service (WMS)
- Web Feature Service (WFS)

Il WMS prevede che una mappa intesa come insieme di strati informativi geografici opportunamente tematizzati sia resa in un formato di immagine digitale; i formati raster previsti sono PNG, GIF o JPEG, pur essendo contemplato anche il formato vettoriale SVG (Scalar Vector Graphic). Lo standard definisce alcune operazioni di base:

- restituzione di metadati sul servizio WMS pubblicato;
- restituzione di una mappa in dipendenza dei valori dei parametri forniti in input (extent geografico, sequenza degli strati da visualizzare in quanto accesi, etc.);
- restituzione dei contenuti alfanumerici associati agli oggetti visualizzati (opzionale).

Le operazioni su un servizio WMS vengono richieste da client che supportano il protocollo http mediante delle URL appositamente composte; nel caso due o più mappe siano prodotte con gli stessi parametri geografici (extent territoriali rispetto al medesimo sistema di coordinate), gli output delle richieste possono essere sovrapposti; la creazione di mappe composite è agevolata dall'uso di formati grafici che supportano la trasparenza.

Si possono richiedere mappe distinte a differenti server; le applicazioni client che inviano richieste ad un servizio WMS possono anche non essere web-based; tutte le richieste e le risposte seguono una sintassi xml-based.

La maggior parte degli ambienti G.I.S. open source e commerciali implementa tale standard per la visualizzazione ed interrogazione di banche dati territoriali. Le specifiche OGC WMS sono sfociate nello standard ISO19128.

Nel WFS, invece, le mappe non sono rese come immagini, bensì i singoli strati consistono in flussi di dati vettoriali codificati in un linguaggio standard xml-based che è il GML (Geography Markup Language); tale protocollo è indicato per la visualizzazione delle mappe in maniera dinamica, ma soprattutto per l'interrogazione dei dati alfanumerici associati alle entità vettoriali, per la manipolazione e la conversione dei dati (editing, esportazione in differenti formati, download dei dati pubblicati). Tutte le operazioni sono esposte dal servizio come specifiche "capabilities".

Come per il WMS, il protocollo per l'interazione tra client e server è l'http, con il supporto di SOAP per lo scambio di messaggi. I client di tale categoria di servizi sono perlopiù non web-based. Il WFS ha contribuito allo sviluppo dello standard ISO19142.

Metadati

Lo standard **ISO19115 - Metadati** fa parte degli standard prodotti da [ISO/TC211](#) e definisce gli schemi necessari per descrivere i dati geografici attraverso informazioni relative all'identificazione, l'estensione, la qualità, gli schemi temporali e spaziali, i riferimenti spaziali e la distribuzione di dati geografici numerici. Lo standard definisce le sezioni di metadati obbligatorie e condizionali, entità di metadati ed elementi di metadati; l'insieme minimo di elementi (*core metadata*) richiesti dalla gamma completa di applicazioni di metadati (scoperta dei dati, determinazione della pertinenza per l'uso, accesso ai dati, trasferimento dei dati e uso dei dati numerici); gli elementi opzionali di metadati per consentire una più estesa descrizione standard dei dati geografici.

Parallelamente, lo standard **ISO19119 - Servizi** fa parte degli standard prodotti da [ISO/TC211](#) e definisce le direttive per l'implementazione di cataloghi di metadati relativi a servizi su dati geografici.

A livello OGC, il più diffuso standard per la pubblicazione dei metadati strutturati in forma di catalogo è il CSW (Web Catalog Service).

Il protocollo CSW permette di realizzare web service di ricerca e consultazione di cataloghi di metadati, oltre a consentire ricerche di metadati su cataloghi distribuiti aderenti alla medesima specifica. INSPIRE sostiene la specifica OGC CSW ISO19115/19119 Application Profile, per una maggiore aderenza allo standard ISO19115.

Attualmente, il recepimento della direttiva europea nella realtà nazionale italiana si concretizza, indirettamente, nel Repertorio Nazionale dei Dati Territoriali (RNDT), implementazione puntuale dello standard ISO19115 concernente i metadati da definire sulle banche dati rese pubbliche.

Tale standard individua gli schemi necessari per descrivere i dati territoriali e i servizi relativi, comprendendo informazioni circa l'identificazione, l'estensione, le accuratezze spaziali e temporali, i sistemi di coordinate adottati e i vari soggetti coinvolti nel processo di costruzione e di distribuzione dei dati stessi.

Lo standard, orientato alla catalogazione e descrizione completa, si applica a dati geografici organizzati in gerarchie di serie, dataset e sezioni; definisce nello specifico;

- sezioni di metadati obbligatorie e condizionali, entità di metadati ed elementi di metadati;
- un insieme minimo di informazioni necessarie per una spiegazione essenziale dei dati;
- alcuni elementi opzionali di metadati per permettere una descrizione standard più dettagliata;
- un metodo per estendere i metadati nella prospettiva di soddisfare esigenze più mirate.

Il materiale relativo al RNDT è consultabile sul sito del CNIPA a partire dall'indirizzo seguente:

http://www.cnipa.gov.it/site/it-IT/Attivit%C3%A0/Sistemi_Informativi_Territoriali/Specifiche_tecniche/Regolamento_Repertorio/

Il formato per la rappresentazione e memorizzazione dei metadati strutturati è basato su XML. Operativamente, il RNDT si traduce in un'applicazione realizzata presso il CNIPA dotata delle seguenti funzionalità:

- possibilità di costruzione dei file xml di descrizione delle singole banche dati (o servizi) attraverso un editor user-friendly che guida nella compilazione dei campi obbligatori, facoltativi o condizionali;
- possibilità di validazione di file xml creati attraverso strumenti esterni all'editor;
- registrazione dei file xml per la repertazione definitiva delle banche dati (o servizi) presso il CNIPA;
- ricerca delle informazioni relative alle banche dati (o servizi) preventivamente repertati mediante criteri alfanumerici o geografici.

Nella logica di attuare la politica di condivisione caldeggiata anche da INSPIRE, attraverso accordi e convenzioni con il CNIPA, ogni Ente produttore di dati territoriali può essere abilitato all'accesso al repertorio nazionale con delle utenze ad hoc.

L'indirizzo web per utilizzare il repertorio è il seguente:

http://www.rndt.cnipa.it/RNDT/home/index.php?%3A%3A_Il_Repertorio_Nazionale.

Servizi per l'accesso al dato

La documentazione e la pubblicazione delle banche dati territoriali costituite dalle Pubbliche Amministrazioni sono regolate da alcune direttive valide sia per enti nazionali sia per organismi a carattere regionale o locale.

Quella più nota e rilevante al tempo stesso per l'ampia portata che la caratterizza è la direttiva INSPIRE 2007/2/EC del 14 marzo 2007 del Parlamento Europeo e del Consiglio, generata nell'ambito di un progetto europeo con lo scopo di realizzare una infrastruttura di dati territoriali nella Comunità Europea risultante dall'integrazione delle infrastrutture dei singoli strati membri; ognuna di queste è vista come il prodotto del coordinamento delle infrastrutture a livello sub-nazionale. L'ottica complessiva è quella di evitare inutili duplicazioni di dati, gestendo la condivisione dei contenuti in maniera efficiente, consistente e non ridondante.

Il testo della direttiva è reperibile in forma integrale al seguente indirizzo web:

[http://eur-lex.europa.eu/LexUriServ/site/it/oj/2007/l_108/l_10820070425it00010014.pdf.](http://eur-lex.europa.eu/LexUriServ/site/it/oj/2007/l_108/l_10820070425it00010014.pdf)

Nel rispetto della salvaguardia della privacy e dei diritti di proprietà intellettuale, la direttiva fissa un insieme di servizi di base che ogni amministrazione deve esporre per rendere accessibili le proprie banche dati geografiche tramite Internet; in maniera schematica, tali servizi vengono di seguito elencati:

- *servizi di ricerca*, fondamentali per ricercare i dati territoriali e i servizi relativi mediante un catalogo dei metadati opportunamente strutturato che ne documenta le caratteristiche qualitative;
- *servizi di consultazione*, utili per la navigazione all'interno delle banche dati organizzate in mappe di strati tematici sovrapposti; è stabilito un set minimo di funzionalità di navigazione che prevede variazione della scala di visualizzazione, zoom in, zoom out, pan, sovrapposizione di tutti i dati resi pubblici, visualizzazione delle legende e collegamento con i metadati associati;
- *servizi di download dei dati*, per il download dei contenuti, compatibilmente con le politiche di riservatezza definiti localmente all'Amministrazione responsabile;
- *servizi di conversione*, tra diversi formati per il supporto all'interoperabilità;
- *servizi che consentano di richiamare altri servizi specifici sui dati territoriali*, di carattere particolare non inclusi nelle categorie precedenti ma comunque descritti nel catalogo dei metadati.

2- Specifiche tecniche per la costruzione dei dati

Realizzazione di reti geodetiche e cartografie di base

La realizzazione dei dati territoriali di base (reti geodetiche, carta tecnica, database topografico, ortofoto, DTM, uso del suolo) deve essere effettuata in conformità alle specifiche tecniche che sono state utilizzate per i prodotti realizzati e resi disponibili dall'Assessorato all'Assetto del Territorio nell'ambito del progetto SIT e che rappresentano il risultato del processo di adozione, a livello regionale, delle specifiche nazionali messe a punto nell'ambito dell'Intesa Stato-Regioni. Essi devono rappresentare un aggiornamento o un approfondimento a scala di maggior dettaglio dei livelli informativi costruiti con il SIT Regionale, funzionale alla realizzazione dei servizi applicativi di settore individuati di interesse prioritario.

Gli standard di riferimento per la costruzione degli strati informativi territoriali prioritari sono il risultato dell'attività di gruppi di lavoro nazionali nati nell'ambito dell'Intesa tra Stato, Regioni ed Enti Locali sui Sistemi Informativi Geografici, approvata dalla Conferenza Stato regioni e Province Autonome e coinvolge le diverse Amministrazioni Centrali ed organismi statali, compreso il CNIPA (Centro Nazionale per l'Informatica nella Pubblica Amministrazione), le Regioni e Province Autonome, i Comuni (ANCI), le Province (UPI), le Comunità Montane (UNCHEM) e le Aziende per la gestione di pubblici servizi (Confservizi). Le specifiche sono note come IntesaGIS e riguardano le seguenti tipologie di banche dati:

- database topografici di interesse generale fino alla scala 1:10000;
- database topografici scala 1:25000;
- modelli digitali del terreno;
- raffittimento della rete fondamentale IGM95

Per quanto riguarda invece la carta dell'uso del suolo, le specifiche di riferimento sono note come CORINE e sono state definite e adottate a livello europeo, con il contributo di vari Stati.

Database topografici di interesse generale

Tali specifiche prevedono un insieme di categorie (classi) nelle quali gli oggetti territoriali sono classificati; per ciascuna classe è dettagliata:

- le tipologie geometriche caratterizzanti (se areali, lineari o puntuali o entrambi);
- il grado di obbligatorietà rispetto alla scala di acquisizione (i database topografici sono considerati “multiprecisione” per cui oggetti acquisiti a scale di dettaglio differenti possono anche coesistere in una stessa classe del database);
- un insieme di attributi in cui i nomi e i tipi dei campi sono fissati, eventualmente con dei domini codificati opportunamente.

L'insieme delle classi costituisce il Catalogo degli Oggetti generale.

Le specifiche sono consultabili all'indirizzo:

http://www.cnipa.gov.it/site/it-IT/Attivit%C3%A0/Sistemi_Informativi_Territoriali/Precedente_comitato_dati_territoriali/

Accanto a tali documenti di carattere descrittivo, i gruppi di lavoro hanno prodotto anche delle linee guida operative di supporto all'implementazione dei database topografici (“Linee guida per l'implementazione” In1014 versione 19/11/2007) reperibile all'indirizzo:

http://www.centrointerregionale-gis.it/public/DB_Topografici/In1014_v_1_4.pdf.

L'attività del progetto del Sistema Informativo Territoriale (SIT) della Regione Puglia ha portato alla localizzazione di tali specifiche, eseguita con la definizione delle corrispondenze tra i contenuti della Carta Tecnica Regionale (CTR), regolati da capitolati tecnici adottati a livello regionale, e quelli delle specifiche nazionali IntesaGIS; l'adattamento ha riguardato contenuti geometrici e alfanumerici, per cui di fatto il Catalogo degli Oggetti è stato revisionato gestendo opportunamente situazioni di collassamento geometrico rispetto alle soglie di acquisizioni della CTR.

Il lavoro è stato supportato dal CNIPA ed ha portato alla definizione di uno standard regionale per la produzione dei database topografici. Le modifiche concordate con il CNIPA sono state poi trasferite da quest'ultimo al tavolo nazionale.

La localizzazione ha coinvolto anche le linee guida per l'implementazione; in tal senso, è stato distribuito un documento valido per le regioni aderenti al PR5SIT, tra cui la Puglia, divenuto standard operativo per la produzione dei database topografici multi precisione (“Linee guida per la realizzazione dei database topografici nelle Regioni del PR5SIT – versione Febbraio 2008”).

Database topografici scala 1:25000

Il documento di riferimento per questo prodotto è “Specifiche di contenuto – La derivazione del DB25 dal Catalogo degli Oggetti – In1007_6”, versione 2006.

Vengono descritti alcuni criteri di massima per la generalizzazione degli oggetti territoriali presenti nei database topografici a scale di dettaglio, oltre alle codifiche da applicare a tutte le feature da includere dal punto di vista dei contenuti geometrici e alfanumerici.

Il documento è reperibile all'indirizzo web:

http://www.cnipa.gov.it/site/files/In1007_6_vers2006_33.pdf

L'applicazione operativa delle indicazioni proposte nel documento nell'ambito del SIT è supportata dall'Istituto Geografico Militare Italiano.

Modelli digitali del terreno

Il documento di riferimento è "Prescrizioni tecniche per la produzione di Modelli Digitali del Terreno versione 16I del 29 aprile 2001", disponibile al seguente indirizzo web:

http://www.centrointerregionale-gis.it/public/DTM/DTM16I_Spec_Apr01_it.pdf.

Il documento esamina possibili formati di rappresentazione, accuratezze planimetriche e altimetriche, metodologie di acquisizione rispetto a strumenti tecnologici. Nell'ambito del SIT, la Regione Puglia ha prodotto un modello digitale del terreno sull'intero territorio regionale migliorando la precisione del livello 3 dello standard IntesaGIS impostando il valore del passo della griglia di acquisizione ad 8 metri.

Reti di Raffittimento della rete fondamentale IGM95

Il documento di riferimento per il raffittimento della rete IGM è "Specifiche Tecniche – Raffittimento della Rete Fondamentale IGM95 – 16 luglio 2001", reperibile al seguente indirizzo web:

<http://www.centrointerregionale-gis.it/script/documenti.asp>.

Il documento affronta le tematiche che vanno dalle modalità operative di materializzazione dei vertici ai contenuti delle documentazioni monografiche, alle procedure di rilievo e alle metodologie di collaudo.

Carta tematica dell'uso del suolo

Lo standard di riferimento è il risultato del programma CORINE (Coordination of Information on the Environment), varato dal Consiglio della Comunità Europea nel 1985 per verificare lo stato dell'ambiente nella Comunità, orientare le politiche comuni, controllarne gli effetti e proporre eventuali miglioramenti.

Tale standard coincide con le regole utilizzate in uno dei progetti del CORINE, il Land Cover, teso a svolgere un'indagine sull'occupazione del suolo, specificamente finalizzato al rilevamento e al monitoraggio delle caratteristiche del territorio, con particolare attenzione alle esigenze di tutela. Il progetto CORINE Land Cover ha portato alla realizzazione di una base informativa riguardante la copertura del suolo alla scala 1:100.000; la legenda è articolata in 44 voci suddivise in 3 unità gerarchiche e si riferisce a unità spaziali omogenee o composte da zone elementari appartenenti ad una stessa classe, chiaramente distinguibili dalle unità circostanti. La superficie minima cartografabile è di 25 ettari, che corrisponde sulla carta ad un quadrato di 500 mt. di lato.

A loro volta le Regioni hanno arricchito nel tempo lo standard Corine introducendo ulteriori livelli gerarchici in funzione della scala di rappresentazione, tanto che il CISIS (Centro Interregionale per i Sistemi Informatici, Geografici e Statistici) ha attivato un gruppo di lavoro sulla tematica con l'obiettivo di definire una proposta di specifiche tecniche di dettaglio condivisa tra le Regioni, che sia riferimento immediato per i progetti in fase di attivazione e base di confronto per i futuri approfondimenti eventualmente sviluppati in sede di Comitato per i Dati Territoriali.

Componente correlata: Dati catastali

Riferimenti normativi

L'utilizzo dei dati catastali nell'ambito dei sistemi informativi degli Enti territoriali è regolato da specifica normativa dell'Agenzia del Territorio di cui si riportano i riferimenti principali:

- D. Lgs. n. 112 del 31/3/1998 in attuazione del capo I della L. 15 marzo 1997, n. 59, regola il conferimento di funzioni e compiti amministrativi dello Stato alle regioni ed agli enti locali, affidando la titolarità delle funzioni catastali ai Comuni che sono comunque lasciati liberi di decidere se svolgere queste funzioni direttamente, in forma associata con altri Comuni oppure delegandole all'Agenzia del Territorio.
- Il Codice dell'Amministrazione Digitale stabilisce che la base dei dati catastali gestita dall'Agenzia del Territorio è di interesse nazionale (Art. 59, comma 7-bis). Tale norma ha portato all'emanazione del decreto del 13 novembre 2007, predisposto da parte del direttore dell'Agenzia del Territorio e approvato preventivamente dal Comitato per le regole tecniche sui dati territoriali delle pubbliche amministrazioni e previa intesa con la Conferenza unificata, al fine di garantire la circolazione e la fruizione dei dati catastali per via telematica tra i sistemi informatici delle altre amministrazioni. Detto provvedimento è stato pubblicato sulla Gazzetta Ufficiale n. 274 del 24 novembre 2007 (supplemento ordinario n. 243) ed è composto da:
 - [Decreto 13 novembre 2007](#)
Definizione delle regole tecnico economiche per l'utilizzo dei dati catastali per via telematica da parte dei sistemi informatici di altre amministrazioni, ai sensi dell'art. 59, comma 7-bis, del decreto legislativo 7 marzo 2005, n. 82.
 - [Allegato A](#): Schema di Convenzione per la fruizione della base dei dati catastali.
 - [Allegato B](#): Regole tecniche per l'accesso alla base dei dati catastali.

L'art. 1 comma 2 del Decreto ne definisce l'ambito di applicazione: "La base dei dati catastali di cui al comma 2 è resa disponibile alle pubbliche amministrazioni di cui all'articolo 1, comma 2, del decreto legislativo 30 marzo 2001, n. 165, ove necessaria per lo svolgimento, diretto o per il tramite dei soggetti dalle stesse delegati, dei compiti istituzionali e nel rispetto della normativa in materia di protezione dei dati personali e della normativa in materia di riutilizzo dei dati e delle informazioni catastali".

Le regole di utilizzo sono riportate nell'art. 4 del Decreto:

- La base dei dati catastali è resa accessibile esclusivamente quando l'utilizzazione del dato è necessaria per lo svolgimento, diretto o per il tramite dei soggetti delegati, dei compiti istituzionali dell'amministrazione richiedente.
- La pubblica amministrazione, all'atto della sottoscrizione della convenzione di cui all'articolo 2, attesta che la fruizione della base dei dati catastali è necessaria per lo svolgimento, diretto o per il tramite dei soggetti dalla stessa delegati, dei propri compiti istituzionali.
- L'accesso e l'utilizzo è consentito nel rispetto di quanto previsto dalla normativa vigente in materia di protezione dei dati personali, in materia di riutilizzazione dei dati e delle informazioni catastali, ferme restando le disposizioni di cui alla legge 7 agosto 1990, n. 241.

- Fatto salvo quanto previsto all'articolo 1, comma 3, le pubbliche amministrazioni non possono cedere a terzi, a qualsiasi titolo, i dati catastali acquisiti.
- Le pubbliche amministrazioni possono utilizzare i dati catastali all'interno dei propri sistemi informativi per lo svolgimento, anche in forma associata, dei compiti istituzionali, nonché integrarli, sotto la propria responsabilità, all'interno di servizi attinenti i medesimi compiti.

L'accesso telematico ai dati catastali è normato dall'art. 2:

1. Le pubbliche amministrazioni accedono ai servizi di interscambio delle catastali, previa sottoscrizione di specifica convenzione conforme allo schema allegato al presente decreto (allegato "A"), ai sensi dell'articolo 58, comma 2, del decreto legislativo 7 marzo 2005, n. 82.
2. Le tipologie dei servizi di cui al comma 1 e i relativi livelli di servizio sono definite nell'allegato B e pubblicate sul sito dell'Agenzia del territorio e del Comitato. L'Agenzia del territorio, sentito il Comitato, ne cura l'aggiornamento con cadenza periodica.
3. Le pubbliche amministrazioni convenzionate possono avvalersi, per l'accesso ai servizi d'interscambio, di altra pubblica amministrazione, ovvero di altro soggetto delegato o incaricato, previa comunicazione all'Agenzia del territorio.

Tipologia di forniture

Sono previste due diverse tipologie di fornitura telematica dei dati per gli enti interessati, nei limiti delle proprie competenze territoriali e dei fini istituzionali:

1. "*a richiesta*" per tutti gli enti interessati, pubblicate su specifica richiesta e riguardanti - sia per il catasto terreni e fabbricati che per la cartografia vettoriale -
 - tutti i dati catastali aggiornati ad una data scelta dall'Ente;
 - gli aggiornamenti registrati in un determinato intervallo temporale.
2. "*specifiche*" per i comuni, ovvero i file contenenti:
 - i dati degli accatastamenti e variazioni da fornire in base all'art. 34 quinquies della Legge 80/2006;
 - i dati derivanti dall'"Adempimento Unico" da fornire ai fini della gestione dell'ICI;
 - l'estrazione di tutti i dati metrici del catasto fabbricati, aggiornati alla data di produzione, ai fini della gestione della TARSU (comma 340 dell'art. 1 L. 311/2004);
 - l'aggiornamenti dei dati metrici del catasto fabbricati registrati in un intervallo temporale determinato ai fini della gestione della TARSU;
 - gli esiti delle attività di riclassamento delle singole unità immobiliari (L. 311/2004 art. 1, comma 336).

Sistema di Interscambio

Il Sistema di Interscambio è il canale comunicativo che, in modalità di cooperazione applicativa, permette ai soggetti cooperanti lo scambio di forniture. Per il prelievo delle forniture, ossia per l'attivazione dei web service di interesse messi a disposizione dall'Agenzia, gli enti devono dotarsi di specifiche applicazioni client. Lo scambio di messaggi e dati tra il Sistema dell'Agenzia e quello degli enti è basato su servizi della tipologia "Servizio di Porta Applicativa Light", secondo la terminologia del CNIPA, tramite buste di e-government nel formato "SOAP with Attachments", preventivamente firmato elettronicamente, secondo lo standard PKCS#7, mediante dispositivo di riconoscimento e sicurezza fornito dall'Agenzia del Territorio.

Condizione necessaria per usufruire dei servizi del Sistema di Interscambio è la disponibilità per l'Ente territoriale dell'accesso ai servizi di rete RUPA/SPC.

L'accesso ai servizi dell'Agenzia tramite le due modalità di connessione sono dettagliate nella documentazione tecnica resa disponibile sul sito dell'Agenzia.

2.2.2 Identificazione in rete del cittadino

L'identificazione in rete del cittadino è realizzabile a norma di legge mediante l'utilizzo delle carte di identificazione: la Carta di Identità Elettronica (CIE) e la Carta Nazionale dei Servizi (CNS).

La relativa normativa è la seguente:

- Legge 16 giugno 1998 n. 191 che all'articolo 2 comma 4 prevede le carte di identità elettroniche affidandone a successivi decreti l'attuazione operativa
- Il decreto del Presidente del Consiglio dei Ministri del 22 ottobre 1999, n. 437 che ha definito il regolamento per il rilascio della carta di identità elettronica e del documento di identità elettronico, mentre il decreto del Ministro dell'interno del 19 luglio 2000 ha fissato le relative regole tecniche e di sicurezza.
- La Carta Nazionale dei Servizi è introdotta nel quadro normativo italiano dal Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa (decreto del Presidente della Repubblica 28 dicembre 2000, n. 445), modificato dal decreto legislativo 23 gennaio 2002 n.10 e dal decreto del Presidente della Repubblica 7 aprile 2003 n. 137, in attuazione della direttiva europea 1999/93/CE relativa ad un quadro comunitario per le firme elettroniche.
- Il decreto legislativo 4 aprile 2006, n. 159 recante "Disposizioni integrative e correttive al decreto legislativo 7 marzo 2005, n. 82, recante codice dell'amministrazione digitale" aggiorna anche, nell'articolo 64, le regole per l'accesso ai servizi erogati in rete dalle pubbliche amministrazioni.
- L'attuazione di quanto previsto nel Testo unico è disciplinata dal decreto del Presidente della Repubblica 2 marzo 2004, n. 117 "Regolamento recante disposizioni la diffusione della carta nazionale dei servizi, a norma dell'articolo 27, comma 8, lettera b), della legge 16 gennaio 2003, n.3". Tale decreto prevede che la Carta Nazionale dei Servizi è emessa dalle pubbliche amministrazioni interessate "al fine di anticiparne le funzioni di accesso ai servizi in rete delle pubbliche amministrazioni" (art. 2 comma 1), intendendo quindi la CNS quale strumento "ponte" verso la carta d'identità elettronica, che resta il mezzo nazionale per l'identificazione in rete. Di conseguenza il Decreto prevede che non sia possibile rilasciare una CNS a cittadini già in possesso di CIE. Questa previsione è modificata dalla Legge n. 69 del 18 giugno 2009 che all'art. 37 autorizza fino al 31 dicembre 2010 il rilascio di CNS anche a cittadini dotati di CIE.

Si richiede che tutti i siti Web che forniscono servizi ai cittadini, quando prevedono l'ingresso di un cittadino in una parte del sito che prevede l'accesso ad informazioni specifiche del cittadino stesso, anche se in sola lettura, siano realizzati in modalità sicura secondo la specifica HTTPS (HTTPS over SSL) in accordo alla specifica tecnica "Linee guida per l'emissione e l'utilizzo della Carta nazionale dei Servizi" del CNIPA, contenuta in Allegato 5.

Il sito web, quando un cittadino si identifica con la carta elettronica, deve sempre restituire gli estremi dell'avvenuta identificazione ricavati dalla Carta:

- Codice fiscale del cittadino
- Soggetto emittitore della Carta
- Numero seriale della Carta

Ammettendo il cittadino ai servizi o, in alternativa se del caso, motivando l'eventuale non ammissione ai servizi.

Il sito Web deve sempre effettuare la verifica della validità della Carta sia valutando le informazioni del certificato che verificando la sua eventuale revoca o sospensione mediante la verifica in tempo reale o differito delle Certificate Revocation List (CRL) e Certificate Suspension List (CSL).

In alternativa all'identificazione del cittadino via CNS/CIE, nel periodo in cui tale strumento non sia ancora completamente diffuso, è accettabile un'autenticazione basata su meccanismi di username e password, purché garantiscano la corretta associazione di tali identificativi di rete all'identità del cittadino.

Esempi di modalità operative che garantiscono tale associazione:

- per il sito web di un qualsiasi Ente Pubblico: identificazione del cittadino e rilascio dei relativi identificativi di rete presso uno sportello dell'Ente Pubblico
- per il sito web di un Comune: autodichiarazione del cittadino sul sito web con invio degli identificativi in parte nella transazione web stessa ed in parte via postale/POSTEL al domicilio del cittadino come risultante dall'Anagrafe

I siti Web dovranno inoltre essere predisposti, in accordo con il paragrafo 10.1.2 "Tecnologie per un'identità federata" delle Linee Guida CNIPA in Allegato 5, per l'utilizzo della tecnologia SAML (Security Assertion Markup Language) versione 2.0 o successiva, che è uno standard aperto per la realizzazione delle funzionalità di autenticazione, autorizzazione e single sign on sul web.

In futuro potrà essere emessa una specifica del CRIPAL concernete questi aspetti ed è atteso che non vi siano ostacoli tecnologici alla sua adozione.

2.2.3 Sportello Unico per l'Edilizia (SUE)

Il **D.P.R. 380/2001** - intitolato "*Testo unico delle disposizioni legislative e regolamentari in materia edilizia*" contiene i principi fondamentali e generali e le disposizioni per la disciplina dell'attività edilizia, istituisce lo *Sportello unico per l'edilizia (art. 5)* e ne disciplina l'operatività:

1. Le amministrazioni comunali, nell'ambito della propria autonomia organizzativa, provvedono, anche mediante esercizio in forma associata delle strutture ai sensi del capo V, Titolo II, del decreto legislativo 18 agosto 2000, n. 267, ovvero accorpamento, disarticolazione, soppressione di uffici o organi già esistenti, a costituire un ufficio denominato sportello unico per l'edilizia, che cura tutti i rapporti fra il privato, l'amministrazione e, ove occorra, le altre amministrazioni tenute a pronunciarsi in ordine all'intervento edilizio oggetto della richiesta di permesso o di denuncia di inizio attività.

2. Tale ufficio provvede in particolare:
- a) alla ricezione delle denunce di inizio attività e delle domande per il rilascio di permessi di costruire e di ogni altro atto di assenso comunque denominato in materia di attività edilizia, ivi compreso il certificato di agibilità, nonché dei progetti approvati dalla Soprintendenza ai sensi e per gli effetti degli articoli 36, 38 e 46 del decreto legislativo 29 ottobre 1999, n. 490;
 - b) a fornire informazioni sulle materie di cui al punto a), anche mediante predisposizione di un archivio informatico contenente i necessari elementi normativi, che consenta a chi vi abbia interesse l'accesso gratuito, anche in via telematica, alle informazioni sugli adempimenti necessari per lo svolgimento delle procedure previste dal presente regolamento, all'elenco delle domande presentate, allo stato del loro *iter* procedurale, nonché a tutte le possibili informazioni utili disponibili;
 - c) all'adozione, nelle medesime materie, dei provvedimenti in tema di accesso ai documenti amministrativi in favore di chiunque vi abbia interesse ai sensi dell'art. 22 e seguenti della legge 7 agosto 1990, n. 241, nonché delle norme comunali di attuazione;
 - d) al rilascio dei permessi di costruire, dei certificati di agibilità, nonché delle certificazioni attestanti le prescrizioni normative e le determinazioni provvedimentali a carattere urbanistico, paesaggistico-ambientale, edilizio e di qualsiasi altro tipo comunque rilevanti ai fini degli interventi di trasformazione edilizia del territorio;
 - e) alla cura dei rapporti tra l'amministrazione comunale, il privato e le altre amministrazioni chiamate a pronunciarsi in ordine all'intervento edilizio oggetto dell'istanza o denuncia, con particolare riferimento agli adempimenti connessi all'applicazione della parte seconda del testo unico.

Il SUE presenta una componente di back office e una componente di front office. La componente di front office deve comprendere una parte pubblica accessibile a tutti i cittadini, che espone le informazioni di carattere generale, e una parte riservata, accessibile all'utente interessato alla specifica pratica.

La componente pubblica, che rende disponibili in rete le informazioni dei procedimenti, deve essere realizzata in modalità web services al fine di garantire l'interoperabilità con i sistemi informativi di altre amministrazioni che necessitano di informazioni di carattere generale sullo stato della realizzazione degli interventi urbanistici, tra cui il SIT della Regione Puglia. E' di interesse dell'Amministrazione Regionale poter disporre di un livello informativo contenente le informazioni minime che consentano di valutare lo stato di attuazione dei Piani Urbanistici. Inoltre, queste informazioni sono utili ai fini dell'aggiornamento, diretto o indiretto, delle cartografie di base.

Il set minimo di informazioni pubbliche richieste è individuato nell'elenco che segue:

- definizione dell'intervento (ai sensi dell'art.3 del D.P.R. 380/2001 - Testo Unico in materia Edilizia ss.mm.ii.)
- data inizio lavori
- data fine lavori
- specifica se la data di fine lavori è reale o presunta
- localizzazione catastale- Numero Foglio
- localizzazione catastale- Numero Particella
- localizzazione catastale- Numero Subalterni
- indirizzo (via, numero civico, interno e piano)
- progettista, esecutore, direttore lavori
- breve descrizione
- numero protocollo pratica, anno protocollo pratica
- richiedente

- tipo pratica, (ai sensi dell'art.3 del D.P.R. 380/2001 - Testo Unico in materia Edilizia – e ss.mm.ii.)
- descrizione tipo pratica “altro”
- specifica se la pratica è “in sanatoria”
- specifica se la pratica è “in deroga agli strumenti urbanistici”
- stato dell'iter della pratica
- funzionario che segue la pratica

2.3 Servizi con Priorità 3

2.3.1 Circolarità Anagrafica

Il Processo di Circolarità Anagrafica prevede che le Amministrazioni Comunali utilizzino il Sistema XML-SAIA V2, messo a disposizione dal Ministero dell'Interno per il tramite del CNSD (Centro Nazionale Servizi Demografici), inizialmente per popolare l'Indice Nazionale delle Anagrafi ed a regime per notificare le variazioni anagrafiche. Il CNSD convalida le informazioni anagrafiche e le inoltra alla Regione Puglia autorizzata dalla Direzione Centrale dei Servizi Demografici a fruire di tali informazioni per i propri scopi istituzionali.

Il Modello Federato di Governance, previsto dalla Convenzione tra Ministero dell'Interno e Regione Puglia approvata con Deliberazione della Giunta Regionale n. 523 del 7/4/2009 (BURP n. 63 del 28/04/2009), integra il Sistema XML – SAIA, in un contesto Infrastrutturale e di Servizi per l'Interoperabilità e Cooperazione Applicativa SPC/SPCoop-Oriented.

La Regione Puglia nel Processo di Circolarità Anagrafica recita un duplice ruolo:

- Coadiutore - delle Amministrazioni Comunali per il popolamento ed aggiornamento dell'INA utilizzando le infrastrutture regionali di rete. (Questo ruolo sarà assunto solo ed esclusivamente quando il processo vedrà una sorta di simbiosi mutualistica CNDS – Regione).
- Coordinatore territoriale - Promuove la circolarità delle informazioni anagrafiche fra le Amministrazioni del proprio territorio utilizzando le infrastrutture tecnologiche ed i Servizi regionali della Cooperazione Applicativa.

2.4 Servizi con Priorità 4

2.4.1 Piani Urbanistici Generali (PUG)

Il Piano Urbanistico Generale (PUG) deve essere realizzato in conformità alla vigente normativa regionale con particolare riferimento al Documento Regionale di Assetto Generale (DRAG) e alle sue applicazioni, deve prevedere il set di strati informativi minimi definito e descritto nelle “Istruzioni Tecniche per l'Informatizzazione dei PUG” come da Atto di Indirizzo di Giunta regionale del 13 Luglio 2009.

Riferimenti normativi

- L. R. 20/ 2001 - “Norme generali di governo e uso del territorio”, art. 4, comma 3, lett. b e art.5, comma 10 bis

- Documento Regionale di Assetto Generale (DRAG) - INDIRIZZI, CRITERI E ORIENTAMENTI PER LA FORMAZIONE, IL DIMENSIONAMENTO E IL CONTENUTO DEI PIANI URBANISTICI GENERALI (PUG) – approvato con Deliberazione di Giunta Regionale n. 1328/2007 - Pubblicato sul B.U.R.P. n. 120 del 29-8-2007.
- Circolare 1/2008 – “Note esplicative sulle procedure di formazione dei Piani Urbanistici Generali dopo l’entrata in vigore del Documento Regionale di Assetto Generale (DRAG)”, approvata con DELIBERAZIONE DELLA GIUNTA REGIONALE 26 febbraio 2008, n. 214 pubblicata sul B.U.R.P. n. 40 del 12-03-2008
- Atto di Indirizzo di Giunta Regionale, adottato con DELIBERAZIONE DELLA GIUNTA REGIONALE del 13 luglio 2009, n. 1178, pubblicato sul B.U.R.P. n. 111 del 21-7-2009, per l’introduzione delle “Istruzioni Tecniche per la Informatizzazione dei PUG”.

La Regione Puglia ha definito uno standard regionale per la produzione degli strati informativi costituenti il nuovo Piano Urbanistico Generale (PUG). Le istruzioni tecniche definiscono gli strati informativi minimi (considerati, secondo la logica del GIS, quali insiemi di elementi ed informazioni coerenti ed omogenee) che è necessario produrre e restituire alla Regione. Naturalmente la composizione di questi strati nelle “Tavole” o “Elaborati” di Piano è lasciata all’assoluta discrezionalità dell’ufficio di Piano, fermo restando l’integrità e la corrispondenza geometrica ed alfanumerica con gli strati richiesti. Nello specifico, le informazioni fondamentali per cui è previsto un confronto a scala sovralocale sono state definite secondo categorie “chiuse”, mentre sono state lasciate “aperte” quelle informazioni necessarie per ricostruire le analisi e le volontà relative alle specificità locali. Le istruzioni tecniche sono definite nei documenti:

- 1) Istruzioni Tecniche per la Informatizzazione dei PUG nell’ambito del SIT Regionale - Modello Logico: DELIBERAZIONE DELLA GIUNTA REGIONALE 13 luglio 2009, n. 1178
- 2) Istruzioni Tecniche per la Informatizzazione dei PUG nell’ambito del SIT Regionale - Modello Fisico (Allegato 4)

E’, inoltre, necessario che i PUG vengano predisposti sulla base di informazioni ufficiali e condivise. A tale scopo la Regione ha predisposto, nell’ambito del Progetto SIT – Puglia, un insieme di basi informative che mette a disposizione attraverso il proprio portale, insieme al patrimonio di conoscenza disponibile a livello regionale affinché queste informazioni (visualizzabili, consultabili, e scaricabili) siano di supporto a tutte le analisi ed elaborazioni che consentono di costruire il sistema delle conoscenze e dei quadri interpretativi, nonché l’elaborazione dei P.U.G..

Sulle medesime basi di dati si stanno realizzando anche i nuovi strumenti urbanistici in corso di definizione, tra i quali il Piano Paesaggistico Regionale (con le sue carte tematiche: Carta dei Beni Culturali e Carta Idrogeomorfologica), che vengono messi a disposizione sul medesimo portale man mano che diventano disponibili.

Questi livelli informativi, oltre ad essere la base sulla quale verrà realizzato il Piano, si configurano anche come gli elementi su cui andare, eventualmente, a realizzare strati cartografici di specifico interesse comunale quali, ad esempio, mappe di maggior dettaglio (1:2.000/ 1:1.000/ 1:500) del centro urbano che, in tal modo, risultano coerenti con quelle regionali, nei contenuti e nell’inquadramento topografico e sistema di riferimento (ETRS89 UTM-WGS84).

3 Componenti rese disponibili dal Centro Tecnico Regionale

Le componenti descritte nel presente capitolo sono state realizzate e sono mantenute a cura del Centro Tecnico Regionale e rese gratuitamente disponibili a tutte le Amministrazioni della Regione.

Queste componenti sono pienamente conformi alle specifiche tecniche di cui al capitolo precedente. L'uso di queste componenti non è obbligatorio, esse costituiscono comunque l'implementazione di riferimento.

Il Centro Tecnico Regionale garantisce, per queste componenti, i seguenti servizi:

- manutenzione conservativa ed evolutiva dei software
- ambiente di download in rete per l'accesso ai software stessi ed alla documentazione tecnica di installazione ed utilizzo
- assistenza tecnica da remoto, tipicamente con l'ausilio della stessa piattaforma di download mediante strumenti quali i forum tecnici che consentono il riuso immediato delle esperienze
- organizzazione su richiesta, al raggiungimento di un numero minimo di richieste, di seminari tecnici (anche WEB Seminars)

3.1 Protocollo Informatico

E' disponibile un sistema di Protocollo Informatico, interamente basato su ambienti Open Source, denominato Protocollo Informatico SCATEL (PIS).

L'architettura software è la seguente:

- Sistema Operativo Linux
- Application Server: Tomcat
- Database: virtualizzato attraverso Hibernate, attualmente distribuito con configurazione per MySQL

3.2 Gestione informatizzata degli atti amministrativi

E' disponibile un sistema di gestione degli atti amministrativi, interamente basato su ambienti Open Source, denominato "MicroActa".

L'architettura software è la seguente:

- Sistema Operativo Linux
- Document Management System (DMS): Alfresco
- Database: MySQL

3.3 PEC

Il Centro Tecnico Regionale di InnovaPuglia S.p.A., essendo uno dei gestori iscritti nell'Albo del CNIPA, eroga gratuitamente il servizio PEC per le caselle istituzionali agli EE.LL. della regione puglia.

3.4 Cooperazione Applicativa

E' disponibile la Porta di Dominio SCATEL (PDDS), già installata presso la Regione Puglia che ha ottenuto la qualificazione CNIPA e quindi l'abilitazione ad operare in ambito SPC.

L'Ente deve installare la Porta di Dominio presso il proprio accesso RUPAR-SPC ed accreditare e qualificare la propria porta presso il CNIPA.

E' opportuno ricordare che la qualificazione della Porta di Dominio di un Ente in SPCoop non concerne la tecnologia della Porta, ma bensì i servizi offerti dalla Porta stessa.

Per questo motivo, se Enti diversi installassero la stessa tecnologia di Porta di Dominio, dovrebbero comunque procedere alla qualificazione della propria Porta. Ovviamente, qualora si installi una tecnologia di Porta di Dominio che abbia già ottenuto, attraverso uno o più Enti, una qualificazione CNIPA, è legittimo attendersi che l'ottenimento della nuova qualificazione non comporti difficoltà particolari.

Le componenti di Protocollo Informatico (PIS) e di Gestione degli Atti Amministrativi (MicroActa), sono dotate delle componenti necessarie per interfacciarsi, una volta correttamente configurate, con la PDDS ed esporre quindi i servizi di cui agli Allegati 1 e 2.

3.5 Circolarità anagrafica

La Convenzione sottoscritta tra Ministero dell'interno e Regione Puglia permette di semplificare gli adempimenti da parte di Comuni, che hanno solo l'obbligo di utilizzare il sistema INA-SAIA già reso disponibile dal Ministero dell'interno.

La Regione Puglia provvede realizzare il sistema che, interfacciandosi ai servizi SPCoop del Ministero, ottiene i dati prodotti dai Comuni per la loro distribuzione ad altri Enti regionali come, in primo luogo, le Aziende sanitarie Locali.

3.6 Identificazione in rete del cittadino

E' disponibile materiale di supporto per la configurazione in modalità SSL e Strong Authentication del più popolare Wb server Open Source: Apache.

E' anche disponibile un sito di riferimento, basato su Apache, che effettua l'identificazione del cittadino fornendo le informazioni richieste.

- Codice fiscale del cittadino
- Soggetto emettitore della Carta
- Numero seriale della Carta

3.7 Sistema Informativo Territoriale (SIT Regionale)

Relativamente a quanto descritto nel capitolo precedente, nell'ambito del SIT Regionale sono stati implementati dati e servizi territoriali che sono resi disponibili alle Amministrazioni Locali, per l'utilizzo a titolo gratuito, dall'Amministrazione Regionale. I dati territoriali rappresentano una infrastruttura omogenea a livello regionale, che contiene i livelli più significativi ai fini della descrizione degli oggetti e delle caratteristiche fisiche del territorio. Sono stati realizzati seguendo le specifiche tecniche descritte nel capitolo precedente e ad un livello di dettaglio tale da essere funzionali ai livelli della pianificazione locale. Eventuali approfondimenti a scale di maggior

dettaglio devono essere realizzati a tutti gli effetti come integrazione e aggiornamento di quanto già esistente.

Il SIT espone servizi di ricerca, consultazione, download dei dati territoriali attraverso il geoportale <http://www.sit.puglia.it>. Il SIT espone poi per gli utenti istituzionali servizi applicativi orientati a specifici settori delle amministrazioni, integrati sia con il database territoriale che tra di loro e conformi alla normativa nazionale/regionale.

L'uso dei servizi territoriali non è obbligatorio, essi costituiscono comunque l'implementazione di riferimento.

Cartografie di base

Tutti i dati cartografici sono realizzati nel Sistema di riferimento ETRS89, proiezione UTM-WGS84, fuso 33N, sono integrati geometricamente tra di loro, in quanto derivati dalle stesse riprese aerofotogrammetriche e dalla CTR quale prima elaborazione di esse.

Nel dettaglio, sono disponibili i seguenti dati:

reti geodetiche regionali: Sono state realizzate sia la rete di raffittimento della rete IGM95 che la rete di appoggio. La rete di raffittimento è formata da 365 vertici di nuova istituzione, materializzati in accordo alle Specifiche Tecniche Raffittimento della Rete Fondamentale IGM95 (IntesaGIS). La rete di appoggio è costituita da 2641 fotografici.

fotogrammi digitali: derivano dal volo aereo realizzato a partire da agosto e conclusosi a novembre 2006 (tranne piccole aree la cui copertura è relativa a marzo 2007), ed eseguito utilizzando la camera fotogrammetrica digitale Z/I Imaging DMC della Intergraph, a colori e con fotogrammi con risoluzione a terra di circa 20 cm.. La copertura totale del territorio regionale ha comportato l'acquisizione complessiva di circa 26.000 fotogrammi.

carta tecnica: è stata realizzata alla scala 1:5.000, la restituzione segue il taglio dei fogli IGM in scala 1:50.000, ma sono anche disponibili i files che seguono il grigliato dei fogli in scala 1:5.000, editati per la stampa e corredati di bandella che riporta i dettagli tecnici della restituzione e dell'area inquadrata

database topografico: rappresenta una evoluzione della carta tecnica regionale nella logica di un vero e proprio database relazionale, aggiornabile nel tempo. E' articolato in un insieme di tipologie di elementi territoriali acquisibili da fonti diversificate (aerofotogrammetria, carta tecnica esistente o carte tematiche) dette CLASSI:

- le classi raccolgono secondo criteri di omogeneità (per geometria e contenuto) gli oggetti che rappresentano il territorio
- per ogni oggetto vengono specificate le caratteristiche attraverso la valorizzazione di attributi stabiliti, individuazioni di componenti geometriche
- per ciascuna classe viene riportata l'obbligatorietà di geometrie e attributi da rilevare alle diverse scale
- esse sono organizzate logicamente in STRATI e TEMI secondo la strutturazione gerarchica
- STRATO-TEMA-CLASSE.

DTM: realizzato secondo lo standard definito nel documento "Prescrizioni tecniche per la produzione di Modelli Digitali del Terreno", prodotto dall'apposito gruppo di lavoro nominato dall'Intesa Stato-Regioni-Enti Locali sui Sistemi Informativi Territoriali. Utilizza per l'orientamento dei modelli direttamente i parametri forniti dalla triangolazione aerea, è conforme al

livello 3 delle specifiche. Il DTM così realizzato è in formato ASCII RASTER e si presenta come un grigliato regolare, con passo di griglia di 8 metri.

Uso del suolo: geometricamente essa è compatibile con la scala 1:5.000, l'unità areale minima cartografata è di 2.500 mq; i contenuti tematici sono conformi allo standard definito a livello europeo con le specifiche del progetto CORINE Land Cover (con ampliamento al IV livello), comportando la caratterizzazione della Legenda in 69 classi.

Ortofoto: digitale a colori: è a scala 1:5.000 con risoluzione a terra del pixel di 50 cm, deriva dal volo aereo realizzato per la produzione della CTR, "proiettando" matematicamente i fotogrammi sulla superficie di riferimento cartografico (l'ellissoide), secondo una proiezione localmente ortogonale.

Oltre alle cartografie di base, il SIT pubblica, con gli stessi criteri e standard tecnici, cartografie e dati tematici funzionali alla redazione dei Piani Urbanistici e in particolare:

Carta idrogeomorfologica: è stata realizzata dall'Autorità di Bacino utilizzando come base di riferimento i dati topografici e le riprese aeree realizzate. I dati tematici rappresentati derivano in parte da banche dati ufficiali realizzate nel corso di precedenti progetti e piani di carattere regionale (ad es. Piano di Tutela delle Acque, Piano Regionale delle Coste), opportunamente verificati e adeguati, e soprattutto da analisi ed elaborazioni eseguite ex novo. E' strutturata in temi ed elementi, la cui scelta nonché i criteri di rappresentazione cartografica sono stati effettuati coerentemente con gli standard previsti dalle linee guida "Carta Geomorfologica d'Italia 1.50.000 – guida al rilevamento", edito dal Servizio Geologico Nazionale (Quaderni Serie III – Vol. 4 - 1994).

Carta dei beni culturali: realizzata con il coinvolgimento organico della Direzione Regionale per i Beni Culturali e Paesaggistici della Puglia, delle quattro Università pugliesi censisce e descrive le caratteristiche culturali del territorio pugliese, utilizzando una strategia contestuale che consente di superare i tradizionali modelli di censimento basati su una concezione puntiforme dei beni culturali. E' articolata in tre tematismi essenziali: Patrimonio culturale, Paesaggio e Vincoli. Oggetto del censimento sono stati tutti i beni immobili e le aree di valore culturale e paesaggistico localizzati in aree extraurbane (in particolare quelli indicati agli articoli 136 e 142 del Codice dei Beni Culturali e del Paesaggio), già editi o i cui dati erano presenti negli archivi delle Soprintendenze, delle Università o di altri enti di ricerca. A questi dati si sono aggiunti tutti quelli raccolti da precedenti strumenti di pianificazione a livello regionale (PUTT/P e relativi adeguamenti dei piani comunali), provinciale (PTCP) e comunale (Piani Urbanistici Generali).

Indagini sui flussi di traffico: localizzate sulle principali arterie regionali, le osservazioni sono state effettuate complessivamente nel periodo luglio – dicembre 2007 e sono relative a:

- conteggi classificati dei flussi di traffico (presso sezioni caratteristiche della viabilità ordinaria regionale);
- indagini Origine-Destinazione (O/D) con interviste dirette ai conducenti di veicoli leggeri e pesanti (su sezioni stradali, caselli autostradali e ai porti di Bari e Brindisi).

Servizi di accesso ai dati

Il SIT ha sviluppato e rende disponibili diverse modalità di accesso e fruizione dei dati, in funzione dei requisiti applicativi e dell'utenza a cui sono destinati.

In particolare:

Consultazione/download.

Sono servizi orientati ai cittadini e ai professionisti con l'obiettivo di condividere la conoscenza del territorio, dagli elementi topografici all'uso del suolo, dai Beni Culturali e del Paesaggio ai risultati delle indagini sui flussi di traffico, anche al fine di promuovere una maggiore consapevolezza dello stato dei luoghi e una maggiore attenzione al territorio. Presentano una semplice interfaccia che consente le operazioni più diffuse di navigazione e consultazione (pan, zoom in/out, identify, ecc.).

I servizi di download mettono a disposizione dei cittadini e dei professionisti gli stessi dati che sono utilizzati dagli utenti istituzionali: carta tecnica regionale completa di tutti i layer e in formato vettoriale shapefile, il modello numerico delle altezze in formato ASCII, l'ortofoto in formato ECW, monografie in formato .pdf. Sono messi a disposizione dell'utenza anche gli strumenti che ne possono agevolare l'utilizzo, quali grigliati, file di proiezione, file di leggende oltre alla documentazione necessaria alla corretta interpretazione dei dati.

Al fine di consentire all'utente finale la duplicazione dei dati in locale, la certezza di consultare/utilizzare una versione certificata dei dati richiesti in quanto il dato viene distribuito direttamente dalla Regione che lo produce o ne certifica l'attendibilità e la certezza di consultare/utilizzare il dato più aggiornato, sono forniti i servizi di pubblicazione dei dati in formato WMS.

Questo insieme di servizi è disponibile nella sezione del portale "Consultazione" che, a sua volta, è suddivisa in sottosezioni Dati Tematici, Dati Topografici e Download. La descrizione di dettaglio è contenuta nell'Allegato 3.

Consultazione avanzata

Sono diversi strumenti che consentono la "gestione" online delle banche dati e, quindi, non solo la consultazione, ma anche la modifica degli strati informativi. Tali funzionalità di base, sviluppate e raggruppate su tre livelli (web services, task e applicazioni), nel loro insieme rappresentano un ambiente webgis pensato per utenti istituzionali. Sono presenti le funzionalità GIS più comunemente utilizzate, dall'editing alla stampa in scala, alla tematizzazione di una mappa, rese disponibili via web. Sinteticamente, consentono all'utente di:

- Personalizzare a piacimento la visualizzazione e tematizzazione (definendone l'ordine nonché le campiture, gli spessori, i colori, i tipi di linea, le trasparenze, la scala di visualizzazione minima e massima, etc.), salvando le impostazioni personalizzate per renderle disponibili per successive applicazioni,
- personalizzare il processo di stampa, a partire da layout predefiniti in cui scegliere scala, dimensione, orientamento, nonché inserendo legende e mascherini e esportare i file da stampare in file in formato .pdf,
- caricare, visualizzare, georiferire e assegnare o modificare sistemi di proiezione anche a propri dati (raster e vettoriali),
- editare gli strati informativi via web: inserire, modificare, cancellare features utilizzando tools quali lo snapping, oppure crearne di nuovi inserendo puntualmente i vertici e definendo tipologia, nome, sistema di proiezione, attributi,
- effettuare operazioni di geoprocessing e operazioni sulle e tra le tabelle, tramite analisi statistiche (semplici o aggregate) e join, su elementi selezionati.

Questo insieme di servizi è disponibile nella sezione del portale "Consultazione avanzata" che, a sua volta, è suddivisa in sottosezioni. La descrizione di dettaglio è contenuta nell'Allegato 3.

Web Services di base

E' possibile accedere ai dati contenuti all'interno del DB del SIT attraverso i web services di base esposti dallo stesso SIT. Questi sono sviluppati con tecnologia J2EE, JAX-WS ed esposti come web services SOAP/XML, descritti secondo lo standard WSDL e catalogati in UDDI. Possono essere pertanto interrogati da client SOAP e utilizzati in altri applicativi. La creazione del Client SOAP e la integrazione dei servizi di base in altri applicativi resta a carico dell'Ente. L'utilizzo dei web services di base è subordinato alla presenza di un account registrato nel SIT.

Rispetto ai servizi di consultazione avanzata, i web services di base ne rappresentano i servizi elementari che poi possono essere associati in funzione di specifiche esigenze applicative.

Questi servizi di base sono descritti nell'Allegato 3.

Catalogo dei metadati

Il SIT, attraverso il riuso del Repertorio Nazionale Dati Territoriali (RNDDT) sviluppato dal CNIPA e la successiva integrazione nell'infrastruttura di servizi regionali, consente di esporre servizi per la creazione del catalogo dei dati territoriali regionali (RRDDT), descrivendone i livelli di qualità attraverso i relativi metadati.

L'RRDDT è un catalogo di metadati basato sugli Standard ISO19115, 19119 e 19139 ed è coerente con la direttiva INSPIRE e con il Regolamento europeo sui metadati. Esso si delinea come un registro pubblico per conoscere con certezza quali informazioni sono disponibili, quali sono le loro caratteristiche tecniche e con quali modalità è possibile utilizzarle.

Questo servizio fornisce le funzionalità tipiche di un servizio di catalogo e realizza due macroprocessi:

- la consultazione dei metadati, accessibile a tutti;
- la gestione dei metadati riservata alle Amministrazioni Pubbliche.

Oltre ai dati, l'RRDDT consente la descrizione dei servizi applicativi, sempre attraverso l'inserimento dei relativi metadati. Quindi in sintesi nel Catalogo sono presenti:

- metadati relativi ai dati territoriali (cartografie tecniche tematiche etc);
- metadati relativi ai servizi (servizi di pianificazione territoriale, protezione civile etc.);
- metadati relativi alle nuove acquisizioni di dati territoriali

Questo insieme di servizi è disponibile nella sezione del portale "Repertorio Metadati" che, a sua volta, è suddivisa in sottosezioni. La descrizione di dettaglio è contenuta nell'Allegato 3.

Piani Urbanistici Comunali

La componente Pianificazione Territoriale del SIT fornisce alle amministrazioni Locali e Regionali servizi a supporto dell'intero processo di pianificazione. In particolare, i servizi messi a disposizione delle amministrazioni comunali consentono:

- a) l'elaborazione dei Piani in generale e in particolare dei PUG. I servizi per la elaborazione tecnica dei piani mettono a disposizione dei tecnici funzionalità di carattere generale che permettono di:

- definire una propria area (Repository), definire e gestire gli accessi ad aree riservate (Schedari/Cartelle) per sottocategorie di utenti (quali i diversi gruppi di professionisti che lavorano al medesimo piano), in cui saranno archiviati, aggiornati e gestiti i dati specifici;
- attivare i servizi di segnalazione, definendo modalità e ordine di visualizzazione dei layers di un progetto, condividerlo con altri utenti che hanno la possibilità di inserire simboli, geometrie, note che verranno memorizzate sotto forma di nuovi strati informativi;
- visualizzare uno stesso progetto su finestre correlate, interrogando alternativamente gli elementi;
- eseguire analisi spaziali e tridimensionali sugli strati; effettuare operazioni di geoprocessing e operazioni sulle e tra le tabelle, tramite analisi statistiche (semplici o aggregate) e join, su elementi selezionati;
- gestire le relazioni al piano, creandole, modificandole, cancellandole, inserendo allegati.

Gli stessi servizi sono quindi personalizzati sui PUG, ovvero è possibile utilizzare le stesse funzionalità su un geodatabase già strutturato e coerente con gli standard definiti a livello regionale.

- b) La gestione informatizzata dell'iter di approvazione del PUG. Il servizio per l'informazione sullo stato della pianificazione permette la gestione informatizzata (attraverso un sistema di workflow management) dell'intero iter del PUG, in conformità alla normativa regionale, inclusa la fase delle segnalazioni e delle osservazioni, della cooperazione interistituzionale e della partecipazione pubblica. Per meglio adeguarsi alla situazione del territorio regionale, rende disponibili tre "iter" (partendo da tre differenti stati del processo) consentendo anche alle Amministrazioni che hanno già avviato la redazione del Piano e provveduto all'approvazione dei primi provvedimenti, di poterne usufruire.
- c) La verifica di compatibilità attraverso l'ausilio di servizi e funzionalità ideate ad hoc con l'obiettivo da un lato di accelerare il processo e, dall'altro, di cogliere elementi di incongruità che potrebbero sfuggire ad una comparazione esclusivamente visuale delle tavole di piano. Realizzati per il livello regionale, queste funzionalità possono consentire una verifica preliminare da parte dell'amministrazione comunale. Le funzionalità consentono di:
- incrociare più strati, permettendone la verifica topologica (sovrapposizioni/esclusioni), memorizzando il risultato in un nuovo strato informativo;
 - verificare le distanze tra elementi e calcolare rapporti tra entità geometriche e/o alfanumeriche;
 - utilizzare un ambiente di visualizzazione tridimensionale per dati raster e vettoriali, sulla base di DTM, utilizzando simboli e librerie 3D, creando viste in relazione a punti di

vista, realizzando profili delle superfici, simulando interventi e scenari di trasformazione territoriale.

- d) l'osservazione delle fasi di attuazione dei vari strumenti integrati (ad es. Programmi di recupero urbano (PRU), Progetti integrati di riqualificazione delle periferie (PIRP),...), localizzando i programmi sul territorio, registrandone l'evoluzione nel tempo, mettendoli in rapporto con le risorse impegnate ed i risultati. Il sistema permette di registrare le richieste di finanziamento con tutte le informazioni correlate (comuni interessati, estensione territoriale e popolazione, tipologia di fondi, data di presentazione/approvazione, importo richiesto/finanziato,...). E' inoltre possibile:
- inserire, modificare, cancellare e compilare le schede dei diversi Programmi, aggiungendo descrizioni e allegati, associando l'estensione dell'area oggetto di Programma;
 - consultare le schede e derivarne report di riepilogo;
 - consultare e confrontare le schede tramite query personalizzate generando report, visualizzando su mappa le informazioni collegate ad entità territoriali, con memorizzazione dello strato corrispondente.
- e) il mosaico dei piani urbanistici comunali: visualizzare e analizzare tutti gli strati informativi prodotti secondo specifiche regionali (Istruzioni Tecniche per l'informatizzazione dei PUG), confrontarli su diversi comuni/province selezionati/e. Tra le funzionalità peculiari di questo servizio, la possibilità di unire su un unico strato o dissolvere sulla base di un attributo.

Questo insieme di servizi è disponibile nella sezione del portale "Pianificazione" che, a sua volta, è suddivisa in sottosezioni. La descrizione di dettaglio è contenuta nell'Allegato 3.

Interscambio dati catastali

Tra le azioni intraprese nell'ambito del SIT, la Regione ha sottoscritto 2 convenzioni con l'Agenzia del Territorio:

1. per l'accesso ai dati catastali attraverso il sistema di interscambio.
2. per la trasposizione della cartografia catastale vettoriale dal sistema di proiezione Cassini Soldner al sistema WGS84 previa correzione e corretto posizionamento della stessa nei sistemi catastali locali, la rasterizzazione e georeferenziazione dei fogli di impianto.

Il SIT adotta il modello logico e fisico del DBTI di SigmaTer, già verificato con l'Agenzia del Territorio, sperimentato da diversi Comuni e aderente agli standard di riferimento del progetto PR5SIT (Db topografico dell'IntesaGIS e metadati ISO TC 211-19115 con gli adattamenti previsti dall'IntesaGIS). Nello specifico, attraverso la partecipazione al partenariato Sigmater, il SIT riusa sia il modello dei dati che i servizi di accesso al dato.

Le informazioni catastali vengono condivise tramite cooperazione applicativa in un ambiente composto da:

Porta Applicativa AdT: E' un componente software del Sistema Informativo dell'Agenzia del Territorio che racchiude un insieme di funzionalità che permettono lo scambio di informazioni con il Sistema Informativo di un altro Ente della PA.

Porta Applicativa Ente: E' un componente software del Sistema Informativo Ente P.A. che racchiude un insieme di funzionalità che permettono lo scambio di informazioni con il Sistema Informativo dell'Agenzia del Territorio

Ambiente di Interscambio: E' l'insieme dei servizi esposti e dei servizi XML (eXtensible Markup Language) fruibili per mezzo dell'infrastruttura di trasporto dedicata e delle porte applicative (di AdT e dell'Ente).

Infrastruttura di trasporto dedicata: E' l'insieme di elementi fisici (cavi di rete per il trasporto dati, server, router) strutturati in modo che possano offrire particolari servizi di trasporto (caratterizzati, ad esempio, da elevati livelli di sicurezza, affidabilità, disponibilità).

Servizi esposti (AdT): E' l'insieme dei servizi XML messi a disposizione, dall'Agenzia del Territorio agli Enti, finalizzati alla fruizione delle informazioni proprie del Sistema Informativo AdT.

Servizi esposti (Ente della P.A.): E' l'insieme dei servizi XML messi a disposizione, dall'Ente ad altri Enti della Pa, fra i quali l'Agenzia del Territorio, finalizzati alla fruizione delle informazioni proprie del Sistema Informativo Ente della PA.

Servizi XML: Sono le applicazioni software (web services) progettate per supportare la comunicazione e cooperazione automatica (interoperabilità) fra diversi elaboratori su una medesima infrastruttura di trasporto dedicata. Offrono funzionalità che permettono ad altri sistemi (software) di interagire, in maniera automatica.

I dati catastali sono integrati nel database e nei servizi applicativi del SIT e sono accessibili, oltre che con i servizi Sigmaster anche attraverso i servizi di consultazione avanzata.

Sportello Unico per l'Edilizia

E' un'applicazione di workflow che governa in maniera agevole e unitaria il ciclo di vita dei procedimenti necessari alla creazione, gestione e controllo delle pratiche riguardanti l'Ufficio Tecnico.

L'applicazione consente di governare il ciclo di vita dei procedimenti, continuando ad utilizzare in modo sinergico le applicazioni di protocollo informatico e gestione degli atti amministrativi dell'Ente.

Tramite il Front-office dell'applicazione, i cittadini e le imprese possono acquisire informazioni sulla pratica da istruire, utilizzare la modulistica, inoltrare il procedimento online e monitorare il suo stato di avanzamento.

Il Back-office applicativo, dal canto suo, provvede alla gestione dei procedimenti integrando il lavoro dei diversi operatori, dei responsabili e degli enti esterni coinvolti.

La gestione degli organi Deliberanti consente la gestione delle sedute della Commissione edilizia.

L'applicazione consente la massima flessibilità nella progettazione degli Iter che si vogliono adottare. Consente inoltre di progettare i singoli elementi procedurali (workstep) e successivamente di aggregarli a piacere in un Iter. Ciascun workstep rappresenta un passo che la pratica compie all'interno del suo iter, tutti i worksteps sono monitorati e ordinati in base al flusso generato dal motore di workflow.

Sono previste due modalità di gestione delle pratiche di Sportello Unico per l'Edilizia destinate, nella logica applicativa, a due tipologie di utenti diversi:

1. gestione verticale (sulla base di quanto definito nel disegno del work flow). Avviene tramite una comoda To Do List che propone agli utenti abilitati le fasi di lavorazione della pratica definite nell'iter amministrativo al momento esatto in cui devono essere espletate
2. gestione orizzontale (indipendentemente dal work flow) permette di gestire la proposta indipendentemente dall'ordine cronologico delle fasi di lavorazione previste dall'iter amministrativo. Consente altresì di gestire una serie di funzionalità naturalmente trasversali, quali:
 - a. il controllo dello stato dell'iter
 - b. il collegamento tra pratiche
 - c. le non conformità rispetto all'iter

Si riportano di seguito le principali funzionalità delle tre componenti:

- gestione della componente di sportello
- gestione delle attività di back office
- gestione degli Organi deliberanti

Il SUE è sviluppato con tecnologia Web.

Funzionalità di Front Office

Tramite il Front-Office dell'applicazione, i cittadini e le imprese possono acquisire una serie di informazioni, alcune a carattere generale, altre specifiche, per la pratica presentata o da presentare. Tutte le informazioni e i dati che possono essere visualizzati e/o gestiti dal Front-Office sono aggiornati, in modo dinamico, dalla componente Back_Office.

Principali funzioni di front-office

Area informativa generale	Elenca tutte le competenze della struttura
Informazioni generali su istanze	l'utente può estrapolare informazioni di carattere generale, sulle istanze e sui procedimenti amministrativi attivabili presso la struttura
Scelta del procedimento	l'utente può individuare il procedimento che intende attivare ed essere quindi guidato lungo tutto l'iter
Consultazione normativa	possibilità di visionare la normativa presente, secondo la struttura decisa dalla struttura, correlata ai procedimenti amministrativi (es: normativa comunitaria, nazionale, regionale, provinciale, locale etc.)
Consultazione modulistica	l'utente può visionare e stampare la modulistica standard relativa ai procedimenti attivabili. Viene inoltre fornito supporto all'autocompilazione on-line della modulistica.
FAQ	mette a disposizione le risposte alle domande più frequenti o di interesse comune
NEWS	in evidenza avvisi e notizie di carattere generale che si desidera portare a conoscenza degli utenti

LINKS	contiene i collegamenti ipertestuali a pagine web di particolare interesse, quali ad esempio Enti terzi che possono fornire informazioni utili su materie o argomenti trattati dalla struttura
Area Registri	contiene l'esito dei procedimenti amministrativi ordinati per anno e mese
Notifica via E-Mail	è possibile notificare al richiedente, via e-mail, il passaggio di avanzamento (iter) di una pratica
Oneri e Pagamenti	calcolo degli oneri e dei pagamenti, con possibilità, da parte del cittadino/impresa di visualizzare la propria posizione e ottenere il necessario supporto alla sua regolarizzazione con servizi di pagamento on-line
Enti terzi coinvolti	possono svolgere le attività loro richieste in riferimento alle fasi procedurali a loro carico (esempio: emissione di pareri, nulla osta, attestazioni di conformità etc.)

La tabella che segue riporta le informazioni minime che si prevede di rendere accessibili a tutti.

Tipologia Informazione Richiesta	Dettaglio Informazione Richiesta	
definizione dell'intervento (ai sensi dell'art.3 del D.P.R. 380/2001 - Testo Unico in materia Edilizia – e ss.mm.ii.)	Da selezionare tra le seguenti definizioni:	
	A	<i>interventi di manutenzione ordinaria (comma a)</i>
	B	<i>interventi di manutenzione straordinaria (comma b)</i>
	C	<i>interventi di restauro e di risanamento conservativo (comma c)</i>
	D	<i>interventi di ristrutturazione edilizia (comma d)</i>
	E1	<i>interventi di nuova costruzione (comma e1)</i>
	E2	<i>interventi di nuova costruzione (comma e2)</i>
	E3	<i>interventi di nuova costruzione (comma e3)</i>
	E4	<i>interventi di nuova costruzione (comma e4)</i>
	E5	<i>interventi di nuova costruzione (comma e5)</i>
	E6	<i>interventi di nuova costruzione (comma e6)</i>
E7	<i>interventi di nuova costruzione (comma e7)</i>	
F	<i>interventi di ristrutturazione urbanistica (comma f)</i>	
data inizio lavori	testo	
data fine lavori	testo	
specifica se la data di fine lavori è reale o presunta	Da selezionare tra:	
	0	<i>presunta</i>
	1	<i>reale</i>
localizzazione catastale- Numero Foglio	alfanumerico	
localizzazione catastale- Numero Particella	alfanumerico	

localizzazione catastale- Numero Subalterni	alfanumerico	
indirizzo (via, numero civico, interno e piano)	testuale	
progettista	testuale	
esecutore	testuale	
direttore lavori	testuale	
breve descrizione	testuale	
numero protocollo pratica	alfanumerico	
anno protocollo pratica	numerico	
richiedente	testuale	
tipo pratica (ai sensi dell'art.3 del D.P.R. 380/2001 - Testo Unico in materia Edilizia – e ss.mm.ii.)	Da selezionare tra:	
	01	<i>permesso di costruire (artt. 10 -21)</i>
	02	<i>dichiarazione di inizio attività (artt. 22 -23)</i>
	03	<i>certificato di agibilità (artt. 24 -26)</i>
	o04	<i>altro</i>
descrizione tipo pratica "altro"	testuale	
specifica se la pratica è "in sanatoria"	Da selezionare tra:	
	0	<i>falso</i>
	1	<i>vero</i>
specifica se la pratica è "in deroga agli strumenti urbanistici"	Da selezionare tra:	
	0	<i>falso</i>
	1	<i>vero</i>
stato dell'iter della pratica	testuale	
funzionario che segue la pratica	testuale	

Funzionalità di Back Office

Il Back-Office applicativo provvede alla gestione dei procedimenti amministrativi integrando il lavoro dei diversi operatori, dei responsabili e degli enti esterni coinvolti.

Le principali funzionalità presenti all'interno della componente Back-Office sono di seguito descritte.

Le principali fasi che la procedura di gestione dello Sportello Unico per l'Edilizia permette di rappresentare e supportare sono le seguenti:

a) Gestione della pratica

Questa attività viene svolta dagli operatori incaricati della presa in carico della domanda presentata dal cittadino.

Le principali fasi sono le seguenti:

- classificazione dell'iter con l'individuazione degli elementi caratteristici
- gestione delle persone fisiche e giuridiche a qualunque titolo collegate alla proposta
- gestione della documentazione, sia cartacea che in formato elettronico, da allegare alla proposta

- gestione dell'Oggetto Territoriale
- gestione dei pareri di Enti terzi coinvolti nel procedimento amministrativo:
 - richiesta di parere
 - registrazione dell'esito del parere richiesto

b) Assegnazione all'Organo Deliberante competente

Questa fase permette la gestione della Conferenza dei Servizi e, qualora previsto, di altre tipologie di Organi Deliberanti.

c) Provvedimento

Questa fase consiste nell'emissione del provvedimento autorizzatorio da parte dell'Ente, con l'attribuzione di una numerazione formale alla pratica, definita per tipologia di pratica e anno di riferimento

d) Gestione diritti di segreteria

Questa fase permette, a seguito dell'emissione del provvedimento autorizzatorio, all'Ente di definire tipologia ed ammontare degli oneri da addebitare al cittadino/impresa.

Consente inoltre di gestire i pagamenti attraverso la registrazione ed emissione di una ricevuta di quietanza.

Principali funzioni di back-office

Modelizzazione dei processi	tramite un WorkFlow integrato è possibile definire graficamente il percorso autorizzatorio dei procedimenti intesi come macroprocedimenti, endoprocedimenti o sottoprocedimenti. E' possibile inoltre impostare le regole associate ad ogni passaggio di stato - dall'avvio sino alla conclusione attraverso tutti i passi intermedi. E' prevista la possibilità, in corrispondenza di ogni fase di workflow, di inviare una comunicazione a mezzo e-mail, parametrizzandola secondo le esigenze dell'Ufficio, indirizzata sia ad utenti interni che a cittadini/utenti esterni.
Template delle fasi di processo	catalogo di modelli delle fasi; combinati fra di loro, detti modelli andranno a costituire e/o variare i processi associati alle istanze
ToDo List	Politiche di push e pull nella formazione delle liste delle attività, ToDo List. gli utenti abilitati prendono in carico, o riassegnano, le attività durante lo sviluppo dell'iter procedimentale
Monitoraggio dei tempi	sistema di controllo dei tempi di ogni attività, con produzione automatica di preavvisi, allarmi e solleciti
Reporting	produzione automatica di elaborati parametrici di dettaglio, consultabili sia su terminale video che su supporto cartaceo
Profili utente	blocco di funzionalità che consentono di abilitare/disabilitare/controllare i diversi livelli di accesso alle funzionalità dell'applicativo (Back Office)
Pubblicazione dati	Manutenzione Aree News, FAQ e Link aggiornamento dinamico da Back Office per la loro pubblicazione su Front-Office
Allegati multiformato	permette di accludere alla pratica documenti in formato elettronico quali .xls, .pdf, .doc, .txt, .rtf e così via
Rilascio ricevute	a fronte della domanda presentata, il sistema rilascia una ricevuta e una quietanza in unica soluzione
Gestione archivi di base	Settori merceologici (permette di definire i settori merceologici a cui sono riferiti i procedimenti gestiti) Albi professionali (definisce gli albi professionali a cui possono essere collegati i professionisti che operano sui procedimenti) Enti (vengono codificati tutti gli Enti che possono essere coinvolti nella gestione dei procedimenti) Tipi di onere (è possibile codificare le varie tipologie di onere collegati alle varie tipologie di procedimento) Tipi di referenze (permette la codifica delle possibili referenze che verranno utilizzate per stabilire a quale titolo ogni

	<p>nominativo è collegato ad un procedimento)</p> <p>Codici Istat (la tabella contiene i codici Istat a cui si possono essere riferiti i procedimenti)</p> <p>Tipi di stampa (permette di definire le stampe che possono essere utilizzate in gestione dei procedimenti. Ad ogni tipologia di stampa corrisponde un modello .rtf)</p> <p>Allegati (è possibile codificare tutti i documenti, allegati o i loro sostituti che dovranno essere abbinati ai procedimenti)</p> <p>Pareri (permette la codifica dei pareri che possono essere richiesti ai vari Enti coinvolti nella gestione dei processi. Ad ogni tipologia di parere corrisponde il testo della richiesta da inviare all'Ente)</p> <p>Moduli (permette di definire e codificare i modelli di domanda. Ad ogni modulo possono essere inoltre abbinati gli allegati precedentemente codificati nell'apposita tabella)</p> <p>Tipi di procedimento (permette di creare le tipologie di procedimento che si intendono utilizzare. Ogni tipologia di procedimento è riferita ad una categoria merceologica e ad ogni tipologia di procedimento sono collegati il modulo della domanda ed il processo di workflow precedentemente istanziato. Ad ogni tipologia di procedimento sono collegati inoltre gli Enti coinvolti con i relativi pareri, gli allegati ed i modelli di stampa)</p> <p>Tipi di pratica (permette di definire le tipologie di pratica. Ad ogni tipologia di pratica corrisponde una tipologia di procedimento)</p> <p>Tipi di provvedimento (definisce le tipologie dei provvedimenti che potranno essere collegate ai procedimenti)</p> <p>Tariffario oneri di urbanizzazione differenziato per tipi di intervento, destinazioni d'uso</p>
Referenti	Permette la codifica o la ricerca dei dati anagrafici relativi alle persone fisiche e giuridiche che abbiano un qualche riferimento con il procedimento. Oltre ai dati anagrafici è possibile abbinare ad ogni referente anche gli indirizzi ed il titolo di referenza. La funzione prevede la possibilità di gestire eventuali volturazioni riferite alle persone precedentemente collegate
Allegati	Permette di visualizzare l'elenco degli allegati abbinati al procedimento. Per ogni allegato può essere indicato il numero di protocollo e la data di presa in carico. Per ogni procedimento può essere modificato l'elenco proposto aggiungendo nuovi allegati o eliminando allegati presenti nell'elenco
Oggetti Territoriali	Permette di gestire il riferimento dell'insediamento al territorio. Per ogni oggetto territoriale sono gestiti i dati relativi agli indirizzi, ai dati catastali, a persone fisiche e giuridiche
Oneri	Vengono indicati gli oneri richiesti per il singolo procedimento. E' possibile gestire più pagamenti e per ogni pagamento è possibile stampare la relativa ricevuta di quietanza
Enti coinvolti	La funzione permette di inviare agli Enti coinvolti sul singolo procedimento la richiesta di pareri. L'elenco degli Enti proposto è quello definito nella tabella di definizione dei procedimenti. In questa sede è comunque possibile eseguire variazioni coinvolgendo più o meno Enti rispetto a quanto proposto.
Numerazione	La funzione permette di numerare ogni singolo provvedimento abbinato al

dell'Atto	procedimento. Il sistema può gestire più registri, uno per ogni tipologia di provvedimento codificato
Visualizzazione stato dell'iter	La funzione permette di visualizzare lo stato avanzamento della pratica. All'operatore che esegue la funzione viene proposta una videata contenente l'elenco delle fasi del workflow. Per ogni fase viene indicato l'operatore che ha in carico la fase e lo stato della fase stessa
Stampe parametriche	La funzione permette di eseguire le stampe partendo dal modello precedentemente predisposto. Durante la fase di stampa la funzione inserisce nel modello i dati del procedimento prelevandoli dall'archivio
Verifiche tecniche	La funzione permette la gestione dei dati tecnici relativi alla singola pratica per il confronto con i parametri impostati a livello centrale
Definizione del contenuto dei regolamenti	La funzione permette la definizione del contenuto dei regolamenti che governano i procedimenti amministrativi
Calcolo degli oneri	La funzione permette la gestione del calcolo di eventuali oneri a carico di cittadini / imprese richiedenti. Gli oneri possono essere calcolati o tramite una procedura di calcolo esterna (in tal caso riportando manualmente i dati nell'iter per proseguire con la gestione del procedimento) oppure con la gestione automatizzata del calcolo (tale modalità utilizza un foglio di calcolo, formato .xls, associato alla relativa pratica e visualizzabile e personalizzabile dall'operatore in qualsiasi momento)
Gestione degli oneri	La funzione permette la gestione degli oneri (rateizzazione e riscossione) calcolati come descritto in precedenza
Gestione delle garanzie	La funzione permette all'operatore di inserire per ogni pratica, qualora necessario, i dati relativi alle garanzie prestate dal cittadino/impresa per il pagamento degli oneri, nonché associare i relativi documenti in formato elettronico
Chiusura della pratica	La funzione di chiusura della pratica permette di chiudere il procedimento e rendere tutte le fasi ed i dati abbinati al procedimento non più modificabili e solamente consultabili.
Conferenza dei Servizi	La funzione consente di gestire la Conferenza dei Servizi o altre Commissioni il cui parere sia richiesto per l'espletamento del procedimento. L'esito espresso dalla Conferenza dei Servizi o da altra Commissione può essere consultato direttamente dalla gestione del procedimento senza dover accedere alla seduta nella quale l'esito è stato espresso. Le funzionalità relative alla gestione della conferenza dei servizi sono descritte nel paragrafo relativo alla gestione degli Organi Deliberanti.

Organi deliberanti

E' un'applicazione con interfaccia web ideata appositamente per gestire le varie fasi di lavorazione delle commissioni coinvolte nell'iter di una pratica.

Di seguito vengono descritte le principali funzionalità a disposizione dell'utente relative alle diverse Fasi Operative:

- Gestione Commissione
- Gestione Seduta
- Tabelle
- Documentazione

L'applicazione consente di gestire le procedure di esame ed approvazione di atti amministrativi da parte di uno o più soggetti quali Conferenza dei Servizi, Commissione Edilizia e così via.

GESTIONE ORGANI DELIBERANTI	Funzionalità
Gestione delle tipologie degli organi deliberanti	Consente di definire le tipologie di organo deliberante, indicare i componenti e quali sono i ruoli per ogni singolo componente
Gestione commissione	Devono essere inseriti: <ol style="list-style-type: none"> 1. Codice univoco di identificazione della Commissione 2. Descrizione commissione 3. Data inizio (data di insediamento commissione) Oltre alle suddette informazioni, può essere aggiunta anche la data di fine mandato della commissione. <i>principali funzionalità</i> <ul style="list-style-type: none"> • Modifica: consente di modificare i dati di una commissione • Elimina: consente di eliminare una commissione • Gestione Componenti: è possibile gestire gli elenchi delle persone inserite nelle commissioni di riferimento; è possibile inserire un nuovo nominativo prelevandolo dall'archivio anagrafico oppure, qualora il nominativo non sia presente nelle anagrafiche, inserendolo ex-novo, eliminare un nominativo, ordinare l'elenco dei nominativi inseriti in una commissione, identificare il presidente e il segretario di seduta.
Gestione seduta	Consente l'accesso a tutte le funzionalità coinvolte nella fase di gestione di una seduta della commissione: <ul style="list-style-type: none"> • creare ordini del giorno associandovi le pratiche che verranno discusse, • gestire le presenze • gestire le votazioni • aggiungere una nuova seduta • associare alla seduta anche uno stato (per es: aperta, chiusa, sospesa...) • eliminare una seduta: consente la cancellazione della seduta selezionata

	<ul style="list-style-type: none"> • Gestire l'Ordine del Giorno: associare gli atti ad una seduta, stampare la lettera di convocazione, aggiornare i componenti della seduta, determinare il criterio di ordinamento degli atti all'interno dell'ordine del giorno e inserire eventuali note (per es: aggiunta di possibili emendamenti). • Stampare utilizzando i modelli associati alla commissione. • Inserire esito discussione per ogni atto • Gestire votazione e presenze per singolo atto • Componenti: rende possibile l'inserimento di nuovi componenti nell'elenco dei partecipanti ad una seduta. Qualora tali componenti non siano compresi nell'elenco associato precedentemente alla commissione si possono aggiungere con gli stessi criteri già descritti nella fase di gestione componenti. Oltre a ciò, l'operatore avrà la possibilità di effettuare l'aggiornamento delle presenze, ovvero stabilire a livello di singola seduta chi è presente o assente al primo appello e durante la discussione delle singole pratiche. • Chiusura pratica
Definizione modelli	<p>Consente di definire modelli di stampa ad hoc per ciascuna commissione gestita all'interno dell'applicazione.</p> <p>Le tipologie di stampa configurabili sono:</p> <ul style="list-style-type: none"> • Convocazione • Ordine del Giorno • Verbale <p>Selezionata la voce di menu, si accede alla maschera di gestione stampe, nella quale sono elencate le varie commissioni e i modelli ad esse associati.</p>
Gestione tabelle	<p>Comprende 4 sottovoci ognuna delle quali consente la gestione di una particolare tabella i cui dati vengono poi richiamati durante le varie fasi di lavorazione della pratica.</p>

ALLEGATO 1

**Ontologia dell'Indice della Pubblica Amministrazione (IPA) e
Servizi Documentali**



**Progetto interregionale ICAR
“Interoperabilità e Cooperazione Applicativa tra le
Regioni”**

<Task AP3>

AP3- Ontologia

Versione <1.2>

STATO DELLE VARIAZIONI

versione	PARAGRAFO O PAGINA	DESCRIZIONE DELLA VARIAZIONE
V 1.0	Tutto il documento	Versione iniziale del documento
V 1.1	Tutto il documento	Revisione completa con aggiunta di paragrafi
V 1.2	Tutto il documento	Revisione completa con dettaglio ontologia servizi documentali

INDICE

1. SCOPO E RIFERIMENTI DEL DOCUMENTO.....	674
1.1 SCOPO DEL DOCUMENTO	674
1.2 RIFERIMENTI.....	674
2. METODOLOGIA PROPOSTA	675
2.1 SEMANTICA DI DOMINIO	675
2.2 SEMANTICA DEI SERVIZI	676
3. INDICE DELLA PUBBLICA AMMINISTRAZIONE.....	678
3.1 QUADRO D'INSIEME	678
3.2 ANALISI DI DOMINIO	678
3.3 SEMANTICA DI RIFERIMENTO	679
3.3.1 <i>Semantica di dominio</i>	680
3.3.2 <i>Semantica dei servizi</i>	680
4. SERVIZI DOCUMENTALI	683
4.1 QUADRO D'INSIEME	683
4.2 ANALISI DI DOMINIO	683
4.3 SEMANTICA DI RIFERIMENTO	684
4.3.1 <i>Semantica di dominio</i>	685
4.3.2 <i>Semantica dei servizi</i>	688
5. CLASSI DI SERVIZIO INDIVIDUATE.....	687
5.1 SERVIZIO INDICE.....	687
5.2 SERVIZIO ARCHIVIO	688

1.Scopo e riferimenti del documento

1.1Scopo del documento

Questo documento illustra la proposta di ontologia definita nell'ambito del task AP3 sui temi Indice della Pubblica Amministrazione (IPA) e Servizi Documentali.

Il documento è rivolto alle Regioni partecipanti.

Il documento si articola nelle seguenti sezioni:

- *Metodologia proposta*: descrive ad alto livello la proposta metodologia per l'annotazione dell'accordo di servizio proposta nel contesto del progetto ICAR.
- *Indice della Pubblica Amministrazione*: illustra la proposta di ontologia per il dominio di cooperazione applicativa dell'Indice della Pubblica Amministrazione
- *Servizi Documentali*: illustra la proposta di ontologia per il dominio di cooperazione applicativa dei Servizi Documentali.
- *Classi di servizio individuate*: raccoglie le ontologie delle classi di servizio individuate nel contesto del dominio di cooperazione.

1.2Riferimenti

- *Progetto Esecutivo del task AP3: ICAR-AP3-ver01.doc*
- *Proposta di metodologia per l'annotazione semantica di accordi di servizio: ICAR-AnnotazioneSemanticaADS-ver1.0.pdf*

2. Metodologia proposta

Nell'ambito dell'interoperabilità e della cooperazione applicativa la semantica è lo strumento che garantisce la possibilità che sistemi informativi distribuiti, basati su differenti concetti associati alle informazioni scambiate, possano collaborare in modo automatico anche se sono stati progettati in modo indipendente. L'obiettivo è di fare in modo che le fonti informative siano in rete e che l'informazione scambiata sia automaticamente comprensibile e utilizzabile da applicazioni non coinvolte nella loro creazione. In sintesi serve per dare un significato preciso al flusso informativo scambiato tra due sistemi consentendo di risolvere eventuali ambiguità interpretative e per individuare corrispondenze e differenze fra concetti in domini diversi.

Una modalità per definire il layer semantico nel contesto della cooperazione applicativa è quella di introdurre delle annotazioni semantiche nell'accordo di servizio. La definizione del layer semantico prevede che a ogni singolo dominio amministrativo sia responsabile di definire una propria ontologia quanto meno delle informazioni e dei servizi erogati in cooperazione applicativa. A livello metodologico si propone di arricchire l'accordo di servizio con gli opportuni riferimenti semantici ai concetti espressi nell'ontologia di riferimento tramite delle annotazioni insistenti sulla parte comune dello stesso.

La metodologia proposta propone un processo di definizione del layer semantico associato ad un dominio di cooperazione organizzato in tre fasi:

- 1) definizione dell'accordo di servizio
- 2) definizione dell'ontologia del dominio erogatore
- 3) annotazione dell'accordo di servizio rispetto all'ontologia di dominio erogatore

La definizione dell'accordo di servizio rappresenta di fatto la definizione del dominio di cooperazione applicativa. Questa fase permette di individuare il modello dati, gli oggetti, le operazioni e l'insieme di servizi che costituiscono insieme il dominio di cooperazione applicativa.

La definizione della semantica del dominio di cooperazione permette di catalogare e strutturare l'insieme dei riferimenti che sono utilizzati nel contesto del dominio di cooperazione applicativa. La semantica del dominio erogatore viene definita analizzando il dominio di cooperazione rispetto a diverse viste ortogonali; in particolare per ora il lavoro fatto a livello della definizione della metodologia si è concentrato nella definizione della *ontologia dei dati* e della *ontologia dei servizi*.

L'annotazione degli elementi contenuti nell'accordo di servizio consente di legare elementi concreti con concetti semantici. Di fatto è lo strumento che permette di definire l'interpretazione autentica del dominio di cooperazione applicativa.

2.1 Semantica di dominio

La semantica di dominio identifica i concetti principali che caratterizzano il dominio di cooperazione applicativa.

In questo senso gli obiettivi della semantica di dominio si possono riassumere in:

1. formalizzazione dei concetti, e delle relazioni tra essi, associati ai dati scambiati tra erogatore e fruitore dei servizi erogati in cooperazione applicativa
2. formalizzazione dei concetti del dominio rilevanti per la cooperazione applicativa

Supponiamo ad esempio che si voglia descrivere la semantica di dominio associata ad un servizio di indice che agisce sull'insieme dei soggetti pubblici. Aggiungiamo inoltre che il servizio di indice definito possa essere fruito solo dai funzionari degli enti della pubblica amministrazione centrale (PAC).

Come risultato avremo un'**ontologia di dominio** che, per quanto concerne il primo punto, formalizza e descrive il concetto di *soggetto pubblico*, mentre, per quanto concerne il secondo punto, formalizza e descrive i concetti di *funzionario pubblico* e *pubblica amministrazione centrale*.

Operativamente l'analisi viene fatta considerando sia gli aspetti contenuti nella documentazione di descrizione di alto livello del dominio che gli XSD Schema del data model utilizzato nel contesto dell'accordo di servizio.

2.2 Semantica dei servizi

La semantica dei servizi permette di categorizzare l'insieme dei servizi del dominio erogati in cooperazione applicativa. Nella categorizzazione è importante:

- classificare il servizio rispetto ad una o più classi di servizio generiche
- esplicitare le relazioni tra il servizio stesso ed i concetti individuati nell'ontologia di dominio.

La semantica dei servizi si appoggia su tre livelli descrittivi:

- il primo livello definisce la semantica dell'accordo di servizio ICAR /SPCoop
- il secondo livello definisce un insieme di classi di servizio generiche legate alla nozione di servizio definita al livello precedente
- infine il terzo livello, quello applicativo, definisce il servizio specifico che istanza di una classe di servizio generico.

Ad ogni livello corrisponde un'ontologia specifica:

- ontologia dell'accordo di servizio
- ontologia dei servizi generici
- ontologia del servizio specifico

L'ontologia dell'accordo di servizio definisce uno schema concettuale esaustivo e rigoroso dello stesso. Nell'ontologia sono descritti concetti quali servizio, operazione, ruolo, credenziale, evento e quality of service e le relazioni, le regole, gli assiomi ed i vincoli tra essi.

L'ontologia dei servizi generici modella a livello concettuale delle classi di servizio che sono di per sé caratteristiche dell'ambito di collaborazione. Nell'ambito dei sistemi informativi della pubblica amministrazione e soprattutto nel contesto dei domini di cooperazione applicativa un esempio evidente di classe di servizi è il servizio di indice.

L'ontologia dei servizi specifici modella a livello concettuale i servizi erogati in cooperazione applicativa da uno specifico dominio esplicitando le classi di servizio di appartenenza ed il legame con il modello dati. In particolare, i servizi specifici erogati sono istanziati rispetto alle classi di servizio generiche che meglio descrivono le funzionalità degli stessi ed inoltre vengono esplicitate le relazioni tra i servizi specifici e l'ontologia di dominio (ontologia dei dati) di riferimento.

3.Indice della Pubblica Amministrazione

In questa sezione è presentata la proposta di ontologia www.lego-lab.org/icar/ipa.owl relativa al dominio di cooperazione dell'Indice della Pubblica Amministrazione (IPA).

Nel contesto di sotto sezioni specifiche sono presentati:

- *quadro d'insieme*: descrive il contesto di riferimento della IPA
- *analisi di dominio*: propone il modello del dominio di cooperazione applicativa dell'IPA risultante dall'attività di analisi
- *semantica di riferimento*: illustra la proposta di *semantica* per il dominio di cooperazione applicativa dell'IPA

3.1Quadro d'insieme

L'Indice delle amministrazioni pubbliche e delle Aree Organizzative Omogenee (IndicePA o iPA) è stato istituito con il DPCM del 31 ottobre 2000, recante le regole tecniche per il protocollo informatico nella pubblica amministrazione.

Attraverso l'IndicePA ogni amministrazione espone la struttura dei propri uffici e l'elenco dei servizi offerti, con le informazioni per il loro utilizzo e gli indirizzi di posta elettronica da impiegare per comunicazioni e per lo scambio di documenti e informazioni, anche ufficiali e a valore legale.

Il CNIPA ne gestisce l'infrastruttura e la relativa evoluzione tecnologica. Il costante aggiornamento dei contenuti è condizione indispensabile per incrementare e migliorare i canali di comunicazione telematica tra le amministrazioni e tra esse e i cittadini e le imprese. Le informazioni contenute nell'indice son altresì prerequisito essenziale per gli obiettivi di trasparenza e di modernizzazione della PA.

L'IndicePA fornisce supporto all'interoperabilità dei sistemi di protocollo informatico delle amministrazioni pubbliche e costituisce un punto di riferimento per l'individuazione e l'accesso alle strutture organizzative ed ai servizi telematici offerti dalla Pubblica Amministrazione centrale e locale.

Le informazioni pubblicate dalle amministrazioni pubbliche sull'IndicePA sono accessibili attraverso il sito www.indicepa.gov.it.

3.2Analisi di dominio

Nel contesto IPA l'obiettivo di progetto del task applicativo AP3 è quello di definire il formato e gli eventi di comunicazione delle variazioni organizzative promosse dalle varie amministrazioni verso l'Indice della Pubblica Amministrazione mantenuto dal CNIPA.

Da un punto di vista informativo, l'IPA può essere considerato composto di due indici logici distinti:

1. l'indice delle unità organizzative (IUO), contenente le informazioni relative la struttura organizzativa delle amministrazioni accreditate presso l'indice;
2. l'indice delle Aree Organizzative Omogenee (IAOO), organizzato per amministrazioni e contenente le informazioni sulla composizione delle relative AOO.

L'IUO descrive la struttura organizzativa di ciascuna amministrazione in termini di unità organizzative e della relativa struttura gerarchica. Esso contiene, per ciascuna unità organizzativa, le informazioni riguardanti la sede o le sedi e la loro denominazione ed indirizzo postale, unitamente alle modalità di accesso telematico ad eventuali servizi applicativi on-line resi disponibili e gli indirizzi delle caselle di posta elettronica, eventualmente afferenti ad un sistema di Posta Elettronica Certificata.

L'IAOO contiene la descrizione dei dati tecnici e di tutte le informazioni rilevanti che caratterizzano l'accesso telematico ad ogni AOO e, in particolare, per lo scambio di messaggi di posta elettronica verso le relative caselle di posta istituzionali, afferenti ad un sistema di Posta Elettronica Certificata. In esso le AOO sono organizzate in base alle amministrazioni di appartenenza e contengono l'indicazione delle unità organizzative utenti per le quali sono riferimento, descrivendo, di fatto, una partizione dell'insieme delle UO dell'amministrazione.

Oltre al formato di comunicazione delle variazioni intercorse di tipo XML vengono individuati anche gli eventi significativi per il processo di aggiornamento dell'indice.

- Inserimento di una nuova Area Organizzativa Omogenea
- Modifica/eliminazione di una Area Organizzativa Omogenea
- Inserimento di un nuovo Ufficio/Unità Organizzativa
- Modifica/eliminazione di un Ufficio/Unità Organizzativa

3.3 Semantica di riferimento

Come sottolineato nel contesto del documento, andremo a dettagliare la semantica di riferimento del dominio di cooperazione applicativa articolandola nella *semantica di dominio* e nella *semantica dei servizi* in modo da descrivere in modo puntuale i concetti individuati e le relazioni tra essi.

Nella formalizzazione della semantica di riferimento è importante sottolineare che il dominio di cooperazione applicativa viene descritto dal punto di vista di una generica amministrazione. In questo senso è opportuno prima di tutto definire, quanto meno ad alto livello, i confini del dominio di cooperazione applicativa che si vuole formalizzare.

L'*amministrazione* è il soggetto demandato a mantenere un "archivio dei documenti" amministrativi che coinvolgono le diverse emanazioni dell'amministrazione stessa. Con *amministrazione* si intende un soggetto della pubblica amministrazione registrato nel contesto dell'IPA.

3.3.1 Semantica di dominio

Nel contesto della semantica di dominio gli aspetti che è interessante modellare sono quelli relativi al modello dati e quelli relativi agli attori che a diverso titolo giocano un ruolo nel contesto dell'erogazione o fruizione del servizio applicativo.

Come abbiamo visto uno degli obiettivi dell'Indice della Pubblica Amministrazione è quello di catturare la struttura organizzativa della PA. In Figura 1¹ viene mostrato come, nel contesto del dominio, la struttura organizzativa della pubblica amministrazione sia rappresentata in un grafo che organizza la stessa in *Amministrazioni*, *Unità Organizzative* (UO) ed in *Aree Organizzative Omogenee* (AOO). Le *Amministrazioni* di fatto sono delle *Unità Organizzative* di alto livello che hanno un'ampia autonomia organizzativa. La radice del grafo coincide con la *radice della PA* che individua il paese di riferimento (Italia). Gli attori coinvolti sono essenzialmente gli *Utenti dell'IPA* ed i *Responsabili dell'aggiornamento dell'IPA*. In questo senso ogni amministrazione è tenuta ad individuare un responsabile e uno o più utenti.

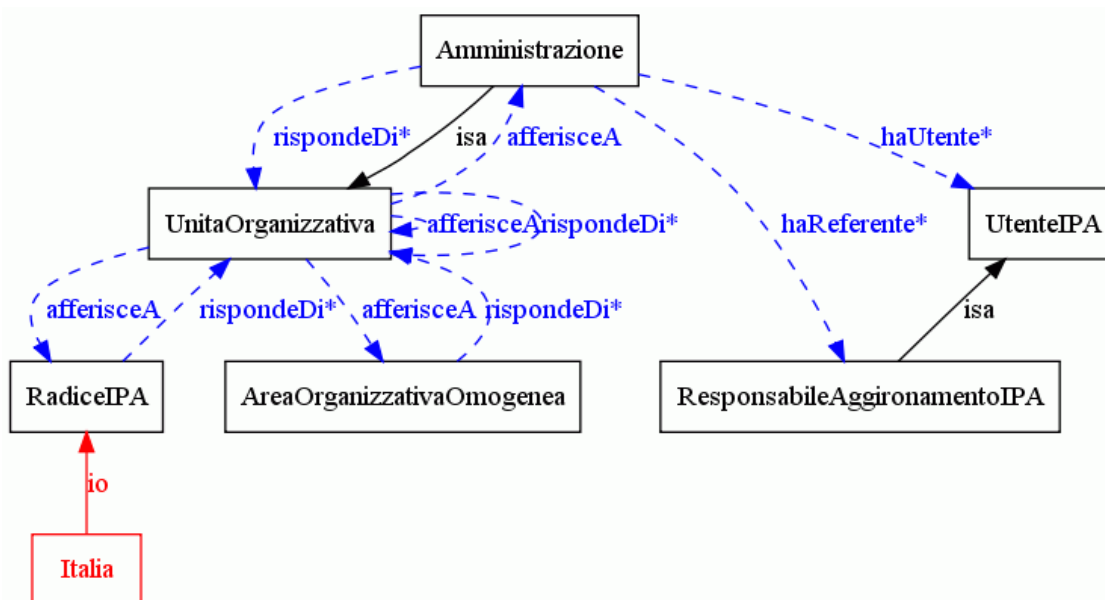


Figura 1: Dominio Indice della Pubblica Amministrazione

3.3.2 Semantica dei servizi

La semantica dei servizi si struttura su tre livelli: la *semantica dell'accordo di servizio*, la *semantica della classe di servizio* e l'*istanza del servizio specifico* del dominio di cooperazione.

¹ Nei diagrammi, i blocchi in nero rappresentano i concetti, i blocchi in rosso rappresentano gli individui afferenti ad un concetto, le righe blu rappresentano le relazioni tra concetti o tra individui.

Il dominio di riferimento fa capo alle classi di *Servizio Indice* descritte nella sezione “*Classi di servizio individuate*” di questo documento.

In particolare, come illustrato nella descrizione di alto livello e mostrato in Figura 2, il dominio di cooperazione applicativa eroga un *servizio indice IPA* che si compone dei due sotto servizi *indice UO* e *indice AOO*.

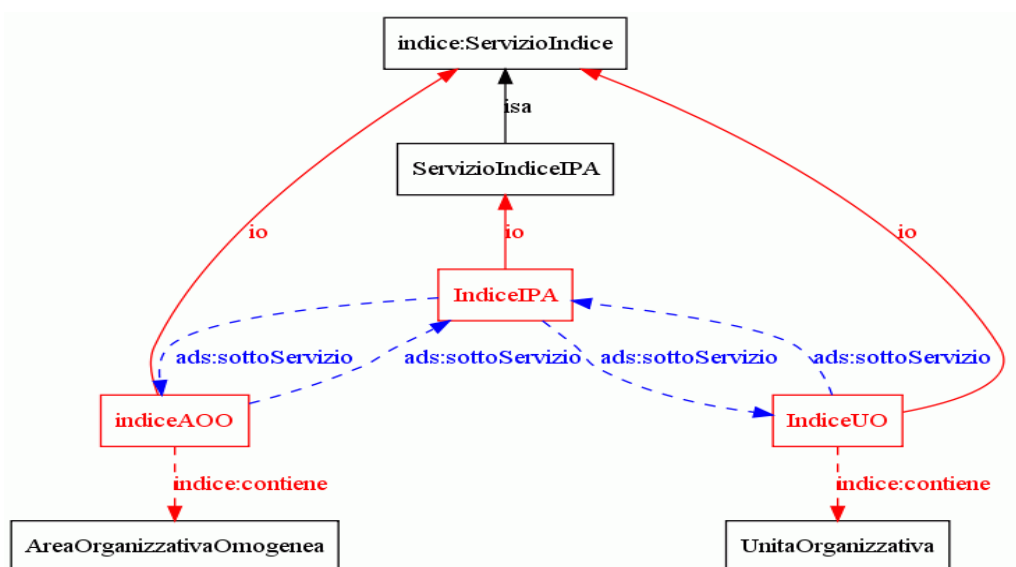


Figura 2: Semantica dei servizi

Oltre alle relazioni tra il servizio ed i sotto servizi, la figura riporta anche il fatto che il *servizio indice IPA* estende il concetto di generico *servizio indice*. Questo dipende dal fatto che dal punto di vista tecnico l'accesso alle operazioni esportate dai servizi *indice delle UO* e *indice delle AOO* viene effettuato tramite la chiamata ad operazioni del servizio *indice IPA* che di fatto media la fase di interazione.

Il dettaglio mostrato Figura 3 evidenzia che il *servizio indice delle AOO* permette di gestire l'inserimento, la cancellazione, la modifica, la notifica di eventuali variazioni e la consultazione delle informazioni relative alle Aree Organizzative Omogenee in cui sono strutturate le diverse amministrazioni pubbliche attraverso operazioni specifiche. Non definisce però alcun attore che sia in grado di eseguire queste operazioni in modo diretto proprio perché l'accesso a dette operazioni viene mediato dal servizio di più alto livello *indice IPA*.

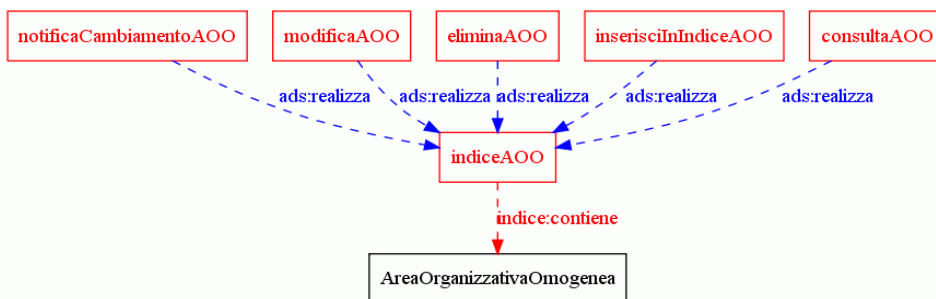


Figura 3: Servizio indice Aree Organizzative Omogenee

Come mostrato in Figura 4 la stessa cosa avviene per l'indice delle UO.

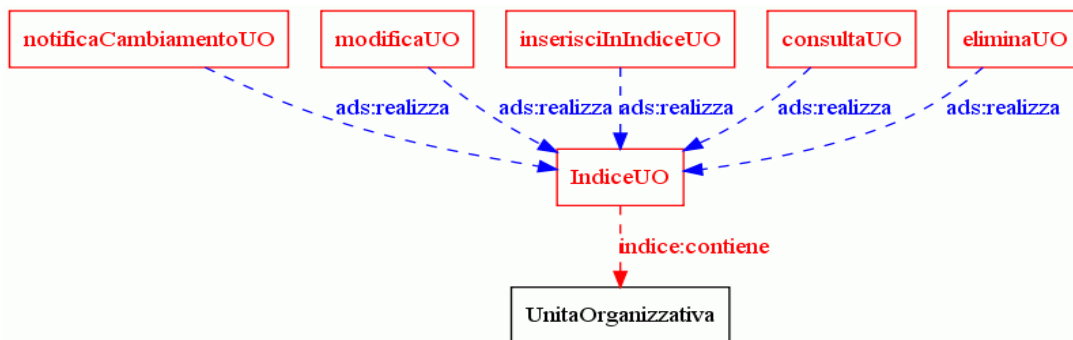


Figura 4: Servizio indice Unita Organizzative

Il servizio *indice IPA* viene illustrato in Figura 5. Come detto precedentemente il servizio indice IPA ha una funzione di mediazione e aggregazione rispetto all'esecuzione delle operazioni dei sotto servizi *indice UO* e *indice AOO*. Oltre a fungere da mediatore rispetto alle operazioni dei sotto servizi, il servizio *indice IPA* estende la classe di servizio *indice* mettendo a disposizione dei metodi che consentono la notifica dell'esito di una modifica, la richiesta di accreditamento di un'amministrazione ed infine la notifica della risultato della richiesta di accreditamento. I ruoli abilitati a eseguire le operazione di più alto livello sono *utente IPA* e *responsabile aggiornamento IPA*.

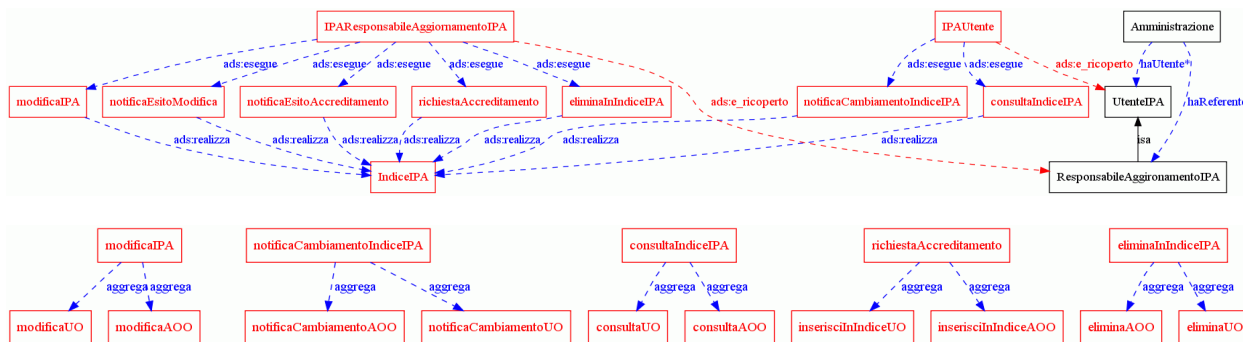


Figura 5: Servizio indice IPA

4. Servizi documentali

In questa sezione è presentata la proposta di ontologia www.lego-lab.org/icar/servizidocumentali.owl relativa al dominio di cooperazione dei servizi documentali.

Nel contesto di sotto sezioni specifiche sono presentati:

- *quadro d'insieme*: descrive il contesto di riferimento dei servizi documentali
- *analisi di dominio*: propone il modello del dominio di cooperazione applicativa dei servizi documentali risultante dall'attività di analisi
- *ontologia di riferimento*: illustra la proposta di ontologia per il dominio di cooperazione applicativa dei servizi documentali

4.1 Quadro d'insieme

Il contesto di riferimento è relativo alla possibilità di attivare, mediante cooperazione applicativa, l'accesso ai sistemi informativi di protocollo da parte delle pubbliche amministrazioni.

Questa esigenza deriva da un'inadempienza del quadro normativo il quale, con il DPR 445/2000 capo IV sezione seconda, rimanda a delle specifiche tecniche ed organizzative per l'accesso ai documenti ed alle informazioni del sistema di gestione dei documenti che ad oggi non risultano definite.

Più in dettaglio, le funzionalità necessarie in questo contesto riguardano la possibilità, per un'Amministrazione richiedente, di:

- visualizzare il contenuto di un fascicolo dell'Amministrazione interrogata
- visualizzare un documento informatico contenuto in un fascicolo dell'Amministrazione interrogata
- effettuare una ricerca sulle protocollazioni dell'Amministrazione interrogata.

4.2 Analisi di dominio

L'obiettivo del task AP3, nel contesto dei servizi documentali, è quello di predisporre dei servizi che permettano il reperimento dei documenti afferenti ad un determinato procedimento che coinvolge due amministrazioni.

Il sistema documentale identifica in modo preciso il concetto di *documento*. Un documento, specializzato in *documento informatico* e *documento cartaceo*, ha uno o più *destinatari*, un *mittente*, una *visibilità*. Destinatario e mittente, nel contesto che ci interessa, sono delle AOO presenti nel registro IPA (in generale questo non è detto). La *visibilità* rappresenta il fatto che il documento sia secretato (non visibile per le ricerche) o pubblico. Pubblico significa visibile ma con la restrizione di *visibilità limitata* alle AOO che compaiono come mittente/destinatario.

Esistono altri attributi propri del documento che sono o necessari per la gestione archivistica:

- la *segnatura* di un documento identifica univocamente un documento all'interno dell'ente (mittente o destinatario). Le informazioni minime previste sono:
 - il progressivo del protocollo
 - la data di protocollo
 - l'identificazione in forma sintetica dell'amministrazione o dell'area organizzativa.
- *oggetto* del documento
- *classifica*: la classificazione è un'operazione logica che permette di ricondurre il documento, in base all'oggetto trattato, a raggruppamenti di ordine generale indicati in un *titolario*

Un documento in generale viene associato ad un *fascicolo*: il fascicolo rappresenta un'aggregazione organizzata di documenti relativi ad un fatto concreto; ogni documento che appartiene ad un fascicolo, avrà l'identificativo del fascicolo (composto da classifica, anno, progressivo fascicolo) come attributo. Il *fascicolo* può essere *virtuale*, in tal caso il documento avrà come attributo la segnatura del primo documento che ha dato luogo all'apertura del fascicolo virtuale. Questo numero viene riportato su tutti i documenti successivi in arrivo e partenza: dal momento che su tutti i documenti è presente il riferimento al primo documento puntando ad esso è poi possibile risalire a tutti i documenti che fanno parte della catena ed avere così una visibilità pari a quella ottenuta interrogando i documenti che sono inseriti in un fascicolo aperto secondo i criteri archivistici classici. Anche il fascicolo la visibilità potrebbe poi essere estesa anche ad altri documenti dello stesso *fascicolo*.

Per quanto riguarda i servizi esportati, ogni amministrazione mette a disposizione delle funzionalità che permettano:

- interrogazione del contenuto di un fascicolo (a partire da una protocollazione)
- estrazione di un documento di un fascicolo
- ricerca generalizzata sulle protocollazioni di propria pertinenza.

4.3 Semantica di riferimento

Come sottolineato nel contesto del documento, andare a dettagliare l'ontologia di riferimento del dominio di cooperazione applicativa articolandola nella *semantica di dominio* e nella *semantica dei servizi* in modo da descrivere in modo puntuale i concetti individuati e le relazioni tra essi.

Nella formalizzazione della semantica di riferimento è importante sottolineare che il dominio di cooperazione applicativa viene descritto dal punto di vista di una generica amministrazione. In questo senso è opportuno prima di tutto definire quanto meno ad alto livello i confini del dominio di cooperazione applicativa che si vuole formalizzare.

L'amministrazione è il soggetto demandato a mantenere un "archivio dei documenti" amministrativi che coinvolgono le diverse emanazioni dell'amministrazione stessa. Con amministrazione si intende un soggetto della pubblica amministrazione registrato nel contesto dell' IPA.

4.3.1 Semantica di dominio

La semantica dei servizi si struttura su tre livelli: la *semantica dell'accordo di servizio*, la *semantica della classe di servizio* e *l'istanza del servizio specifico* del dominio di cooperazione.

Nel contesto della semantica di dominio gli aspetti che è interessante modellare sono essenzialmente quelli relativi al modello dati e quelli relativi agli attori che a diverso titolo giocano un ruolo nel contesto dell'erogazione o fruizione del servizio applicativo.

In particolare, per quanto concerne il dominio in oggetto, il modello dati è rappresentato dal *documento*, mentre gli attori individuati sono le amministrazioni *mittente e destinatario* del documento.

Come è possibile notare in Figura 6 il modello di documento riporta esattamente tutti i concetti espressi nell'analisi. Ogni *documento*, sia esso *cartaceo* o *elettronico*, è parte di un *fascicolo* che raccoglie tutti i *documenti* relativi alla pratica amministrativa specifica. Ogni documento ha associata una particolare *visibilità*, ha associata una specifica *segnatura*, ha un riferimento alla *segnatura del mittente* e riporta i dati del *mittente* e del *destinatario*.

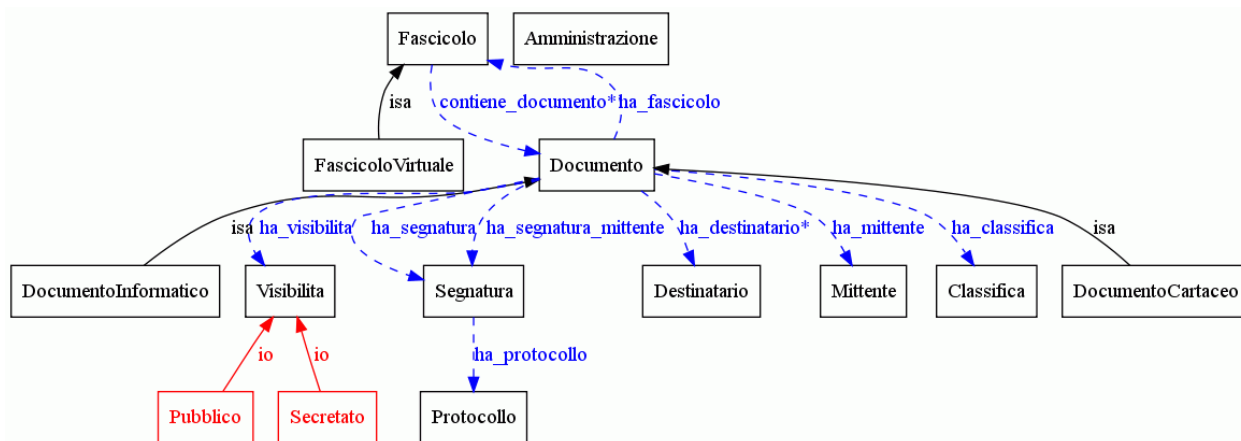


Figura 6: Dettaglio del concetto di documento

In Figura 7 è mostrato il dettaglio degli attori rilevanti per il dominio che come già detto sono le amministrazioni *mittente* e *destinatario* dello stesso. Dalla figura si evince che mittente e destinatario sono entrambe delle *aree organizzative omogenee* che afferiscono a specifiche amministrazioni.



Figura 7: Dettaglio attori coinvolti nel dominio

4.3.2 Semantica dei servizi

Nel contesto dell'analisi è stato rilevato che il dominio di riferimento fa capo solo alla classe di servizio *Servizio Archivio*. Il generico servizio archivio è istanziato per gestire specificatamente l'insieme dei *documenti* che arrivano ad un'area organizzativa omogenea.

In Figura 8 è rappresentato lo stralcio dell'ontologia di riferimento che formalizzata la struttura del *Servizio Archivio dei servizi documentali* erogato dal dominio di cooperazione applicativa. Il diagramma mostra come il *Servizio Archivio dei Servizi Documentali* gestisce un generico documento, implementa diverse operazioni di consultazione e prevede come utente il *mittente* del documento.

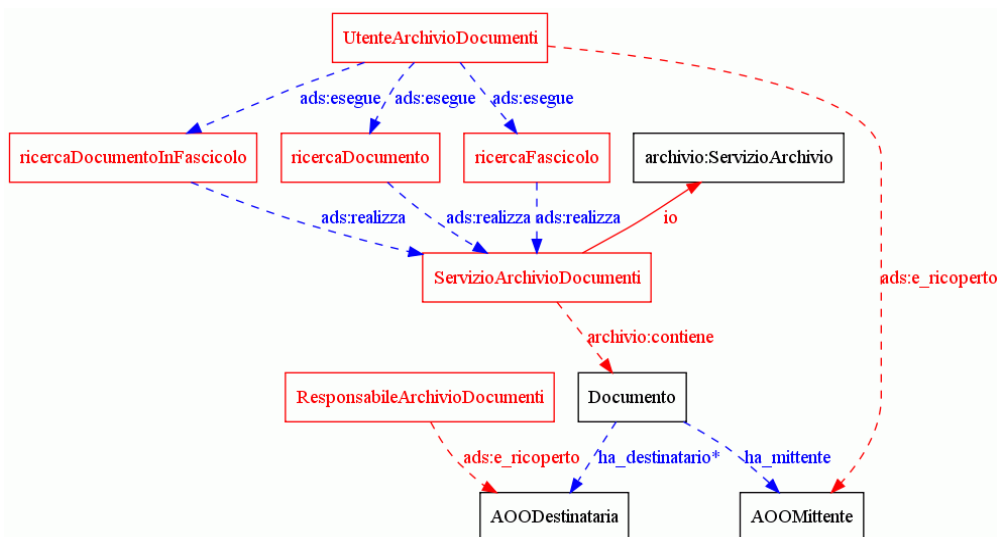


Figura 8: Servizio Archivio Servizi Documentali

5.2 Servizio Archivio

In Figura 10 è rappresentata l'ontologia che definisce la semantica di riferimento che formalizza la struttura del Servizio Archivio [www.lego-lab.org/icar/servizioArchivio.owl]. Dal diagramma si evince che il generico Servizio Archivio gestisce uno specifico *elemento* (dato memorizzato), prevede le operazioni di *aggiornamento*, *consultazione* e *notifica delle variazioni* dell'archivio ed inoltre individua i ruoli *responsabile* ed *utente* che a vario titolo possono eseguire le operazioni individuate.

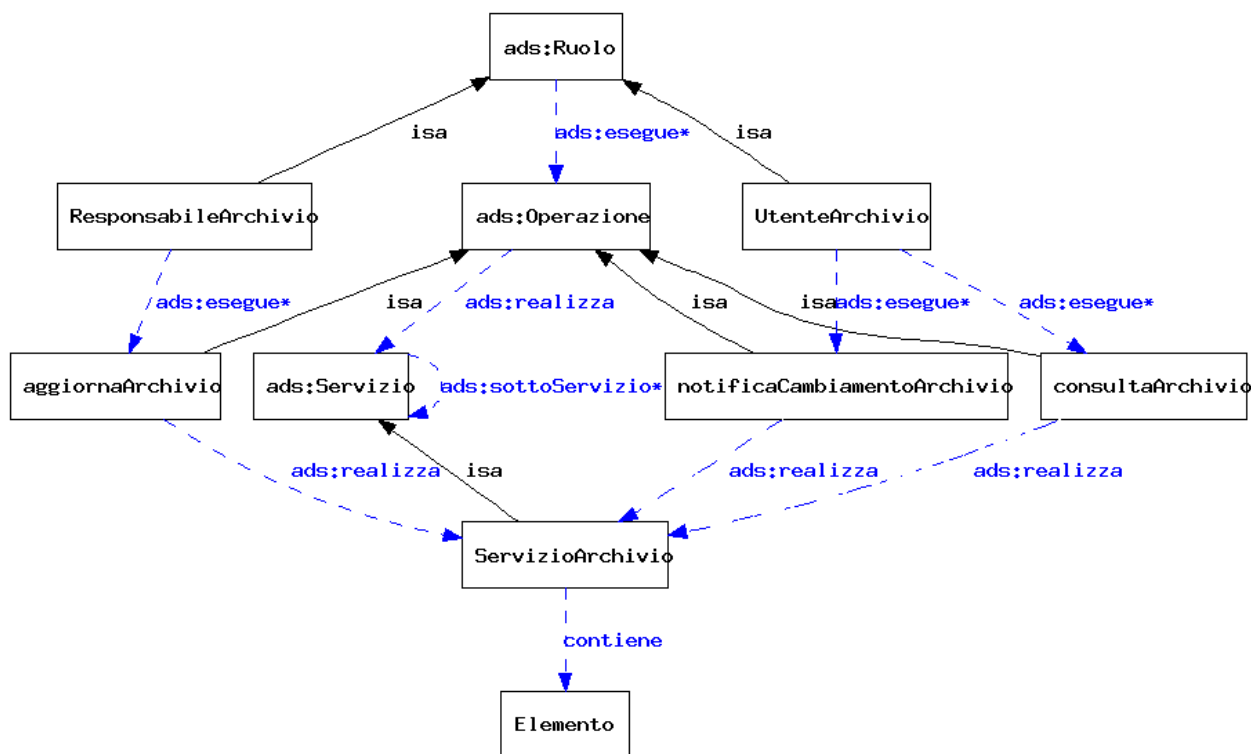


Figura 10: Ontologia Servizio Archivio

ALLEGATO 2

Accordi di Servizio per l'Indice della Pubblica Amministrazione (IPA) e Servizi Documentali



**Progetto interregionale ICAR
“Interoperabilità e Cooperazione Applicativa tra le
Regioni”**

<Task AP3>

AP3-Documento Descrittivo degli Accordi di Servizio

Versione <1.2>

STATO DELLE VARIAZIONI

versione	PARAGRAFO O PAGINA	DESCRIZIONE DELLA VARIAZIONE
V 1.0	Tutto il documento	Versione iniziale del documento
V 1.1	Tutto il documento	Aggiunti Accordi di servizio IPA
V 1.2	Tutto il documento	Aggiunti Accordi di Servizio Servizi Documentali e Revisione completa

INDICE

1. SCOPO E RIFERIMENTI DEL DOCUMENTO.....	692
1.1 SCOPO DEL DOCUMENTO	692
1.2 RIFERIMENTI.....	692
2. INTRODUZIONE AGLI ACCORDI DI SERVIZIO.....	693
2.1 CONCETTI DI BASE	693
2.1.1 SCAMBI DI MESSAGGI E SCENARI DI COORDINAMENTO	693
2.1.2 CLASSI DI SERVIZI	694
2.1.3 VERSIONI DI UN ADS.....	694
2.2 SPECIFICA DI UN ADS.....	694
2.2.1 PARTE COMUNE.....	694
2.2.2 PARTE SPECIFICA.....	695
2.2.3 TASK INF1 E ADS	695
2.3 RACCOMANDAZIONI	695
2.4 PROPOSTA STRUTTURA ADS	695
3. SERVIZI DOCUMENTALI	696
3.1 INTERROGAFASC	696
3.1.1 ACCORDO DI SERVIZIO	699
3.1.2 CASO D'USO	701
3.2 INTERROGADOC	701
3.2.1 ACCORDO DI SERVIZIO	702
3.2.2 CASO D'USO	706
3.3 RICERCA	706
3.3.1 ACCORDO DI SERVIZIO	707
3.3.2 CASO D'USO	710
4. AGGIORNAMENTO INDICE PUBBLICA AMMINISTRAZIONE	710
4.1 AGGIORNAMENTOIPA	710
4.1.1 ACCORDO DI SERVIZIO	710
4.1.2 CASO D'USO	715

1.Scopo e riferimenti del documento

1.1Scopo del documento

Questo documento illustra gli accordi di servizio definiti nell'ambito del task AP3 sui temi Indice della Pubblica Amministrazione (IPA) e Servizi Documentali.

Il documento è rivolto alle Regioni partecipanti.

Il documento si articola nelle seguenti sezioni:

- Introduzione agli Accordi di Servizio
- Accordi di servizio per i Servizi Documentali.
- Accordi di servizio per AggiornamentoIPA.

1.2Riferimenti

- Documenti CNIPA/SPCoop
 - [1] SPCoop-AccordoServizio_v1.0_20051014.pdf
 - [2] Linee_guida_per_la_compilazione_degli_accordi_di_servizio_v0.1.pdf
 - [3] SPCoop-NomenclaturaSemantica_v1.0_20051014.pdf
- Documenti ICAR
 - [4] ICAR_TaskINF1-SpecificheAS1.0.doc
- Documenti AP3
 - [5] PropostaCompilazioneADS.ppt
 - [6] AccordiDiServiziov1.2.zip

2. Introduzione agli Accordi di Servizio

Un Accordo di Servizio (ADS) definisce le prestazioni di un servizio e le modalità di erogazione/fruizione del servizio stesso.

Il contenuto di un ADS è descritto ampiamente nel documento [1] ed il task INF ha ulteriormente specificato il formato adottato per la rappresentazione di un ADS nel documento [4]. Nel seguito viene comunque fornita una breve introduzione all'argomento (ripresa in parte dai documenti citati) che ha lo scopo di facilitare nella comprensione del documento stesso.

2.1 Concetti di base

2.1.1 Scambi di messaggi e scenari di coordinamento

Nell'architettura SPCoop, tra due sistemi s'instaura una relazione di servizio se uno dei due sistemi, che riveste il ruolo di fruitore, utilizza i risultati di trattamenti informatici effettuati dall'altro sistema, che riveste il ruolo di erogatore. La modalità in cui erogatore e fruitore interagiscono è tramite scambio di messaggi. Ne esistono di tre tipi:

- *messaggio senza replica*: un sistema *mittente* invia un messaggio a un sistema *destinatario*;
- *messaggio/replica sincroni*: un sistema *richiedente* trasmette un *messaggio sincrono* a un sistema *rispondente* e si mette in attesa della *replica sincrona*. Successivamente il rispondente trasmette una *replica sincrona* al richiedente correlata logicamente con il messaggio;
- *messaggio/replica asincroni*: un sistema *richiedente* trasmette un *messaggio asincrono* a un sistema *rispondente*. Il rispondente trasmette in seguito una *replica asincrona* al richiedente correlata logicamente con il messaggio ricevuto. La correlazione a livello logico tra messaggio e replica asincroni è rappresentata esplicitamente dall'inserzione nella replica di un identificatore di correlazione.

Lo scambio elementare di messaggi è utilizzato per definire gli *scenari di coordinamento*. Sono previsti alcuni tipi di *scenari elementari di coordinamento* dell'erogazione/fruizione del servizio:

- *Richiesta senza risposta*: viene implementato utilizzando il *messaggio senza replica*.
- *Richiesta/risposta*: dal punto di vista del fruitore è possibile avere:
 - *Richiesta/risposta sincrona*: utilizza uno scambio elementare di tipo *messaggio/replica sincroni*.
 - *Richiesta/risposta asincrona*: utilizza lo scambio elementare di tipo *messaggio/replica asincroni*. L'identificatore di correlazione messaggio/replica può essere utilizzato come identificatore di correlazione richiesta/risposta.
- *Notificazione senza risposta*: utilizza uno scambio elementare di tipo *messaggio senza replica*.
- *Notificazione/risposta*: utilizza lo scambio elementare messaggio/replica sincrono o asincrono.

2.1.2 Classi di servizi

I servizi disponibili su SPCoop si distinguono in 4 classi.

- *Servizi mono-erogatore/multi-fruitore*
Il servizio è erogato da un solo sistema erogatore e destinato alla fruizione di un unico sistema fruitore.
- *Servizi mono-erogatore/multi-fruitore*
Il servizio è erogato da un solo sistema erogatore e destinato alla fruizione di M fruitori
- *Servizi multi-erogatore/mono-fruitore*
Il servizio è erogato da un insieme di N sistemi erogatori e destinato alla fruizione di un unico sistema fruitore.
- *Servizi multi-erogatore/multi-fruitore*
Il servizio è erogato da un insieme di N sistemi erogatori e destinato alla fruizione di M fruitori.

2.1.3 Versioni di un ADS

I servizi disponibili su SPCoop sono gestiti per versioni dell'accordo di servizio; più versioni di uno stesso servizio (corrispondenti a versioni diverse dell'accordo di servizio) possono essere erogate/fruite nello stesso momento. Ogni versione segue un ciclo di vita autonomo.

2.2 Specifica di un ADS

Un ADS è composto da:

- una *Parte Comune* che formalizza gli aspetti riusabili in differenti contesti
- una *Parte Specifica* che completa la parte comune, aggiungendo le informazioni specifiche per una particolare coppia di erogatore-fruitore.

2.2.1 Parte Comune

La Parte Comune di un ADS è composta da:

- **specifica delle Interfacce:** descrive l'interfaccia del servizio a livello di scenario di coordinamento e di scambio elementare di messaggi del fruitore e dell'erogatore:
 - wsdl concettuale
 - wsdl logico fruitore (da includere sempre anche se vuoto)
 - wsdl logico erogatore;
- **specifica delle Conversazioni:** (opzionale) quando necessaria, descrive le conversazioni supportate dal servizio (sequenza di scambi che il servizio supporta). Viene rappresentata con il WSBL (Web Service Behaviour Language) e consiste in:
 - wsbl concettuale
 - wsbl logico fruitore
 - un wsbl logico erogatore;

- **riferimento alla semantica:** (opzionale) contiene un riferimento all'ontologia/schema concettuale (o porzioni di essa) che definisce la semantica dell'informazione veicolata dal servizio. La descrizione della semantica viene solo riferita nell'ADS e lasciata come elemento esterno.

2.2.2 Parte Specifica

La Parte Specifica di un ADS contiene:

- **Specifica dei Porti di Accesso:** descrive gli aspetti implementativi (livello fisico) dei Web Service dell'erogatore e fruitore, ovvero l'URI dei punti d'accesso ed i binding (basati sulla Busta eGov) delle varie operazioni.
- **Specifica dei Livelli di Servizio:** (opzionale) descrive gli elementi necessari per poter definire i livelli di servizio concordati tra erogatore e fruitore, ed il modo di valutarli e misurarli.
- **Specifica delle Caratteristiche di Sicurezza:** (opzionale) descrive le caratteristiche di sicurezza supportate e richieste dal servizio.

2.2.3 Task INF1 e ADS

Tra i vari file previsti in [1] per un accordo di servizio, il task INF1 aggiunge:

- un file manifest.xml conforme allo schema descritto in [4] e formalizzato sia per la parte comune che per la parte specifica (incluso nel path META-INF)
- un file informazioni-egov.xml che descrive in modo semiformale (per lo schema vedi [4]) per ogni operazione presente in un servizio il mapping in informazioni eGov.

I vari file di un ADS possono essere distribuiti separatamente o in archivi secondo la codifica zip. Per la parte comune è previsto un unico file zip (con suffisso ads), mentre la parte specifica può essere composta da:

1. un unico file zip che racchiude il manifesto e i vari documenti per un accordo di servizio [monofruitore-**monoerogatore**] o [multifruitore-**monoerogatore**];
2. diversi file zip che racchiudono ognuno il manifesto e i vari documenti di una parte specifica di ogni servizio erogato, nel caso di un contesto [monofruitore-**multierogatore**] o [multifruitore-**multierogatore**].

2.3 Raccomandazioni

Nel documento [1] sono fornite delle raccomandazioni (v. §6.3) sulla struttura dei WSDL e delle convenzioni sintattiche, che sono state recepite dagli ADS del task AP3, per es. riguardo la nomenclatura di tipi, elementi, messaggi e operazioni definite.

2.4 Proposta Struttura ADS

Nell'impacchettamento dei file componenti l'ADS, abbiamo ipotizzato e utilizzato, non essendoci ancora una specifica ufficiale in merito, la struttura che segue (per la parte Specifica è analoga). Attualmente il CNIPA sta ultimando il documento ufficiale che descrive anche la

struttura dell'ADS in termini di directory e non solo di file contenuti, ma non essendo ancora ultimato il documento si è deciso di mantenere la struttura proposta, la cui conversione in una diversa è sicuramente immediata.

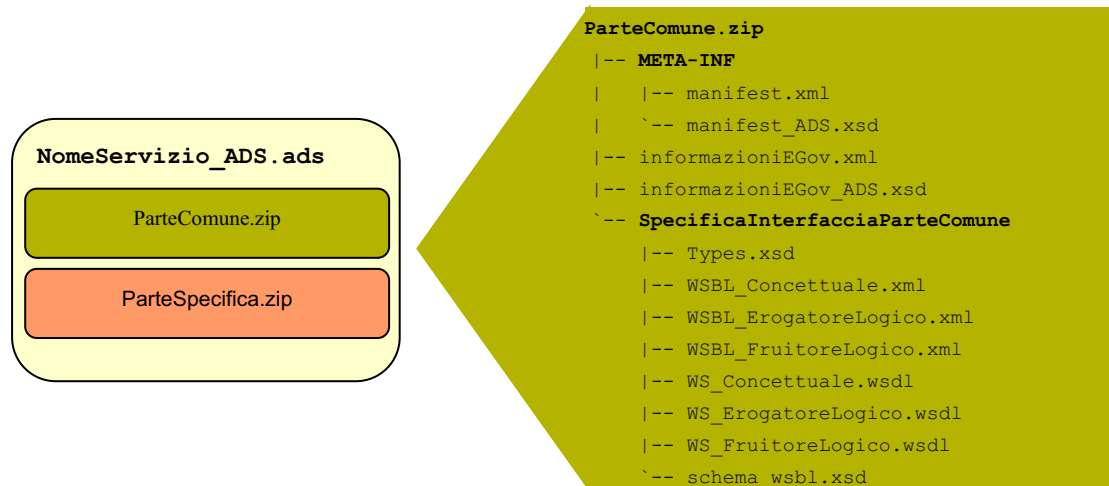


Figura 1- Struttura “impacchettamento” Parte Comune ADS

3.Servizi Documentali

I servizi documentali oggetto di specifica sono:

- InterrogaFasc
- InterrogaDoc
- Ricerca

Per ognuno di questi verrà data la descrizione dettagliata nei paragrafi che seguono.

3.1 InterrogaFasc

Richiesta del servizio

Il servizio riceve un oggetto di tipo AP3InterrogaFascRequest di cui viene riportato di seguito lo schema XML:

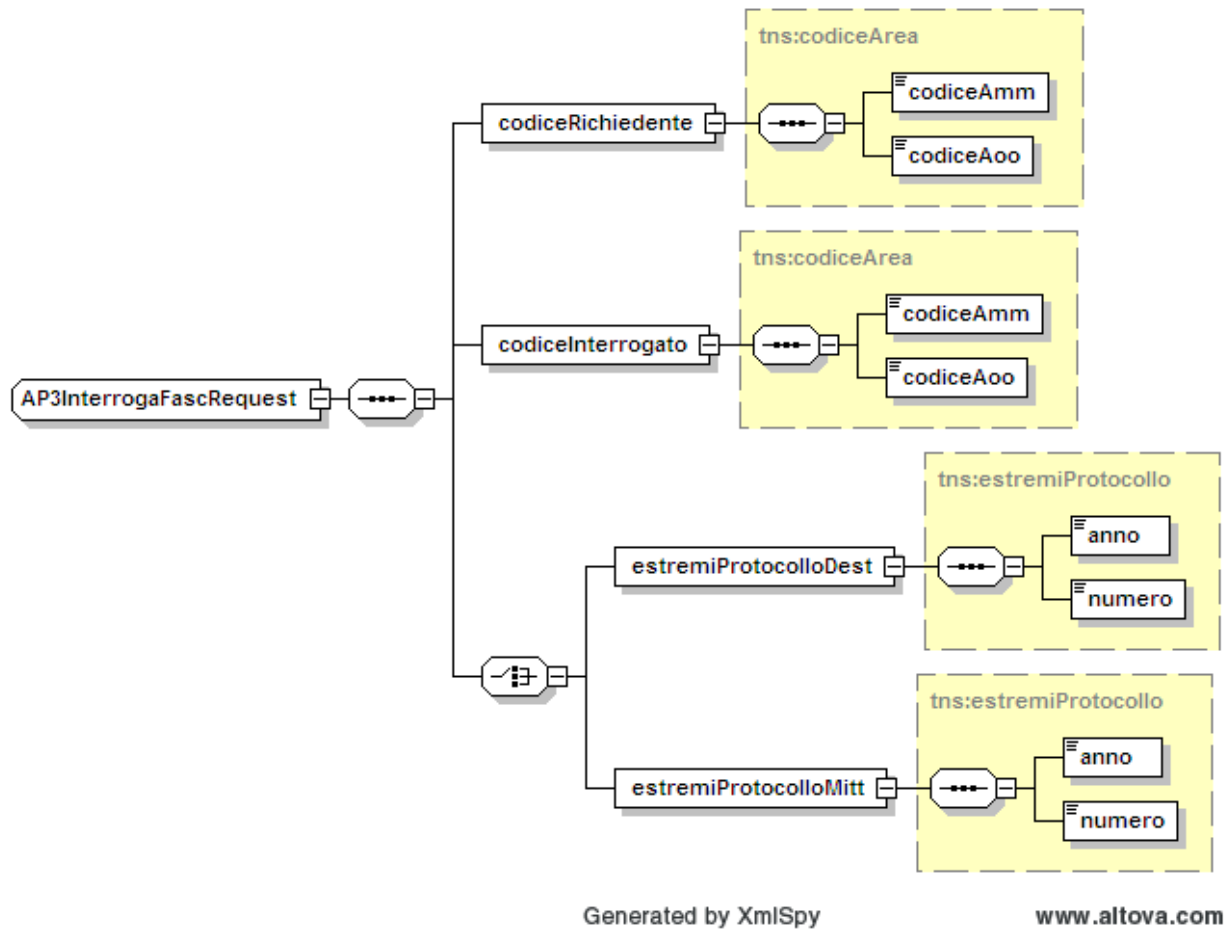


Figura 2- Richiesta InterrogaFasc

Risposta del Servizio

Il servizio risponde inviando un oggetto di tipo AP3InterrogaFascResponse il cui schema xsd è il seguente:

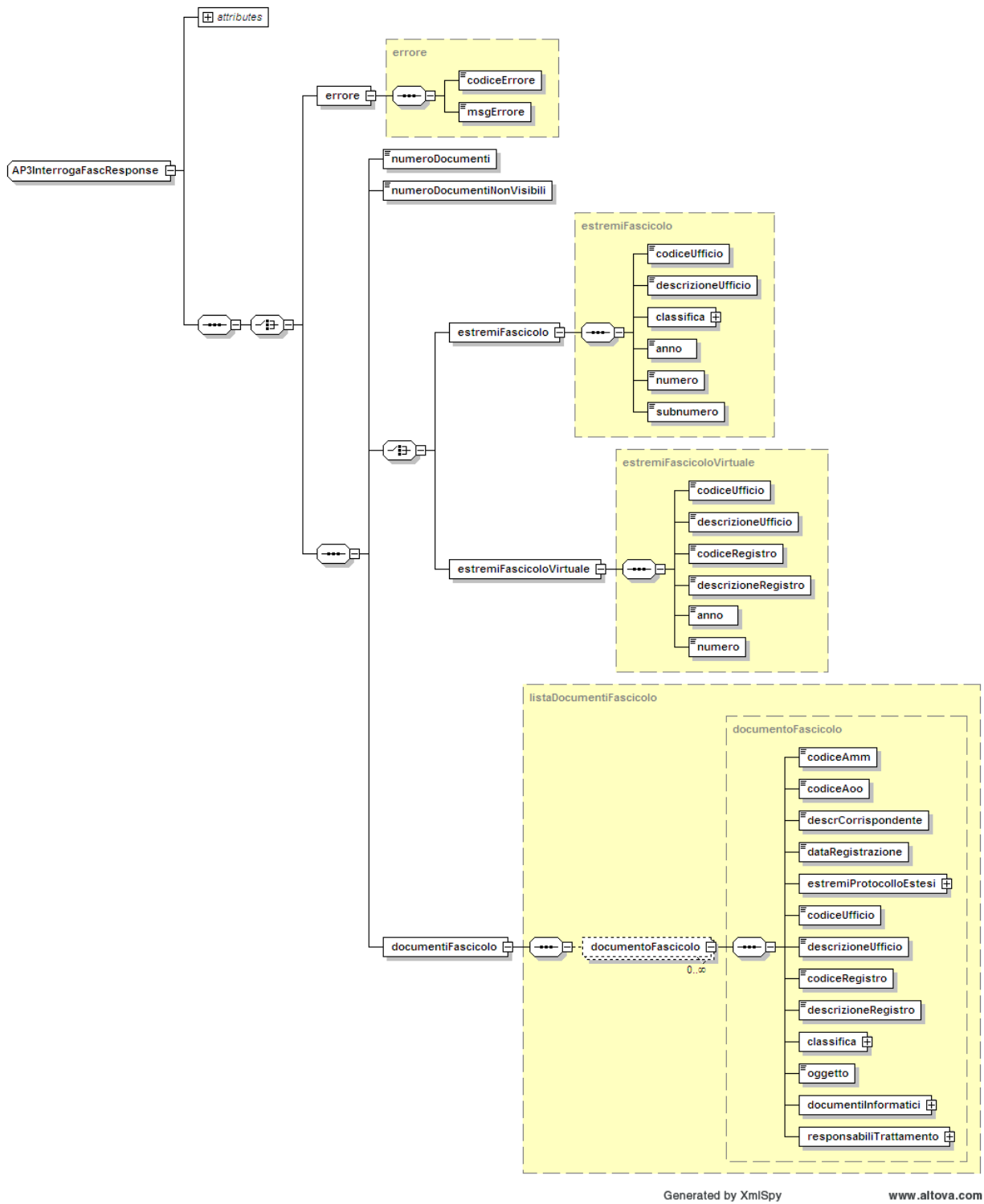


Figura 3- Risposta InterrogaFasc

3.1.1 Accordo di Servizio

Il servizio “Interroga Fascicolo” verrà implementato seguendo uno *scenario di coordinamento* di tipo “*Richiesta/Risposta Sincrono*”; pertanto, l’unica operazione definita dovrà rispettare uno *scambio elementare di messaggi* di tipo “*messaggio/replica sincrone*”. Esisterà quindi solo un “*WSDL Implementativo Erogatore*”, mentre sarà presente un “*WSDL Implementativo Fruitore*” vuoto in quanto non necessario.

L’ADS relativo sarà del tipo multi-erogatore/multi-fruitore.

Di seguito la struttura dell’accordo di servizio definito per “Interroga Fascicolo”. Per i file indicati fare riferimento al file InterrogaFasc_ADSv1.2.ads contenuto in [6].

Per la parte relativa alla Sicurezza, non essendoci ancora una versione ufficiale del documento di aggiornamento su tale tema da parte del CNIPA, si è preferito non includere tale parte, opzionale, nell’ADS.

Parte Comune

La parte comune dell’accordo di servizio descrive la specifica delle interfacce e delle conversazioni. Gli elementi che la compongono sono descritti nei sottoparagrafi che seguono.

manifest.xml

Il manifesto comprende il nome dell’accordo, una descrizione non formale, il nome del soggetto referente per l’accordo e i riferimenti ai documenti che compongono la parte comune. E’ incluso anche il riferimento al file delle ontologie definite per il task Ap3, che è utilizzato per annotare semanticamente il wsdl concettuale.

informazioniEgov

Le informazioni eGov descrivono, in particolare, le azioni presenti in un servizio ed il profilo di collaborazione (sincrono).

WS_Concettuale.wsdl

Il WSDL Concettuale descrive le operazioni offerte dal servizio in termini di scenari elementari di coordinamento.



Figura 4- InterrogaFasc - WSDL Concettuale

WS_ErogatoreLogico.wSDL

Il WSDL Logico dell'erogatore definisce lo scambio elementare dei messaggi di competenza dell'erogatore.

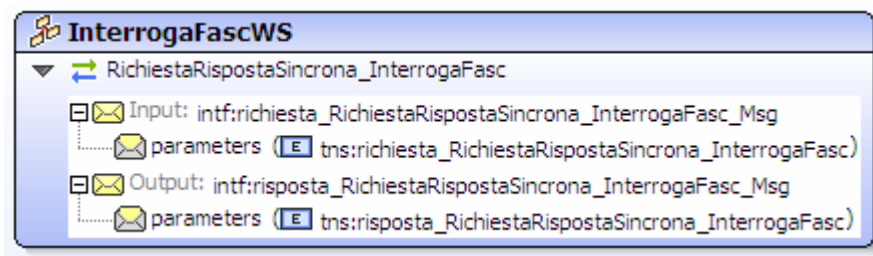


Figura 5- InterrogaFasc - WSDL Erogatore Logico

WS_FruitoreLogico.wSDL

Il WSDL Logico del fruitore definisce lo scambio elementare dei messaggi di competenza del fruitore. Per questo servizio sarà presente ma vuoto (in conformità alle indicazioni CNIPA), in quanto il servizio InterrogaFasc rispetta uno scenario di coordinamento di tipo *richiesta/risposta sincrono*.

Parte Specifica

La parte specifica dell'accordo di servizio dettaglia la parte comune, istanziandola per un particolare coppia di <erogatore-fruitore>. Gli elementi che la compongono sono descritti nei sottoparagrafi che seguono.

manifest.xml

Il manifesto specifica il nome dell'accordo, i fruitori ed erogatori del servizio, e i riferimenti ai documenti descrittivi (WSDL) che compongono la parte specifica.

E' incluso, anche se commentato perché non specificato nell'xsd relativo, anche il riferimento al file WSAG di definizione degli SLA.

informazioniEgov

Le informazioni eGov descrivono, in particolare, le azioni presenti in un servizio ed il profilo di collaborazione (sincrono).

WS_ErogatoreImplementativo.wSDL

Il WSDL implementativo dell'erogatore definisce il binding del servizio su una

particolare implementazione, specificandone gli endpoint per l'invocazione.

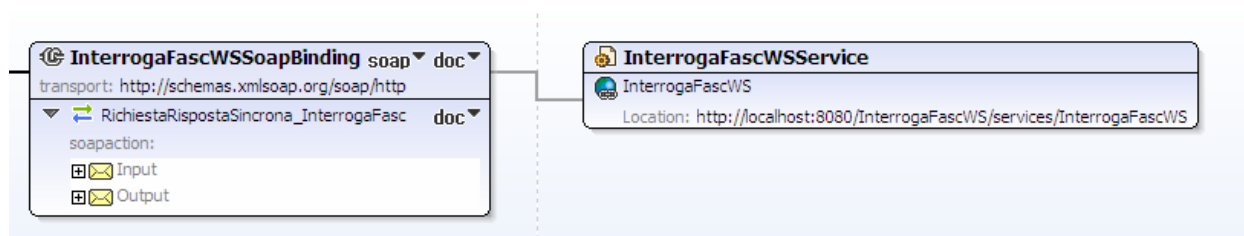


Figura 6- InterrogaFasc - WSDL Erogatore Implementativo

WS_FruitoreImplementativo.wsdl

Il WSDL implementativo del fruitore è presente anche se vuoto.

WS_Parametri_SLA.wsag (Dichiarazione dei parametri SLA)

E' una specifica opzionale che descrive gli elementi necessari per poter definire i livelli di servizio concordati tra erogatore e fruitore ed il modo di valutarli e misurarli.

Il servizio di "InterrogaFascicolo" definisce la seguente metrica di risorsa:

- **tempoRisposta:** rappresenta l'intervallo di tempo, espresso in secondi, che intercorre tra l'invocazione del servizio e l'invio della risposta sincrona da parte dell'erogatore al fruitore.

Viene anche definito il seguente parametro SLA:

- **TempoRispostaMedio1M:** Rappresenta la media, osservata in una finestra temporale di un mese, del tempo di risposta del servizio (metrica di base "tempoRisposta"). Affinché il parametro risulti soddisfatto si impone che questo valore sia inferiore a 3 secondi.

3.1.2Caso d'uso

Nel front-end sviluppato per il task Ap3 il servizio InterrogaFasc utilizzerà, per l'integrazione con la Porta di Dominio sviluppata nel task INF1, la modalità trasparente.

3.2 InterrogaDoc

Richiesta del servizio

Il servizio riceve un oggetto di tipo AP3InterrogaDocRequest di cui viene riportato di seguito lo

schema XML:

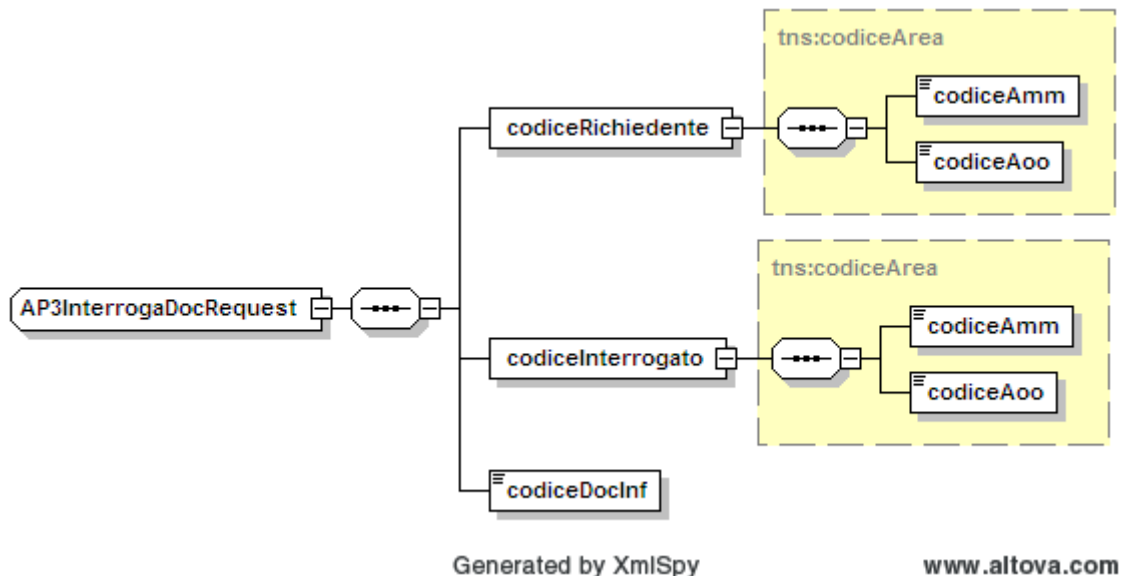


Figura 7- Richiesta InterrogaDoc

Risposta del Servizio

Il servizio risponde inviando un oggetto di tipo AP3InterrogaDocResponse il cui schema xsd è il seguente:

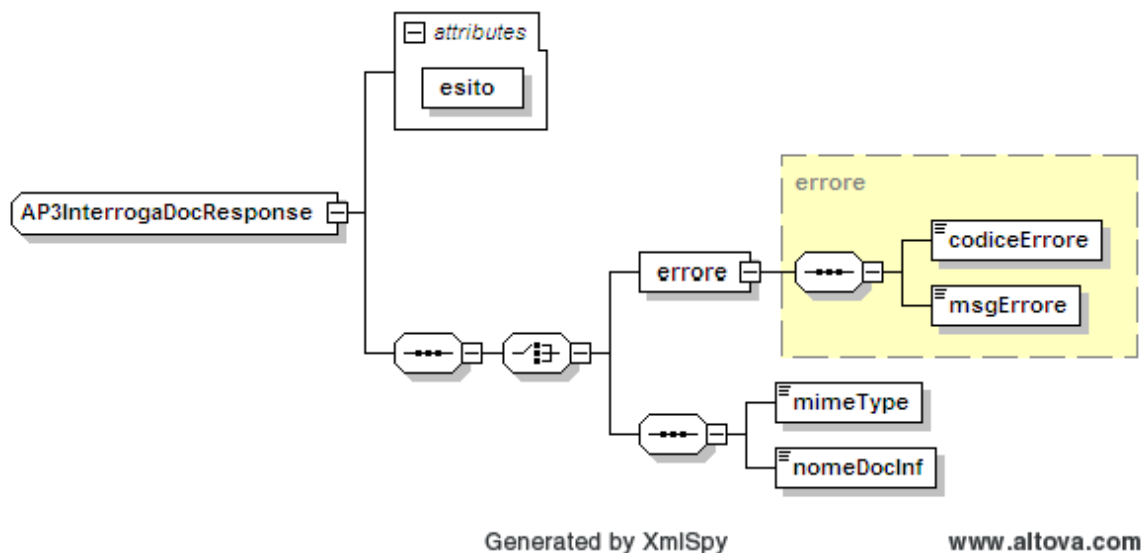


Figura 8- Risposta InterrogaDoc

3.2.1 Accordo di Servizio

Il servizio “Interroga Documento” verrà implementato seguendo uno *scenario di coordinamento* di tipo “*Richiesta/Risposta Sincrono*”; pertanto, l’unica operazione definita dovrà rispettare uno *scambio elementare di messaggi* di tipo “*messaggio/replica sincrone*”. Esisterà quindi solo un “*WSDL Implementativo Erogatore*”, mentre sarà presente un “*WSDL Implementativo Fruitore*” vuoto in quanto non necessario.

L’ADS relativo sarà del tipo multi-erogatore/multi-fruitore.

Per la parte relativa alla Sicurezza, non essendoci ancora una versione ufficiale del documento di aggiornamento su tale tema da parte del CNIPA, si è preferito non includere tale parte, opzionale, nell’ADS.

Di seguito la struttura dell’accordo di servizio definito per “Interroga Documento”. Per i file indicati fare riferimento al file InterrogaDoc_ADSv1.2.ads contenuto in [6].

Parte Comune

La parte comune dell’accordo di servizio descrive la specifica delle interfacce e delle conversazioni. Gli elementi che la compongono sono descritti nei sottoparagrafi che seguono.

manifest.xml

Il manifesto comprende il nome dell’accordo, una descrizione non formale, il nome del soggetto referente per l’accordo e i riferimenti ai documenti che compongono la parte comune. E’ incluso anche il riferimento al file delle ontologie definite per il task Ap3, che è utilizzato per annotare semanticamente il wsdl concettuale.

informazioniEgov

Le informazioni eGov descrivono, in particolare, le azioni presenti in un servizio ed il profilo di collaborazione (sincrono).

WS_Concettuale.wsdl

Il WSDL Concettuale descrive le operazioni offerte dal servizio in termini di scenari elementari di coordinamento.



Figura 9- InterrogaDoc - WSDL Concettuale

WS_ErogatoreLogico.wSDL

Il WSDL Logico dell'erogatore definisce lo scambio elementare dei messaggi di competenza dell'erogatore.

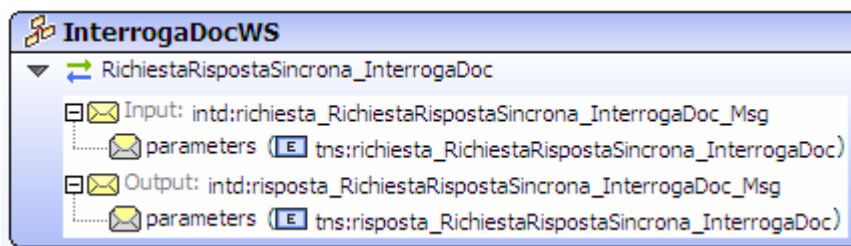


Figura 10- InterrogaDoc - WSDL Erogatore Logico

WS_FruitoreLogico.wSDL

Il WSDL Logico del fruitore definisce lo scambio elementare dei messaggi di competenza del fruitore. Per questo servizio sarà presente ma vuoto (in conformità alle indicazioni CNIPA), in quanto il servizio InterrogaFasc rispetta uno scenario di coordinamento di tipo *richiesta/risposta sincrono*.

Parte Specifica

La parte specifica dell'accordo di servizio dettaglia la parte comune, istanziandola per un particolare coppia di <erogatore-fruitore>. Gli elementi che la compongono sono descritti nei sottoparagrafi che seguono.

manifest.xml

Il manifesto specifica il nome dell'accordo, i fruitori ed erogatori del servizio, e i

riferimenti ai documenti descrittivi (WSDL) che compongono la parte specifica.

E' incluso, anche se commentato, perché non specificato nell'xsd relativo, anche il riferimento al file WSAG di definizione degli SLA.

informazioniEgov

Le informazioni eGov descrivono, in particolare, le azioni presenti in un servizio ed il profilo di collaborazione (sincrono).

WS_ErogatoreImplementativo.wsdl

Il WSDL implementativo dell'erogatore definisce il binding del servizio su una particolare implementazione, specificandone gli endpoint per l'invocazione.



Figura 11- InterrogaDoc - WSDL Erogatore Implementativo

WS_FruitoreImplementativo.wsdl

Il WSDL implementativo del fruitore è presente anche se vuoto.

WS_Parametri_SLA.wsag (Dichiarazione dei parametri SLA)

E' una specifica opzionale che descrive gli elementi necessari per poter definire i livelli di servizio concordati tra erogatore e fruitore ed il modo di valutarli e misurarli.

Il servizio di "InterrogaFascicolo" definisce la seguente metrica di risorsa:

- **tempoRisposta**: rappresenta l'intervallo di tempo, espresso in secondi, che intercorre tra l'invocazione del servizio e l'invio della risposta sincrona da parte dell'erogatore al fruitore.

Viene anche definito il seguente parametro SLA:

- **TempoRispostaMedio1M**: Rappresenta la media, osservata in una finestra temporale di un mese, del tempo di risposta del servizio (metrica di base "tempoRisposta"). Affinché il parametro risulti soddisfatto si impone che questo valore sia inferiore a 3 secondi.

3.2.2 Caso d'uso

Nel front-end sviluppato per il task Ap3 il servizio InterrogaDoc utilizzerà, per l'integrazione con la Porta di Dominio sviluppata nel task INF1, la modalità trasparente.

3.3 Ricerca

Richiesta del servizio

Il servizio riceve un oggetto di tipo AP3RicercaRequest di cui viene riportato di seguito lo schema XML:

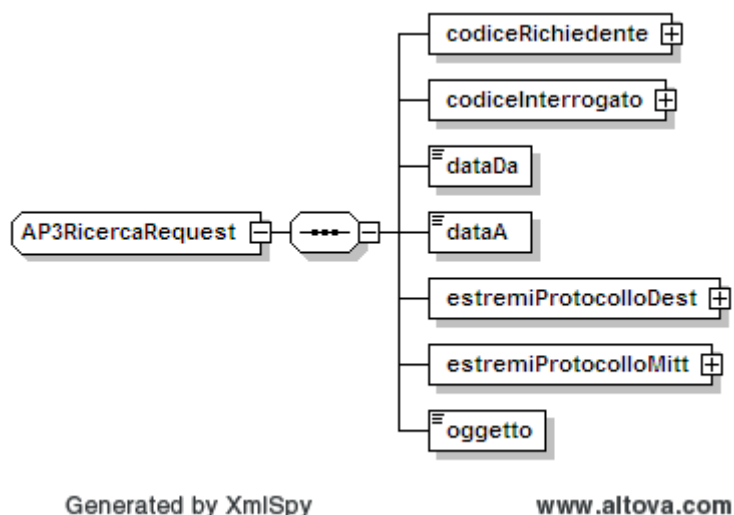


Figura 12- Richiesta Ricerca

Risposta del Servizio

Il servizio risponde inviando un oggetto di tipo AP3RicercaResponse il cui schema xsd è il seguente:

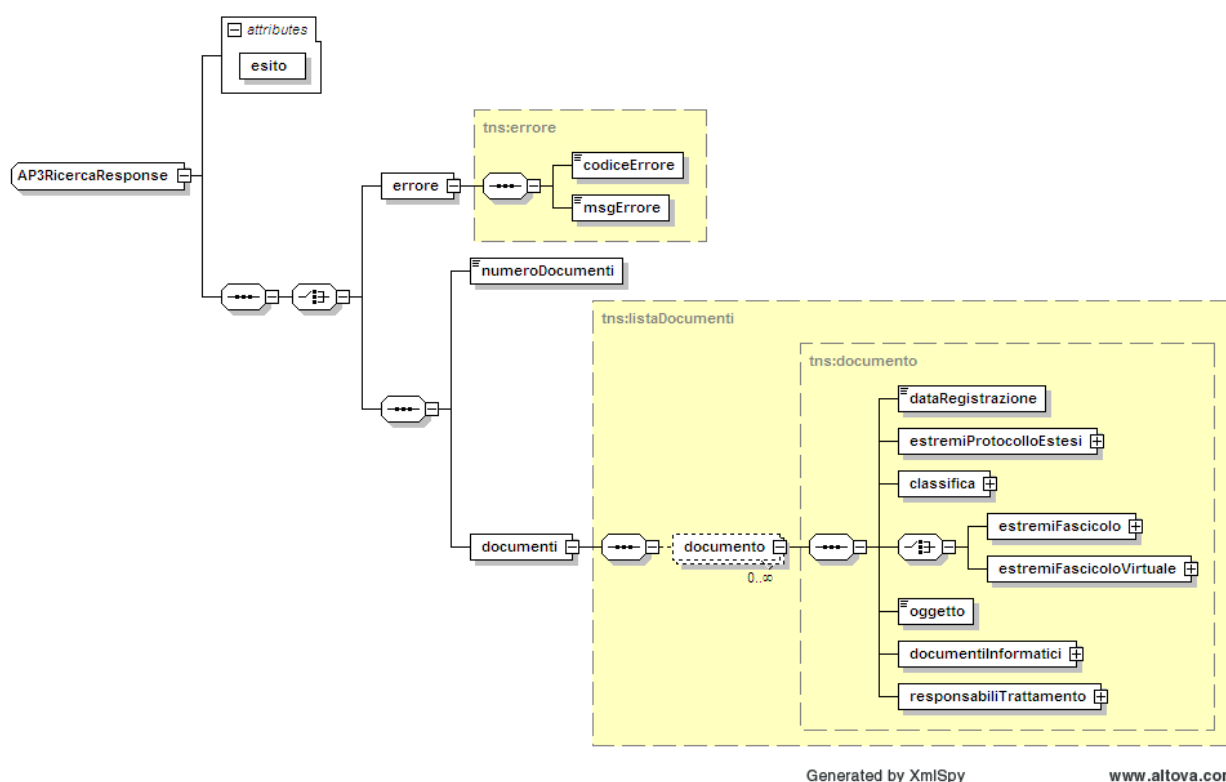


Figura 13- Risposta Ricerca

3.3.1 Accordo di Servizio

Il servizio “Ricerca” verrà implementato seguendo uno *scenario di coordinamento* di tipo “*Richiesta/Risposta Sincrono*”; pertanto, l’unica operazione definita dovrà rispettare uno *scambio elementare di messaggi* di tipo “*messaggio/replica sincrono*”. Esisterà quindi solo un “*WSDL Implementativo Erogatore*”, mentre sarà presente un “*WSDL Implementativo Fruitore*” vuoto in quanto non necessario.

L’ADS relativo sarà del tipo multi-erogatore/multi-fruitore.

Per la parte relativa alla Sicurezza, non essendoci ancora una versione ufficiale del documento di aggiornamento su tale tema da parte del CNIPA, si è preferito non includere tale parte, opzionale, nell’ADS.

Di seguito la struttura dell’accordo di servizio definito per “Ricerca”. Per i file indicati fare riferimento al file Ricerca_ADSv1.2.ads contenuto in [6].

Parte Comune

La parte comune dell’accordo di servizio descrive la specifica delle interfacce e delle conversazioni. Gli elementi che la compongono sono descritti nei sottoparagrafi che seguono.

manifest.xml

Il manifesto comprende il nome dell'accordo, una descrizione non formale, il nome del soggetto referente per l'accordo e i riferimenti ai documenti che compongono la parte comune. E' incluso anche il riferimento al file delle ontologie definite per il task Ap3, che è utilizzato per annotare semanticamente il wsdl concettuale.

informazioniEgov

Le informazioni eGov descrivono, in particolare, le azioni presenti in un servizio ed il profilo di collaborazione (sincrono).

WS_Concettuale.wsdl

Il WSDL Concettuale descrive le operazioni offerte dal servizio in termini di scenari elementari di coordinamento.



Figura 14- Ricerca - WSDL Concettuale

WS_ErogatoreLogico.wsdl

Il WSDL Logico dell'erogatore definisce lo scambio elementare dei messaggi di competenza dell'erogatore.

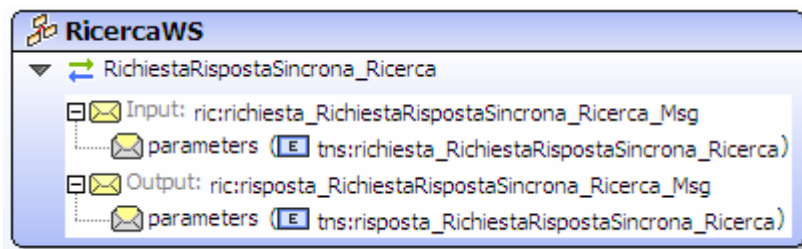


Figura 15- Ricerca - WSDL Erogatore Logico

WS_FruitoreLogico.wsdl

Il WSDL Logico del fruitore definisce lo scambio elementare dei messaggi di competenza del fruitore. Per questo servizio sarà presente ma vuoto (in conformità alle indicazioni CNIPA), in quanto il servizio InterrogaFasc rispetta uno scenario di

coordinamento di tipo *richiesta/risposta sincrono*.

Parte Specifica

La parte specifica dell'accordo di servizio dettaglia la parte comune, istanziandola per un particolare coppia di <erogatore-fruttore>. Gli elementi che la compongono sono descritti nei sottoparagrafi che seguono.

manifest.xml

Il manifesto specifica il nome dell'accordo, i fruitori ed erogatori del servizio, e i riferimenti ai documenti descrittivi (WSDL) che compongono la parte specifica.

E' incluso, anche se commentato perché non specificato nell'xsd relativo, anche il riferimento al file WSAG di definizione degli SLA.

informazioniEgov

Le informazioni eGov descrivono, in particolare, le azioni presenti in un servizio ed il profilo di collaborazione (sincrono).

WS_ErogatoreImplementativo.wSDL

Il WSDL implementativo dell'erogatore definisce il binding del servizio su una particolare implementazione, specificandone gli endpoint per l'invocazione.

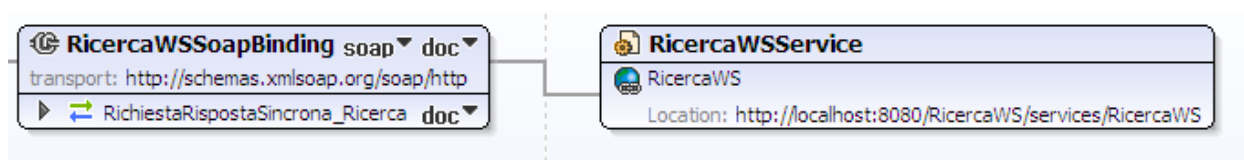


Figura 16- Ricerca - WSDL Erogatore Implementativo

WS_FruitoreImplementativo.wSDL

Il WSDL implementativo del fruitore è presente anche se vuoto.

WS_Parametri_SLA.wsag (Dichiarazione dei parametri SLA)

E' una specifica opzionale che descrive gli elementi necessari per poter definire i livelli di servizio concordati tra erogatore e fruitore ed il modo di valutarli e misurarli.

Il servizio di "InterrogaFascicolo" definisce la seguente metrica di risorsa:

- **tempoRisposta:** rappresenta l'intervallo di tempo, espresso in secondi, che intercorre tra l'invocazione del servizio e l'invio della risposta sincrona da parte dell'erogatore al fruitore.

Viene anche definito il seguente parametro SLA:

- **TempoRispostaMedio1M:** Rappresenta la media, osservata in una finestra temporale di un mese, del tempo di risposta del servizio (metrica di base "tempoRisposta"). Affinché il parametro risulti soddisfatto si impone che questo valore sia inferiore a 3 secondi.

3.3.2Caso d'uso

Nel front-end sviluppato per il task Ap3 il servizio Ricerca utilizzerà, per l'integrazione con la Porta di Dominio sviluppata nel task INF1, la modalità trasparente.

4. Aggiornamento Indice Pubblica Amministrazione

E' stato specificato in questo contesto un unico servizio:

- AggiornamentoIPA

Il servizio verrà descritto in dettaglio nei paragrafi che seguono.

4.1 AggiornamentoIPA

4.1.1Accordo di Servizio

Il servizio "AggiornamentoIPA" verrà implementato seguendo uno *scenario di coordinamento* di tipo "Richiesta/Risposta Asincrona"; pertanto, le operazioni incluse in esso dovranno rispettare uno *scambio elementare di messaggi* di tipo "messaggio/replica asincroni".

Questo scenario di coordinamento prevederà quindi un "WSDL Implementativo Erogatore", in grado di trattare le richieste inviate da un Fruitore ed un "WSDL Implementativo Fruitore" in modo da poter ricevere le risposte e trattarle conseguentemente. Infine, il comportamento e l'interazione delle operazioni incluse nel servizio di "AggiornamentoIPA" sarà descritto con una macchina a stati mediante il linguaggio WSBL.

L'ADS relativo sarà di tipo mono-erogatore/multi-fruitore.

Di seguito la struttura dell'accordo di servizio definito per "AggiornamentoIPA". Per i file indicati fare riferimento al file AggiornamentoIPA_ADSv1.2.ads contenuto in [6].

Parte Comune

La parte comune dell'accordo di servizio descrive la specifica delle interfacce e delle conversazioni. Gli elementi che la compongono sono descritti nei sottoparagrafi che seguono.

manifest.xml

Il manifesto comprende il nome dell'accordo, una descrizione non formale, il nome del soggetto referente per l'accordo e i riferimenti ai documenti che compongono la parte comune. E' incluso anche il riferimento al file delle ontologie definite per il task Ap3, che è utilizzato per annotare semanticamente il wsdl concettuale.

informazioniEgov

Le informazioni eGov descrivono, in particolare, le azioni presenti in un servizio ed il profilo di collaborazione (asincrono).

WS_Concettuale.wsdl

Il WSDL Concettuale descrive le operazioni offerte dal servizio in termini di scenari elementari di coordinamento.

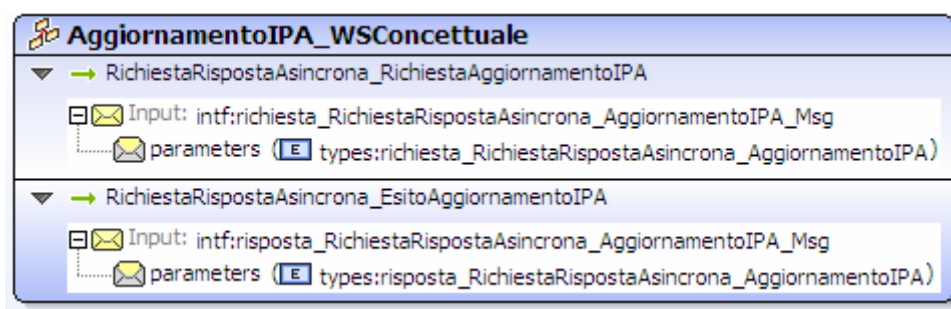


Figura 17- AggiornamentoIPA - WSDL Concettuale

WS_ErogatoreLogico.wsdl

Il WSDL Logico dell'erogatore definisce lo scambio elementare dei messaggi di competenza dell'erogatore.



Figura 18- AggiornamentoIPA - WSDL Erogatore Logico

WS_FruitoreLogico.wsdl

Il WSDL Logico del fruitore definisce lo scambio elementare dei messaggi di competenza del fruitore. Per questo servizio sarà presente e valorizzato trattandosi di servizio asincrono. Esso definisce il binding del servizio su una particolare

implementazione, specificandone gli endpoint per l'invocazione.



Figura 19- AggiornamentoIPA - WSDL Fruitore Logico

WSBL_Concettuale.xml:

Specifica concettuale delle conversazioni supportate dal servizio.

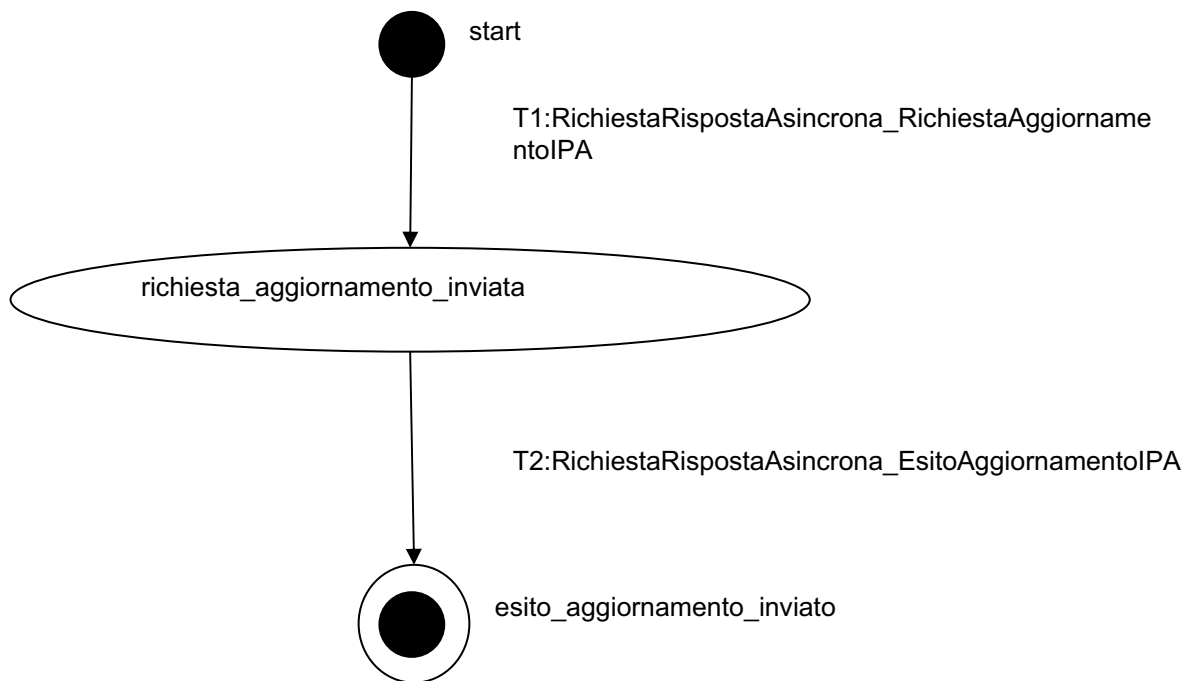


Figura 20- AggiornamentoIPA – WSBL Concettuale

WSBL_Erogatore.xml:

Nella figura seguente è mostrata la macchina a stati dell'Erogatore.



Figura 21- AggiornamentoIPA – Macchina a stati dell'erogatore

WSBL_Fruitore.xml:

Nella figura seguente è mostrata la macchina a stati del Fruitore.



Figura 22- AggiornamentoIPA – Macchina a stati del fruitore

Parte Specifica

La parte specifica dell'accordo di servizio dettaglia la parte comune, istanziandola per un particolare coppia di <erogatore-fruttore>. Gli elementi che la compongono sono descritti nei sottoparagrafi che seguono.

manifest.xml

Il manifesto specifica il nome dell'accordo, i fruitori ed erogatori del servizio, e i riferimenti ai documenti descrittivi (WSDL) che compongono la parte specifica.

E' incluso, anche se commentato perché non specificato nell'xsd relativo, anche il riferimento al file WSAG di definizione degli SLA.

informazioniEgov

Le informazioni eGov descrivono, in particolare, le azioni presenti in un servizio ed il profilo di collaborazione (asincrono).

WS_ErogatoreImplementativo.wSDL

Il WSDL implementativo dell'erogatore definisce il binding del servizio su una particolare implementazione, specificandone gli endpoint per l'invocazione.

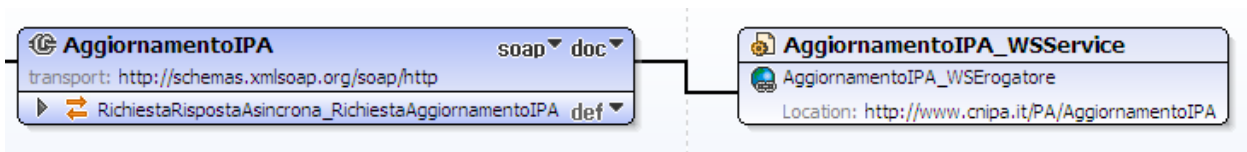


Figura 23- AggiornamentoIPA - WSDL Erogatore Implementativo

WS_FruitoreImplementativo.wSDL

Il WSDL implementativo del fruitore è presente e valorizzato trattandosi di servizio asincrono. Esso definisce il binding del servizio su una particolare implementazione, specificandone gli endpoint per l'invocazione.

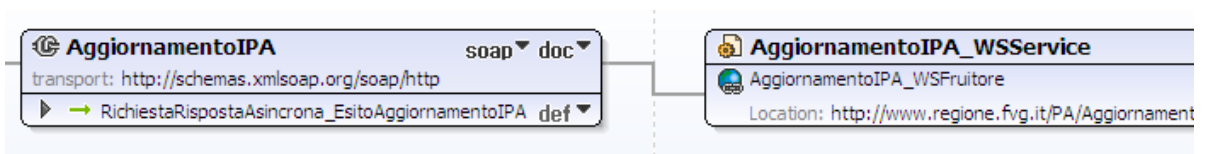


Figura 24- AggiornamentoIPA - WSDL fruitore Implementativo

WS_Parametri_SLA.wsag (Dichiarazione dei parametri SLA)

E' una specifica opzionale che descrive gli elementi necessari per poter definire i livelli di servizio concordati tra erogatore e fruitore ed il modo di valutarli e misurarli.

Il servizio di "InterrogaFascicolo" definisce la seguente metrica di risorsa:

- **tempoRisposta:** rappresenta l'intervallo di tempo, espresso in secondi, che intercorre tra l'invocazione del servizio e l'invio della risposta sincrona da parte dell'erogatore al fruitore.

Viene anche definito il seguente parametro SLA:

- **TempoRispostaMedio1M:** Rappresenta la media, osservata in una finestra temporale di un mese, del tempo di risposta del servizio (metrica di base "tempoRisposta"). Affinché il parametro risulti soddisfatto si impone che questo valore sia inferiore a 3 secondi.

4.1.2Caso d'uso

Il front-end sviluppato per il task Ap3 si limita all'utilizzo dei servizi documentali.

ALLEGATO 3

Servizi del SIT Regionale

Catalogo e metadati

Il Repertorio Regionale Dati Territoriali (RRDT) del SIT riuota il Repertorio Nazionale Dati Territoriali (RNDT). Finalità principe è il supporto all'interoperabilità nel campo dell'informazione geografica favorendo l'armonizzazione, l'accessibilità e il riutilizzo del vasto patrimonio di dati territoriali costituito dalla Regione.

L'RRDT è un catalogo di metadati basato sugli Standard ISO19115, 19119 e 19139 ed è coerente con la direttiva INSPIRE e con il Regolamento europeo sui metadati. Esso si delinea come un registro pubblico per conoscere con certezza quali informazioni sono disponibili, quali sono le loro caratteristiche tecniche e con quali modalità è possibile utilizzarle.

Ciò contribuisce anche a favorire la realizzazione di servizi che richiedono l'integrazione di dati di competenza di più Amministrazioni e ad agevolare la cooperazione tra Amministrazioni pubbliche nel programmare l'acquisizione di nuovi dati, razionalizzandone i costi.

Questo servizio fornisce le funzionalità tipiche di un catalogo e realizza due macroprocessi:

- la consultazione dei metadati, accessibile a tutti;
- la gestione dei metadati riservata alle Amministrazioni Pubbliche.

Nel Catalogo sono presenti:

- metadati relativi ai dati territoriali (cartografie tecniche tematiche etc);
- metadati relativi ai servizi (servizi di pianificazione territoriale, protezione civile etc.);
- metadati relativi alle nuove acquisizioni di dati territoriali

Le informazioni, in termini di metadati, relative ai dati territoriali e ai servizi di cui sono titolari le Pubbliche Amministrazioni sono liberamente consultabili, anche da parte dei privati, come previsto dall'art. 9 del DPCM.

Le informazioni contenute nel catalogo sono integrabili e aggiornabili solo dalle pubbliche Amministrazione accreditate e vengono gestite in un'area riservata.

Il RRDT pubblica le informazioni (metadati) prodotte da ciascuna Amministrazione titolare di dati/servizi territoriali, la quale, secondo la normativa vigente, resta pienamente responsabile in merito alla gestione ed al riutilizzo dei propri dati, compresi vincoli ed eventuali costi applicati.

La consultazione può avvenire in modalità estesa, con l'utilizzo di un navigatore geografico, o in modalità accessibile con semplici maschere alfanumeriche.

La tabella che segue riporta le principali funzionalità del RRDT.

Repertorio Regionale Dati Territoriali - RRDT:	
Permette di condividere le informazioni relative ai dati e servizi territoriali, comprese le loro caratteristiche e le modalità di utilizzo ed acquisizione, al fine di agevolare l'accessibilità al patrimonio pubblico disponibile. Le funzionalità di questo servizio di catalogo sono gestite attraverso le sezioni di consultazione e gestione dei metadati.	
Funzionalità	Descrizione
Consultazione Estesa (MapView)	Permette la ricerca e la consultazione dei metadati nella loro componente geografica.
Consultazione Accessibile	Gestisce l'interrogazione e la navigazione all'interno dei metadati.

Gestione Metadati	L'applicazione gestisce la logica dei processi di gestione, editing ed analisi dei metadati.
Ricerca documenti	Gestisce le operazioni di interrogazione e la navigazione all'interno dei metadati
Conformità RNDT	Controlla la conformità di un documento alle linee guida CNIPA – INSPIRE.
Importa singolo XML	Permette di inviare al repertorio direttamente file xml; la funzionalità è disponibile solo per utenti di gestore di metadati.
Importazione multipla	Consente di inviare al repertorio direttamente file xml; la funzionalità è disponibile solo per utenti di gestore di metadati. È propedeutica all'attivazione della funzionalità la validazione del documento agli standard CNIPA.
Editor metadati	Permette la creazione di una sessione di editing all'interno della quale andranno compilati i nuovi metadati attraverso inserimento di tutti i campi obbligatori e salvataggio della sessione con contestuale invio dei metadati.
Pubblicazione Repertorio (solo per l'amministratore)	Consente di sincronizzare i metadati inviati dagli utenti dal DB di staging al DB definitivo.

Consultazione avanzata

L'interfaccia di consultazione avanzata inclusa nel sistema del SIT Regionale offre un'insieme di funzionalità per una migliore e più articolata fruizione delle mappe pubblicate. Ogni mappa è inclusa in una distinta web application configurata ad hoc e può eventualmente essere estesa con altri strati informativi previa specifica configurazione del sistema.

Le funzionalità possono essere concepite come "servizi applicativi" richiamanti alcuni dei "servizi di base" implementati nel sistema come web service composti da metodi atomici.

L'insieme complessivo delle funzionalità disponibili può essere suddiviso in due categorie:

- *funzionalità di base per la navigazione*, disponibili in tutte le applicazioni di consultazione avanzata configurabili nel sistema, di supporto alla navigazione interattiva nella mappa;
- *funzionalità di elaborazione più complesse*, caratterizzate dagli obiettivi più svariati, che possono essere incluse o meno a seconda di come ogni singola applicazione esposta è configurata; per la loro complessità, possono essere definite come "servizi applicativi" in maniera più appropriata.

Nelle tabelle seguenti si intende fornire una panoramica succinta di tutte le funzionalità disponibili nella consultazione avanzata:

Funzionalità di base per la navigazione	
Funzionalità	Descrizione
Zoom in	Ingrandisce un'area della mappa individuata mediante selezione interattiva aumentando il dettaglio e variando la scala di visualizzazione.
Zoom out	Rimpicciolisce un'area della mappa individuata mediante selezione interattiva diminuendo il dettaglio e variando la scala di visualizzazione.
Pan	Trasla il centro di visualizzazione della mappa senza alterare la scala di visualizzazione a seconda di come si è spostata interattivamente la mappa.
Extent precedente	Recupera gli ultimi extent geografici visualizzati.
Extent successivo	Operazione contraria al recupero degli extent precedenti, in conseguenza del quale la funzionalità si attiva.
Extent completo	Recupera l'extent territoriale massimo associato alla mappa visualizzata.
Impostazione della scala di visualizzazione	Consente di impostare la scala di visualizzazione della mappa, esclusivamente selezionandola da un elenco di valori predefiniti comunque modificabile.
Misurazione di distanza o area	Permette di misurare lunghezze o aree sulla mappa disegnando, rispettivamente, delle linee spezzate o dei poligoni.

Funzionalità avanzate sui dati pubblicati	
Nome	Descrizione
Query alfanumeriche tramite query builder	Consente di effettuare query alfanumeriche basate su attributi per un singolo strato alla volta tra quelli caricati nella mappa; le query seguono la sintassi SQL e si definiscono con il supporto di un query builder user-friendly.
Ricerca spaziale	Consente di effettuare query spaziali su un singolo strato alla volta tra quelli caricati nella mappa; vengono intercettati gli oggetti contenenti un punto selezionato o intersecanti un poligono

	disegnato interattivamente sulla mappa; è possibile applicare un buffer all'area disegnata sulla mappa.
Stampa	Consente di inserire la mappa pubblicata all'interno di layout stampabili preimpostati per esportarla in un file pdf; è possibile scegliere se utilizzare la scala corrente o definire un valore preciso; i layout di stampa sono definiti a livello di configurazione dell'applicazione.
Calcolo percorsi	Consente di ricavare la descrizione dettagliata del percorso ottimo che collega N punti di fermata segnati sulla mappa visualizzata; i percorsi sono calcolati rispetto ad un grafo stradale prestabilito.
Localizzazione	Consente di localizzare un riferimento geografico sulla mappa tramite un indirizzo o una coppia di coordinate.
Estrazione dati	Permette l'estrazione di una porzione di territorio secondo il sistema di riferimento desiderato dopo averla scelta; la funzionalità è general-purpose e può essere applicata su una qualsiasi delle mappe pubblicate in consultazione avanzata; i file estratti dinamicamente sono 2D.
Estrazione dati CTR	Permette l'estrazione degli strati informativi della Carta Tecnica Regionale suddivisi per fogli; è un'estrazione mirata che ha senso includere solo in mappe (applicazioni) che visualizzano la Carta Tecnica Regionale; è mutuamente esclusivo rispetto all'estrazione dati generica.
Consultazione catalogo metadati	Consente di attivare la ricerca nel catalogo metadati CNIPA implementato nel SIT Regionale restringendo la ricerca all'extent corrente o effettuandola comunque sull'intero catalogo.
Selezione tematismi	Consente di aggiungere dinamicamente all'interno della mappa uno o più strati informativi tra quelli configurati ad hoc ed abilitati nel sistema per poter essere integrati al volo nelle applicazioni.
Accesso al db documentale	Funzionalità di accesso ai documenti associate agli oggetti geometrici visualizzati nella mappa; attiva una ricerca nel DB documentale incluso nel sistema.
Editing	Consente di effettuare editing geometrico e alfanumerico in maniera separata sugli strati caricati nella mappa.
Procedura editing on line	Consente di effettuare editing geometrico e alfanumerico sugli strati informative configurati nel sistema secondo uno schema di work-flow prestabilito; alle sessioni di lavoro sono associati degli stati opportuni secondo una sequenza predefinita che consente di tenere sottocontrollo l'intero processo da parte degli amministratori del sistema.

Web Services di base

E' possibile accedere ai dati contenuti all'interno del DB del SIT attraverso i web services di base esposti dallo stesso SIT. Questi sono sviluppati con tecnologia J2EE, JAX-WS ed esposti come web services SOAP/XML, descritti secondo lo standard WSDL e catalogati in UDDI. Possono essere pertanto interrogati da client SOAP e utilizzati in altri applicativi. La creazione del Client SOAP e la integrazione dei servizi di base in altri applicativi resta a carico dell'Ente.

L'utilizzo dei web services di base è subordinato all'utilizzo di un account registrato nel SIT. Pertanto, prima che l'Ente possa utilizzare i web services all'interno di proprie applicazioni dovrà inviare formale richiesta al Centro Servizi che provvederà a generare uno userId, ad associarlo all'Ente, a registrarlo nel DB del SIT e a trasmetterlo all'Ente richiedente.

Da questo momento l'Ente sarà autorizzato ad utilizzare i web services di base per accedere ai dati e ai documenti correlati, effettuare operazioni di download, compiere operazioni di tipo generico (inserimento, modifica, cancellazione, query, join...) su dati alfanumerici di tabelle del GeoDatabase, "normalizzare" un indirizzo dato secondo lo standard SIT, di eseguire il calcolo di percorsi e delle Service Area basandosi sul DBTI, estrarre dati geografici nel formato scelto dall'utente, effettuare la compressione di file presenti sul file system dei server del SIT, effettuare proiezioni da un sistema di riferimento ad un altro fra quelli disponibili nel SIT, effettuare operazioni GIS complesse sui layer presenti nel SIT, effettuare operazioni di geoprocessing avanzate. Di seguito sono elencate le funzionalità esposte dai singoli web services:

AccessoDatiGeograficiService: permette l'accesso ai dati geografici, ai layers, ai servizi e permette le operazioni geografiche base.	
Moduli del web service	Descrizione
getServices	richiede ad ArcGIS la lista dei servizi di pubblicazione attivi.
getLayers	richiede ad ArcGIS la lista dei layers di un servizio.
updateLayerCatalog	permette di aggiornare la tabella LAYER_CATALOG
Identify	permette l'interrogazione di tutti i layers selezionati di un dato servizio su ArcGIS server, viene effettuata un'operazione di 'carotaggio' ricercando le features presenti
getMappa	permetta la creazione di una mappa su di un'estensione data e su di un servizio selezionato
estrazioneSingolaFeature	permette l'estrazione in formato XML della componente geografica di una feature data
estrazioneAttributiSingolaFeature	permette l'estrazione in formato XML degli attributi alfanumerici di una feature data.
estrazioneMultiFeature	permette l'estrazione in formato XML della componente geografica di più features
estrazioneAttributiMultiFeature	permette l'estrazione in formato XML degli attributi alfanumerici di più features.
EstrazioneShapefile	permette di estrarre un dato vettoriale presente sul Geodatabase nel formato ESRI shape file
EstrazioneRaster	permette di estrarre un dato raster presente sul Geodatabase nel formato raster TIFF georeferenziati.
EstrazioneUserDefined	permette di estrarre un dato raster o vettoriale presente sul Geodatabase in formato scelto dall'utente

getSupportedFormat	permette di ricevere una lista dei formati supportati dal SIT e degli identificativi relativi
ProiezioneLayerOnLayer	permette di proiettare un layer geografico presente sul SIT su di un nuovo layer. Il layer restituito potrà essere temporaneo o definitivo
ProiezioneFeatureOnLayer	permette di proiettare una feature presente su di un layer geografico
ProiezioneFeature	permette di proiettare una feature qualsiasi passata al metodo come input.
getProjectionIDList	permette di ricevere la lista degli identificativi dei sistemi di riferimento supportati dal SIT.
ClippingFeaturesByFeature	permette di eseguire la funzionalità di Clip su di un layer utilizzando una feature passata in input, il risultato dell'operazione viene salvato su di un layer temporaneo o definitivo.
ClippingLayerByFeatures	permette di eseguire la funzionalità di Clip su di un layer utilizzando una feature passata in input, il risultato dell'operazione viene salvato su di un layer temporaneo o definitivo.
Dissolve	permette di eseguire la funzionalità di Dissolve su di un layer utilizzando uno degli attributi alfanumerici, il risultato dell'operazione viene salvato su di un layer temporaneo o definitivo.
Erase	permette di eseguire la funzionalità di Erase su di un layer utilizzando un altro layer, il risultato dell'operazione viene salvato su di un layer temporaneo o definitivo.
Identity	permette di eseguire la funzionalità di Identity su di un layer utilizzando un altro layer, il risultato dell'operazione viene salvato su di un layer temporaneo o definitivo
Intersect	permette di eseguire la funzionalità di Intersect su più layers, il risultato dell'operazione viene salvato su di un layer temporaneo o definitivo
SpatialJoin	permette di eseguire la funzionalità di Spatial Join fra due layer, il risultato dell'operazione viene salvato su di un layer temporaneo o definitivo.
SymmetricalDifference	permette di eseguire la funzionalità di Symmetrical Difference su di un layer utilizzando un altro layer, il risultato dell'operazione viene salvato su di un layer temporaneo o definitivo
Union	permette di eseguire la funzionalità di Union su più layers, il risultato dell'operazione viene salvato su di un layer temporaneo o definitivo
Update	permette di eseguire la funzionalità di Update su di un layer utilizzando un altro layer, il risultato dell'operazione viene salvato su di un layer temporaneo o definitivo
SelezioneCoppieStereo	permette di eseguire il servizio territoriale di selezione coppie stereo da un elenco di layer
OpDataAlfaService: permette operazioni di tipo generico su dati alfanumerici di tabelle generiche del GeoDatabase, saranno utilizzati in tutti i processi che prevedono accesso generico a tabelle sul geodatabase.	
Moduli del web service	Descrizione
richiestaMetaInformazioni	restituisce le informazioni che descrivono una tabella, compresi i campi e i formati attesi.

CreazioneTabella	permette la creazione di una tabella generica
CancellazioneTabella	permette la cancellazione fisica di una tabella generica
InserimentoDati	permette l'inserimento di dati dentro una tabella generica
ModificaDati	permette la modifica dei dati dentro una tabella generica
Query	interroga una tabella generica e restituisce i risultati trovati
Query2	interroga una tabella generica e restituisce risultati distinti e ordinati
Cancellazione	cancella dei record da una tabella generica
Join	interroga due tabelle generiche eseguendone un join e restituisce i risultati trovati.
Normalizzazione Indirizzo: Il Web service permette di eseguire la normalizzazione e la geocodifica di un indirizzo dato secondo lo standard del progetto.	
Moduli del web service	Descrizione
NormalizzaIndirizzo	interroga il server di Normalizzazione e restituisce i risultati trovati
RicercaIndirizzo	interroga il server di Normalizzazione e Geocodifica e restituisce i risultati trovati.
EliminareCivico	permette l'eliminazione delle informazioni di un civico dalla banca dati del normalizzatore.
EliminareToponimo	permette l'eliminazione delle informazioni di un toponimo dalla banca dati del normalizzatore
NuovoCivico	permette di inserire un nuovo civico nella banca dati del normalizzatore
ModificareCivico	permette di aggiornare le informazioni di un civico dalla banca dati del normalizzatore
ModificareToponimo	Elimina l'anagrafica di una scheda
DownloadStradario	permette di estrarre l'intero database di Normalizzazione nel formato CSV
EstraiStradario	permette di estrarre un Comune all'interno del database di Normalizzazione nel formato XML
NetworkAnalysisService: Il Web service permette di eseguire il calcolo di percorsi e delle Service Area basandosi sul DBTI. Tutte le informazioni presenti, inerenti ai nomi strada, versi di percorrenza e restrizioni, saranno derivate da tale banca dati.	
Moduli del web service	Descrizione
RicercaPercorso	permette di calcolare il percorso più breve fra due punti, con opzionalmente, l'obbligo di passaggio da altri punti
ServiceAreaByTime	permette di calcolare la Service Area, cioè l'area coperta a partire da un punto in un dato lasso di tempo
ServiceAreaByDistance	permette di calcolare la Service Area, cioè l'area coperta a partire da un punto entro una determinata distanza
CompressService: Il Web service permette la compressione di file presenti sul file system dei server SIT.	
CompressFile	Il metodo permette di comprimere uno o più files presenti in una directory accessibile all'utente.
CompressDir	permette di comprimere una directory accessibile all'utente.
DBRegistroAggiornamentiService: saranno utilizzati per l'accesso al DB Registro degli aggiornamenti, essenziale per la gestione dell'aggiornamento del Database con le procedure di editing.	
Moduli del web service	Descrizione
StandAloneActivityInsert	permette l'inserimento di dati dentro la tabella STANDALONE
StandAloneActivityUpdate	permette l'aggiornamento dei dati dentro la tabella STANDALONE
StandAloneActivityQuery	permette l'interrogazione di un record dentro la tabella

	STANDALONE
WebEditingActivityInsert	permette l'inserimento di dati dentro la tabella WEBEDITING
WebEditingActivityUpdate	permette l'aggiornamento dei dati dentro la tabella WEBEDITING
WebEditingActivityQuery	restituisce l'attività richiesta dalla tabella WEBEDITING
RegisterActivityInsert	permette l'inserimento di dati dentro le tabelle SA_REGACTIVITIES e WEB_REGACTIVITIES
QueryActivities	interroga le tabelle SA_REGACTIVITIES e WEB_REGACTIVITIES e restituisce i risultati trovati
AdminQueryDatabase	interroga le tabelle STANDALONE e WEBEDITING con i privilegi di amministratore e restituisce i risultati trovati.
QueryDatabase	interroga le tabelle SA_REGACTIVITIES e WEB_REGACTIVITIES e restituisce i risultati trovati
EditingTracelInsert	esegue una INSERT sulla tabella TRACEDIT
AminEditingTracelInsert	esegue una SELECT sulla vista WEB_REGACTIVITIES con i privilegi di amministratore
DBDocumentaleImplService: Il web service permette l'accesso da parte delle applicazioni ai dati contenuti nel DB Documentale. E' permesso l'inserimento, la cancellazione e l'aggiornamento di documenti di qualunque tipo, purché siano uno streaming di dati binari univoci. Il sistema è in grado di ritrovare documenti utilizzando parole chiave contenute nei metadati che accompagnano l'inserimento di un documento.	
Moduli del web service	Descrizione
InserimentoDocumento	permette l'inserimento di un documento nel DB documentale
downloadDocumento	permette il download di un documento dal DB documentale, la ricerca è effettuata tramite la chiave primaria IDDocumento.
scaricaDocumento	permette il download di un documento dal DB documentale, la ricerca è effettuata tramite la chiave primaria IDDocumento, a differenza del metodo download Documento non è possibile aprire subito lo streaming dei dati ma occorre utilizzare la URL restituita in indirizzo
ricercaDocumentale	permette la ricerca all'interno del database dei documenti che soddisfanno a determinati criteri di ricerca. L'output è un Array di una struttura che contiene tutti i documenti trovati.
aggiornaDocumento	permette l'aggiornamento di un documento già presente nel DB documentale
cancellazioneDocumento	permette la cancellazione di un documento presente nel database, la cancellazione ricerca per chiave primaria
LogOperationService: I seguenti WebServices possono essere utilizzati nelle applicazioni verticali per tracciare operazioni particolari non altrimenti gestite.	
Moduli del web service	Descrizione
LOInserimentoInformazioni	permette l'inserimento dei dati di tracciamento delle operazioni
LORichiestaInformazioni	permette la lettura da parte di un utente delle proprie operazioni effettuate nell'intervallo di due date
LOStatistics	restituisce le statistiche calcolate sulla tabella di tracciamento in base all'intervallo temporale richiesto dall'utente
DataDownloadingService: Il web service consente il download dei file nel formato originale DWG o Raster.	
DownloadFoglio	consente il download dei file nel formato originale DWG o Raster

Servizi a supporto della elaborazione tecnica dei piani e della definizione delle politiche territoriali

Il Sistema mette a disposizione, attraverso il portale www.sit.puglia.it, nella sezione “pianificazione” una serie di funzionalità predisposte per supportare le Amministrazione nella fase di redazione del Piano.

In particolare viene messo a disposizione un ambiente di lavoro personalizzato e riservato per ogni Amministrazione Comunale, suddiviso in più pannelli di gestione:

- ⇒ Gestione Repository
- ⇒ Gestione Servizi di Mappa
- ⇒ Gestione Piani
- ⇒ Gestione Osservazioni

Gestione Repository: consente di personalizzare e gestire il proprio ambiente di lavoro, definendo anche gli accessi.	
Nome Attività	Sintetica Descrizione
Amministrazione Repository	consente di gestire i contenuti del Repository (Schedari, Cartelle) creandone di nuovi, cancellando quelli esistenti o copiando il contenuto
Amministrazione Cartelle	consente di <ul style="list-style-type: none"> ⇒ creare una nuova Cartella o cancellarne una esistente ⇒ cancellarne una esistente o copiare il contenuto ⇒ associare i permessi di Accesso alla Cartella ad un singolo utente
Gestione Contenuti Repository	consente di collezionare Informazioni eterogenee (dati statistici, dati personali in forma di file di qualsiasi tipo, Strati Informativi in forma di file shp, vettoriali in formato dxf) nel Repository, visualizzarle, cancellarle, aggiornarle, scaricarle

<p>Gestione Servizi di Mappa: permette di accedere ad un ambiente GIS web con tutte le funzionalità previste da applicazioni di questo tipo (navigazione mappa, visualizzazione legenda, interrogazione strati informativi e consultazione risultati, ...), oltre che altre specifiche, inserite appositamente per supportare l'Amministrazione nelle fasi di analisi e gestione del territorio.</p>	
Nome Attività	Sintetica Descrizione
<p>Pubblicare Strati Informativi tramite Mappa per gruppo di lavoro interno</p>	<p>consente di</p> <ul style="list-style-type: none"> ⇒ selezionare la Cartella all'interno del Repository in cui caricare gli Strati Informativi per la pubblicazione, Cartella che è accessibile a tutti gli utenti autorizzati alla visualizzazioni ⇒ aggiungere, rinominare o rimuovere gli Strati Informativi destinati alla pubblicazione ⇒ tematizzare gli Strati Informativi destinati alla pubblicazione <p>La pubblicazione avviene tramite Mappa in un ambiente GIS web con tutte le funzionalità previste da applicazioni di questo tipo (navigazione mappa, visualizzazione legenda, interrogazione strati informativi e consultazione risultati, ...), oltre ad altre specifiche</p> <p>E' possibile inoltre:</p> <ul style="list-style-type: none"> ⇒ modificare la Mappa ⇒ cancellare la Mappa ⇒ copiare la Mappa
<p>Tematizzare strati informativi</p>	<p>consente di scegliere per ciascuno strato se tematizzare l'intero Strato con uno stesso tema o se definire temi differenti per intervalli di scala o per intervalli di valori di un determinato campo alfanumerico dello Strato. Inoltre consente di:</p> <ul style="list-style-type: none"> ⇒ definire trasparenza e scala massima/minima per ogni Strato Informativo (e/o degli intervalli di cui sopra); ⇒ associare un tema specifico ad ogni Strato Informativo (e/o degli intervalli di cui sopra) (colore, bordo, riempimento, tipo linea, ...); ⇒ accendere/spegnere Strati Informativi (e/o degli intervalli di cui sopra) nella visualizzazione finale; ⇒ salvare un simbolo o caricarne di precedentemente salvati; ⇒ pubblicare gli Strati Informativi selezionati, lo Strato dedicato alla Gestione delle Segnalazioni e il file di mappa MXD associato con un nome definito dall'utente <p>Nel caso di tematizzazione di intervalli di scala o valore-attributo, è possibile:</p> <ul style="list-style-type: none"> ⇒ definire delle tematizzazioni nulle (colore del tratto e/o di riempimento e bordo trasparente) per uno o più intervalli definiti) ⇒ definire un alias per l'intervallo definito
<p>Elaborare Analisi Aree</p>	<p>a partire dall' ambiente GIS web di pubblicazione (dotato di tutte le funzionalità previste da applicazioni di questo tipo -navigazione mappa, visualizzazione legenda, interrogazione strati informativi e consultazione risultati, ...), consente di effettuare le seguenti operazioni su uno o due</p>

	<p>Strati Informativi selezionati tra quelli pubblicati all'interno del servizio di mappa correntemente in consultazione e sui relativi campi alfanumerici:</p> <ul style="list-style-type: none"> ⇒ effettuare una Ricerca Spaziale, Alfanumerica, ... e salvarne il Risultato ⇒ effettuare Statistiche Semplici su un determinato campo (valore massimo, valore minimo, somma dei valori, media. ⇒ deviazione standard, varianza) ⇒ effettuare Rapporti tra due campi dello stesso Strato Informativo e salvarne il Risultato ⇒ effettuare Operazioni di Join tra due Strati Informativi, filtrare il Risultato e salvarlo ⇒ effettuare Statistiche Aggregate su uno o più Strati Informativi ⇒ unire Strati Informativi (in un unico strato o dissolvendo sulla base di un attributo) <p>consente di selezionare Strati Informativi su cui effettuare analisi, tramite:</p> <ul style="list-style-type: none"> ⇒ definizione alfanumerica (tramite le funzionalità di Analisi Statistica - Interrogazione DB Statistico) ⇒ definizione geometrica (funzionalità di Ricerca in cartografia)
Interrogazione DB Statistico	<p>a partire dall' ambiente GIS web di pubblicazione (dotato di tutte le funzionalità previste da applicazioni di questo tipo -navigazione mappa, visualizzazione legenda, interrogazione strati informativi e consultazione risultati, ...), consente di selezionare il Dato Statistico di interesse utilizzando tre controlli di tipo dropdown-list che vengono aggiornati in cascata ad ogni selezione; definito il Dato, viene visualizzato in forma tabellare il Risultato dell'Interrogazione.</p> <p>A seguito della visualizzazione del Risultato, è possibile creare una join on-the-fly con uno Strato Informativo (ove esistano due campi su cui definire la clausola di join) definendo i seguenti campi:</p> <ul style="list-style-type: none"> ⇒ una colonna della tabella Risultato ⇒ un campo da un determinato Strato Informativo selezionato tra i visualizzati <p>Lo Strato Informativo risultato dalla join può essere salvato</p>
Creare Mappe in Pdf	<p>a partire dall' ambiente GIS web di pubblicazione (dotato di tutte le funzionalità previste da applicazioni di questo tipo -navigazione mappa, visualizzazione legenda, interrogazione strati informativi e consultazione risultati, ...), consente di</p> <ul style="list-style-type: none"> ⇒ selezionare un Titolo ed un Sottotitolo ⇒ utilizzare uno dei template custom presenti a Sistema per la generazione del file PDF ⇒ caricare a Sistema un template precedentemente creato ⇒ eliminare uno dei template precedentemente creati ⇒ selezionare la dimensione del pdf, il suo orientamento e il nome del template ⇒ eseguire l'upload di un file immagine in formato A4 di nome Mascherino.jpg che contenga le informazioni che devono essere stampate nel Mascherino ⇒ scaricare il pdf

<p>Editare Strato Informativo</p>	<p>a partire dall' ambiente GIS web di pubblicazione (dotato di tutte le funzionalità previste da applicazioni di questo tipo -navigazione mappa, visualizzazione legenda, interrogazione strati informativi e consultazione risultati, ...), consente di selezionare lo Strato Informativo sul quale verranno effettuate le modifiche, sia di tipo geometrico che alfanumerico</p>
<p>Assegnare Sistema Proiezione</p>	<p>a partire dall' ambiente GIS web di pubblicazione (dotato di tutte le funzionalità previste da applicazioni di questo tipo -navigazione mappa, visualizzazione legenda, interrogazione strati informativi e consultazione risultati, ...), consente di selezionare lo Strato Informativo al quale si intende assegnare il sistema di proiezione: effettuata la selezione verrà automaticamente popolato il campo relativo al vecchio Sistema di Proiezione (ove presente) e verrà offerta la possibilità di definire il nuovo Sistema di Riferimento da assegnare allo Strato selezionato</p>
<p>Realizzare Nuovo Strato Informativo</p>	<p>a partire dall' ambiente GIS web di pubblicazione (dotato di tutte le funzionalità previste da applicazioni di questo tipo -navigazione mappa, visualizzazione legenda, interrogazione strati informativi e consultazione risultati, ...), consente di creare uno Strato Informativo ex-novo, definendo</p> <ul style="list-style-type: none"> ⇒ nome ⇒ tipo geometria ⇒ sistema di proiezione ⇒ campi alfanumerici dello Strato (nome, tipo, ...) <p>consente di creare uno Strato Informativo da Strato esistente (il sistema di proiezione sarà ereditato dallo Strato esistente; sarà eventualmente compito dell'utente modificare il sistema di proiezione associato), definendo:</p> <ul style="list-style-type: none"> ⇒ nome ⇒ Strato Informativo di partenza ⇒ contenuti del nuovo Strato (tutte le feature dello Strato di partenza o solo quelle correntemente selezionate)
<p>Effettuare Ricerca</p>	<p>a partire dall' ambiente GIS web di pubblicazione (dotato di tutte le funzionalità previste da applicazioni di questo tipo -navigazione mappa, visualizzazione legenda, interrogazione strati informativi e consultazione risultati, ...), è possibile utilizzare diverse funzionalità:</p> <ul style="list-style-type: none"> ⇒ Selezione Manuale ⇒ Selezionare Da Mappa ⇒ Ricerca Spaziale ⇒ Ricerca Alfanumerica
<p>Servizi Correlati</p>	<p>consente di selezionare il servizio di mappa master e il servizio di mappa slave tra due differenti servizi di mappa presenti all'interno della Cartella e utilizzarli per comporre la vista di entrambi i servizi all'interno di uno stesso GIS Web di pubblicazione (dotato di tutte le funzionalità previste da applicazioni di questo tipo -navigazione mappa, visualizzazione legenda, interrogazione strati informativi e consultazione risultati, ...), al fine di:</p> <ul style="list-style-type: none"> ⇒ propagare azioni di navigazione e interrogazione mappa sul servizio master ⇒ invertire i servizi di master e slave per effettuare navigazioni e

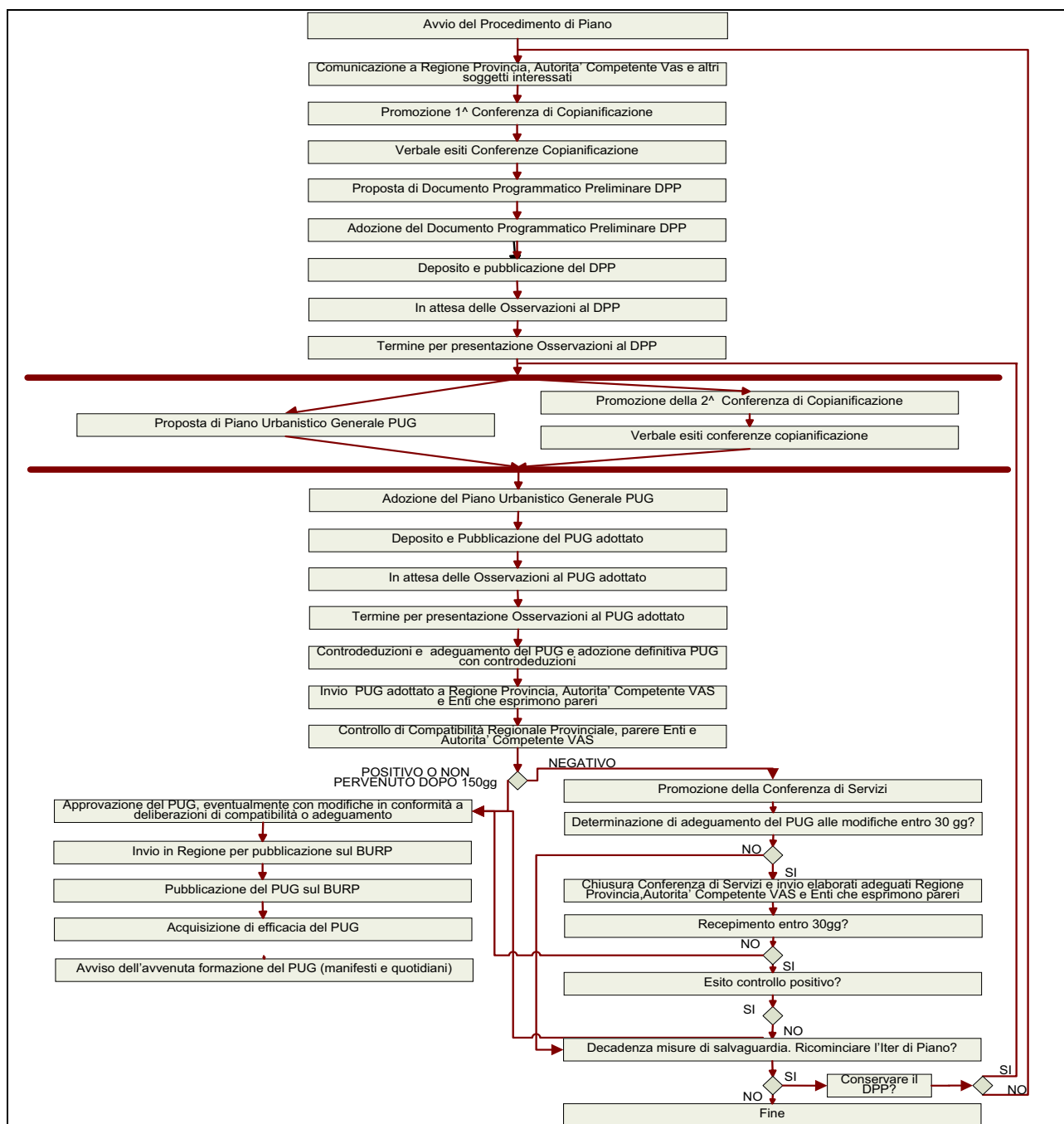
	<p>interrogazioni sul entrambi i servizi ⇒ spegnere singoli Strati Informativi.</p>
--	--

Gestione Piani: permette di accedere a funzioni di supporto all'elaborazione dei Piani, facilitandone la gestione informatizzata, a partire dalle funzionalità specifiche dei pannelli di gestione prima descritti. In particolare, nel caso dell'elaborazione di un PUG è stato implementato un workflow management dell'intero iter di piano, in conformità alla normativa, inclusa la fase delle segnalazione e delle osservazioni, della cooperazione interistituzionale e della partecipazione pubblica. Nell'ambiente, inoltre, vengono messe a disposizione sia tutti gli strati informativi di base realizzati nell'Ambito del Progetto SIT Puglia, che quelle relativi alla Pianificazione Sovraordinata (disponibili al SIT Puglia), relativi al territorio di competenza di ciascuna Amministrazione. Vengono resi disponibili, inoltre, gli strati informativi minimi richiesti per il PUG informatizzato, che vengono caricati automaticamente nel Sistema secondo il formato definito dalle "Istruzioni Tecniche".

Nome Attività	Sintetica Descrizione
Procedimento Redazione Piano	<p>consente di eseguire fisicamente l'Avvio del Procedimento, selezionando il tipo di piano (nell'elenco di quelli disponibili), inserendo i dati generali del Piano ed avviando l'iter procedurale ove disponibile.</p> <p>Inoltre consente di</p> <ul style="list-style-type: none"> ⇒ cancellare un Piano ⇒ far avanzare il piano secondo l'Iter e le relative funzionalità predefinite (si veda descrizione seguente) ⇒ visualizzare i piani attivi (con la possibilità di visualizzare in dettaglio le informazioni connesse al Piano selezionato)
Gestire Strati Informativi Del PUG	<p>consente di procedere alle operazioni di editing degli Strati Informativi minimi previsti dalle "Istruzioni Tecniche", sia di tipo geometrico che alfanumerico (nel qual caso, in riferimento alle categorie "chiusure" il Sistema precarica gli attributi possibili tra cui l'utente deve scegliere)</p>
Gestire Relazione	<p>consente, nel caso di un Piano a cui sia associato un Iter che prevede una Relazione, di:</p> <ul style="list-style-type: none"> ⇒ creare una nuova Relazione caricando a Sistema un file testuale precedentemente creato dall'utente sul proprio desktop ⇒ caricare gli allegati associati alla Relazione. ⇒ modificare una Relazione (come download del file testuale, eventuale modifica lato desktop utente e successivo caricamento) per sovrascrivere la versione precedente ⇒ stampare una Relazione (come download della relazione e/o dei singoli file allegati e successivamente dell'invio alla stampa) ⇒ salvare una Relazione in formato PDF (come download della relazione e degli eventuali allegati e nella generazione dei file PDF a lato desktop; tali file potranno poi essere caricati a Sistema all'interno della Relazione corrente) ⇒ inviare la relazione in Regione (consiste nella definizione di destinatari e-mail e testo dell'e-mail cui saranno allegati la

	Relazione e gli Allegati associati)
Pubblicare Strati Informativi all'esterno	consente di definire del Servizio di Mappa pubblicato verso l'esterno, specificandone nome. Questo Servizio è, quindi, disponibile alla funzionalità di Inserimento Segnalazioni da parte di un utente generico. La pubblicazione avviene in un ambiente GIS web con tutte le funzionalità previste da applicazioni di questo tipo (navigazione mappa, visualizzazione legenda, interrogazione strati informativi e consultazione risultati, ...), oltre che quelle specifiche
Analisi Segnalazione	a partire dall' ambiente GIS web di pubblicazione (dotato di tutte le funzionalità previste da applicazioni di questo tipo -navigazione mappa, visualizzazione legenda, interrogazione strati informativi e consultazione risultati, ...), consente di analizzare le segnalazioni inserite da altri utenti

L'iter di Piano del PUG è stato configurato, secondo quanto definito dalla normativa di riferimento, come segue:



Sono inoltre stati predisposti altri Iter relativi al PUG per i Piani che erano già in corso di elaborazione al momento della definizione delle Linee Guida regionali, secondo la normativa di riferimento.

In particolare gli Iter di Piano predisposti per il PUG consentono di seguire e agevolare il processo, prevedendo, a seconda dei diversi momenti previsti:

- ⇒ definizione e inserimento di informazioni specifiche
- ⇒ archiviazione (inserendo note e altre informazioni specifiche, aggiungendo allegati)
- ⇒ invio e-mail (con la possibilità di gestire una mail-list, inserire allegati, inviare link)
- ⇒ avanzamento di stato (automatico o manuale)
- ⇒ attivazione servizio segnalazione tra enti
- ⇒ attivazione servizio segnalazione pubblico
- ⇒ elaborazioni statistiche

Dati catastali

Il SIT adotta il modello logico e fisico del DBTI di SigmaTer, già verificato con l'Agenzia del Territorio, sperimentato da diversi Comuni e aderente agli standard di riferimento del progetto PR5SIT (Db topografico dell'IntesaGIS e metadati ISO TC 211-19115 con gli adattamenti previsti dall'IntesaGIS). Nello specifico, attraverso un accordo con la Regione Emilia Romagna, il SIT riusa sia il modello dei dati che i servizi di accesso al dato.

SigmaTER nasce per facilitare il processo di decentramento catastale e per migliorare la capacità di pianificazione, di gestione amministrativa e fiscale del territorio, nonché migliorare la qualità dei servizi per cittadini, professionisti ed imprese che necessitano di integrare le informazioni catastali con quelle territoriali.

Le informazioni catastali vengono condivise tramite il sistema di interscambio, composto da un modulo dell'Agenzia del Territorio ed uno regionale, raccolte ed integrate a livello regionale all'interno di un Database Territoriale Integrato e rese disponibili dalla Regione mediante i servizi di backoffice. Tali servizi offrono una serie di funzionalità elementari sulla base delle quali sono realizzate e messe a disposizione degli Enti Locali le cosiddette applicazioni General Purpose per la consultazione nel DBTI regionale dei dati catastali (censuario e cartografico).

Applicazioni General Pur pose

Le applicazioni General Purpose sono erogate direttamente dal portale del SIT ed utilizzano esclusivamente le informazioni presenti nel DataBase Territoriale Integrato (DBTI) a livello regionale. Non possono quindi sostituirsi alle applicazioni che devono essere sviluppate dagli Enti Locali per gli adempimenti ad essi in carico. Tuttavia, in assenza di applicazioni locali specifiche, gli Enti Locali possono utilizzare le applicazioni General Purpose per estrarre dal DBTI le informazioni necessarie alla evasione manuale delle pratiche.

Di seguito una sintesi delle applicazioni general purpose rese disponibili attraverso il portale SIT come riuso di SigmaTER.

Navigazione cartografica interattiva nel Dbti	Il servizio consente di consultare attraverso un normale browser la banca dati catastale congiuntamente ad informazioni territoriali tecniche ed urbanistiche, effettuando interrogazioni puntuali e spaziali sulle banche dati disponibili e accedendo alle fonti informative cartografiche ed alfanumeriche disponibili.
Informazioni ICI	Il servizio fornisce le informazioni necessarie alle comunicazioni/denunce ICI ed al pagamento dell'ICI.
Accertamento ICI	Il servizio permette di reperire a partire da diverse chiavi di ricercate informazioni presenti nel database necessarie all'attività di accertamento dell'evasione dell'ICI

Accertamento Tarsu	Il servizio permette di reperire le informazioni presenti nel database necessarie all'attività di accertamento della evasione della TARSU.
Consultazione catastale estesa (terreni, fabbricati e soggetti)	Il servizio consente di reperire informazioni catastali, senza valenza legale, relativamente alla situazione oggettiva e alla titolarità di particelle catastali o di Unità Immobiliari Urbane. La consultazione può prevedere il reperimento della sola situazione oggettiva e/o titolarità attuale o storica.
Scarico dati nativi catastali	Il servizio consente il download sui sistemi informativi dell'utente degli scarichi nativi relativi al Comune in un periodo di tempo specificato. L'utente fornisce al sistema il Comune di riferimento, la tipologia di dati e l'intervallo temporale in anni e ottiene la lista degli scarichi da cui può effettuare il download di quelli di interesse.
Recupero Planimetrie disponibili su esplicita delega del Comune	Il servizio consente di visualizzare e stampare le planimetrie per una Unità Immobiliare Urbana, laddove tale informazione sia presente nel database. L'utente fornisce al sistema i dati identificativi dell'UIU e il formato di immagine che desidera (JPEG o PNG).
Recupero foglio raster	Il servizio consente il recupero di tutta la cartografia in formato raster presente nel database relativa ad un foglio di mappa catastale. L'utente fornisce al sistema i dati identificativi di un foglio di mappa catastale ed ottiene il download di tutte le sezioni registrate nel database in formato PNG.
Estrazione mappe catastali per Certificato di Destinazione Urbanistica (Cdu)	Il servizio consente la stampa dell'estratto di mappa catastale e le relative informazioni dimensionali secondo diverse modalità di emissione (scala, formato, temi). L'utente fornisce al sistema i dati identificativi di una o più particelle, specifica i temi aggiuntivi (Strade, Confini, Acque, Centroidi) e la Maggiorazione, e richiede un formato per la risposta che può essere sia raster (PDF o immagine) che vettoriale, dimensioni della pagina e fattore di scala.
Ricerca ed estrazione di metadati	Il servizio consente la ricerca dei metadati, memorizzati nel DBTI secondo le specifiche ISO 19115, seguendo le specifiche della direttiva Europea INSPIRE. I metadati possono essere consultati in maniera estesa o solo per il "Core Metadata" e possono essere importati od esportati secondo alcuni profili definiti a livello italiano.



Unione Europea
FESR



Ministro
per l'Innovazione
e le Tecnologie

Piano Nazionale di e-Government



Regione Puglia – POR 2000-2006

ALLEGATO 4

Istruzioni Tecniche per la informatizzazione dei Piani Urbanistici Generali (PUG) nell'ambito del SIT Regionale

Modello fisico

***BANCA DATI DEGLI STRATI INFORMATIVI
DEL PIANO URBANISTICO GENERALE***

SIT REGIONALE

Indice

1	Introduzione.....	738
2	Analisi delle tabelle relazionali	739
2.1	SIT_PUG41G_IS_GM.....	739
2.2	SIT_PUG42G_IS_SC.....	740
2.3	SIT_PUG43G_IS_PA.....	740
2.4	SIT_PUG44G_IS_AP.....	741
2.5	SIT_PUG52G_IS.....	742
2.6	SIT_PUG45G_INF.....	743
2.7	SIT_PUG49G_CT.....	745
2.8	SIT_PUG63G_PREV_PROGRAMMATICHE.....	746
2.9	SIT_PUG01G_PAI_PG.....	748
2.10	SIT_PUG03G_PAI_PI.....	749
2.11	SIT_PUG05G_PAI_R.....	750
2.12	SIT_PUG07G_PUTT_ATDGEOL.....	752
2.13	SIT_PUG10G_PUTT_ATDGROTT.....	753
2.14	SIT_PUG57G_PUTT_ATDGROTT_P.....	754
2.15	SIT_PUG13G_PUTT_ATDCOSTE.....	756
2.16	SIT_PUG74G_PUTT_ATDIDRO_BACINO.....	757
2.17	SIT_PUG15G_PUTT_ATDIDRO_CORSO.....	758
2.18	SIT_PUG58G_PUTT_ATDIDRO_L.....	759
2.19	SIT_PUG70G_PUTT_ATDIDRO_P.....	761
2.20	SIT_PUG19G_PUTT_ATDVECRI.....	761
2.21	SIT_PUG72G_PUTT_ATDVECRI_L.....	763
2.22	SIT_PUG22G_PUTT_ATDBOMA.....	763
2.23	SIT_PUG24G_PUTT_ATDNATUR.....	765
2.24	SIT_PUG26G_PUTT_ATDBEDI.....	766
2.25	SIT_PUG71G_PUTT_ATDBEDI_L.....	767
2.26	SIT_PUG28G_PUTT_ATDBECU.....	768
2.27	SIT_PUG60G_PUTT_ATDBECU_P.....	769
2.28	SIT_PUG77G_PUTT_ATDBECU_L.....	770
2.29	SIT_PUG31G_PUTT_ATDPAGRI.....	771
2.30	SIT_PUG33G_PUTT_ATDCIVIC.....	772
2.31	SIT_PUG69G_PUTT_ATDAREEPA.....	774
2.32	SIT_PUG35G_PUTT_ATDPUPA.....	774
2.33	SIT_PUG36G_PUTT_ATDSTRAP.....	775
2.34	SIT_PUG37G_PUTT_ATE.....	776
2.35	SIT_PUG39G_PUTT_TC.....	777
2.36	SIT_PUG79G_VINCOLI.....	777
3	Contenuto delle tabelle dei domini codificati	779
3.1	SIT_PUG46T_C_CLASSE_INF.....	779
3.2	SIT_PUG47T_C_TIPO_INF.....	779
3.3	SIT_PUG48T_C_STA_FATTO_INF.....	779
3.4	SIT_PUG50T_C_AMBITO.....	779
3.5	SIT_PUG51T_C_TIPO_CT.....	779
3.6	SIT_PUG64T_C_MOD_ATT_PP.....	780
3.7	SIT_PUG65T_C_AMB_APPL_PP.....	780
3.8	SIT_PUG66T_C_ARCO_VAL_PP.....	780
3.9	SIT_PUG02T_C_CLASSE_PAI_PG.....	780
3.10	SIT_PUG04T_C_CLASSE_PAI_PI.....	780
3.11	SIT_PUG06T_C_CLASSE_PAI_R.....	780
3.12	SIT_PUG08T_C_CLASSE_ATDGEOL.....	781
3.13	SIT_PUG09T_C_TIPO_PUTT.....	781

3.14	SIT_PUG12T_C_MOD_PUTT.....	781
3.15	SIT_PUG54T_C_MOD_PUTT_A.....	781
3.16	SIT_PUG55T_C_MOD_PUTT_L.....	781
3.17	SIT_PUG56T_C_MOD_PUTT_P.....	782
3.18	SIT_PUG11T_C_CLASSE_ATDGROTTE.....	782
3.19	SIT_PUG14T_C_CLASSE_ATDCOSTE.....	782
3.20	SIT_PUG18T_C_TIPO_ADTDCOSTE.....	782
3.21	SIT_PUG73T_C_DESC_CI_ATDCOSTE.....	782
3.22	SIT_PUG75T_C_CLASSE_ATDIDRO_BACINO.....	783
3.23	SIT_PUG76T_C_DESC_CI_ATDIDROB.....	783
3.24	SIT_PUG16T_C_CLASSE_ATDIDRO_CORSO.....	783
3.25	SIT_PUG75T_C_DESC_CI_ATDIDROC.....	783
3.26	SIT_PUG59T_C_CLASSE_ATDIDRO_L.....	783
3.27	SIT_PUG78T_C_DESC_CI_ATDIDRO_L.....	784
3.28	SIT_PUG17T_C_PROPR_ATDIDRO.....	784
3.29	SIT_PUG20T_C_CLASSE_ATDVECRI.....	784
3.30	SIT_PUG21T_C_TIPO_ATDVECRI.....	784
3.31	SIT_PUG23T_C_CLASSE_ATDBOMA.....	784
3.32	SIT_PUG25T_C_CLASSE_ATDNATURA.....	784
3.33	SIT_PUG27T_C_CLASSE_ATDBEDI.....	785
3.34	SIT_PUG29T_C_CATEG_ATDBECU.....	785
3.35	SIT_PUG53T_C_PERIM_ATDBECU.....	785
3.36	SIT_PUG30T_C_CLASSE_ATDBECU.....	785
3.37	SIT_PUG67T_C_CATEG_ATDBECU_L_P.....	786
3.38	SIT_PUG32T_C_CLASSE_ATDPAGRI.....	786
3.39	SIT_PUG34T_C_CLASSE_ATDCIVICI.....	787
3.40	SIT_PUG68T_C_RIF_CL_INT.....	787
3.41	SIT_PUG38T_C_CLASSE_PUTT_ATE.....	787
3.42	SIT_PUG40T_C_CLASSE_PUTT_TC.....	787
3.43	SIT_PUG80T_TIPO_VINCOLO.....	787
4	Analisi delle tabelle di decodifica.....	789
4.1	SIT_PUG46T_C_CLASSE_INF.....	789
4.2	SIT_PUG47T_C_TIPO_INF.....	789
4.3	SIT_PUG48T_C_STA_FATTO_INF.....	789
4.4	SIT_PUG50T_C_AMBITO.....	790
4.5	SIT_PUG51T_C_TIPO_CT.....	790
4.6	SIT_PUG64T_C_MOD_ATT_PP.....	791
4.7	SIT_PUG65T_C_AMB_APPL_PP.....	791
4.8	SIT_PUG66T_C_ARCO_VAL_PP.....	791
4.9	SIT_PUG02T_C_CLASSE_PAI_PG.....	792
4.10	SIT_PUG04T_C_CLASSE_PAI_PI.....	792
4.11	SIT_PUG06T_C_CLASSE_PAI_R.....	793
4.12	SIT_PUG08T_C_CLASSE_ATDGEOL.....	793
4.13	SIT_PUG09T_C_TIPO_PUTT.....	794
4.14	SIT_PUG11T_C_CLASSE_ATDGROTTE.....	794
4.15	SIT_PUG12T_C_MOD_PUTT.....	795
4.16	SIT_PUG54T_C_MOD_PUTT_A.....	795
4.17	SIT_PUG54T_C_MOD_PUTT_L.....	796
4.18	SIT_PUG54T_C_MOD_PUTT_P.....	796
4.19	SIT_PUG14T_C_CLASSE_ATDCOSTE.....	796
4.20	SIT_PUG18T_C_TIPO_ADTDCOSTE.....	797
4.21	SIT_PUG16T_C_CLASSE_ATDIDRO_CORSO.....	797
4.22	SIT_PUG59T_C_CLASSE_ATDIDRO_L.....	798
4.23	SIT_PUG17T_C_PROPR_ATDIDRO.....	798
4.24	SIT_PUG20T_C_CLASSE_ATDVECRI.....	798

4.25	SIT_PUG21T_C_TIPO_ATDVECRI.....	791
4.26	SIT_PUG23T_C_CLASSE_ATDBOMA.....	791
4.27	SIT_PUG25T_C_CLASSE_ATDNATURA.....	800
4.28	SIT_PUG27T_C_CLASSE_ATDBEDI.....	800
4.29	SIT_PUG67T_C_CATEG_ATDBECU_L_P.....	801
4.30	SIT_PUG29T_C_CATEG_ATDBECU.....	801
4.31	SIT_PUG53T_C_PERIM_ATDBECU.....	801
4.32	SIT_PUG30T_C_CLASSE_ATDBECU.....	802
4.33	SIT_PUG32T_C_CLASSE_ATDPAGRI.....	803
4.34	SIT_PUG34T_C_CLASSE_ATDCIVICI.....	803
4.35	SIT_PUG38T_C_CLASSE_PUTT_ATE.....	803
4.36	SIT_PUG40T_C_CLASSE_PUTT_TC.....	804
4.37	SIT_PUG68T_C_RIF_CL_INT.....	804
4.38	SIT_PUG73T_C_DESC_CI_ATDCOSTE.....	805
4.39	SIT_PUG75T_C_DESC_CI_ATDIDROC.....	805
4.40	SIT_PUG76T_C_DESC_CI_ATDIDROB.....	805
4.41	SIT_PUG78T_C_DESC_CI_ATDIDRO_L.....	806
4.42	SIT_PUG80T_TIPO_VINCOLO.....	806
5	Ulteriori osservazioni e vincoli.....	808
5.1	Osservazioni sui vincoli topologici.....	808
5.2	Osservazioni sul valore Booleano.....	808
5.3	Campi richiesti nell' introduzione di nuovi strati.....	808

1 Introduzione

Obiettivo del presente documento è fornire una descrizione di dettaglio del modello relazionale progettato per la gestione degli strati informativi che costituiscono alcuni degli elaborati del Piano Urbanistico Generale.

Il documento descrive infatti le modalità con cui gli strati informativi descritti nel modello logico si traducono in layer fisici GIS, ossia singoli archivi indipendenti caratterizzati da geometrie con associate un tracciato record alfanumerico (modello fisico).

Per ogni layer introdotto vengono specificati:

- i campi che costituiscono la chiave primaria (con i nomi che fisicamente occorrerà assegnare loro)
- la tipologia del campo geometrico (se areale, poligonale o puntuale)
- tutti gli eventuali campi aggiuntivi che completano il tracciato record (con i nomi fisici dei campi)

Per ogni campo, inoltre, oltre al nome fisico, è specificato il tipo e l'obbligatorietà.

Il documento è comprensivo anche delle descrizioni delle voci presenti in tutti i domini codificati, per tutti i campi che ne fanno uso.

Ogni paragrafo relativo a ciascun layer contiene il riferimento allo strato informativo logico che implementa, garantendo un buon livello di tracciabilità tra entità logiche del modello logico e layer del modello fisico; questo incrementa, peraltro, la leggibilità modello fisico.

2 Analisi delle tabelle relazionali

Come premessa all'esame delle tabelle relazionali, si specifica che le tabelle relazionali sono tutte di natura geometrica, eccetto quelle deputate ad ospitare dei domini per valori codificati; le tabelle geometriche memorizzano strati informativi suddivisi per Comune. Il nome reale di ciascuna tabella fisica si ottiene concatenando il codice ISTAT del comune preceduto da “_” a quelli generali introdotti. Le tabelle dei domini non si intendono duplicate.

2.1 SIT_PUG41G_IS_GM

Descrizione

La tabella è di natura geometrica e contiene lo strato informativo relativo alle **invarianti strutturali geo-morfo-idrologiche**, nucleo essenziale del Piano Urbanistico Generale. Gli oggetti geometrici sono poligonali.

Riferimento alle “Linee Guida” DRAG/PUG

PARTE IV - Il Piano Urbanistico Generale, Parte Strutturale (PUG/S).

Regole di editing

Gli strati informativi delle discipline dei singoli sistemi di invarianti strutturali sono costituiti da areali sovrapponibili tra di loro, ogni parte del territorio può essere infatti interessata da nessuna, una o più invarianti allo stesso tempo. Lo strato informativo inerente i sistemi di Invarianti geomorfo-idrologiche non copre necessariamente l'intero territorio comunale potendo esserci elementi non interessati da poligoni. Ad ogni areale individuato deve essere associato un insieme di attributi (informazioni) che lo identifichino e ne descrivano le caratteristiche.

Relazioni principali

La tabella non è coinvolta in relazioni rilevanti.

Campi

Chiavi primarie			
FILE_ID	Identificativo numerico univoco che contraddistingue ogni geometria nell'ambito della tabella.	Intero lungo	Obbligatorio
COD_ISTAT	Codice ISTAT del Comune al quale lo strato informativo si riferisce.	Stringa max 6 caratteri	Obbligatorio
Campi geometrici			
SHAPE	Campo geometrico poligonale relativo ad una singola istanza dello strato informativo; le geometrie sono 2D.	Tipo geometrico binario	Obbligatorio
Campi ulteriori			
DESCRIZION	Descrizione sintetica dell'invariante corrispondente alla singola geometria.	Stringa max 255 caratteri (testo libero)	Obbligatorio
RISCHI	Valutazione dei rischi a cui è soggetta l'invariante.	Stringa max 255 caratteri (testo libero)	Obbligatorio
OPPORTUN	Valutazione circa le potenzialità dell'ambito.	Stringa max 255 caratteri (testo libero)	Obbligatorio
RIFERIMENT	Riferimento al paragrafo o articolo degli “indirizzi e direttive strutturali” del PUG.	Stringa max 255 caratteri (testo libero)	Obbligatorio

DISCIPLINA	Sintesi della disciplina da applicarsi all'invariante.	Stringa max 255 caratteri (testo libero)	Obbligatorio
------------	--	--	--------------

2.2 SIT_PUG42G_IS_SC

Descrizione

La tabella è di natura geometrica e contiene lo strato informativo relativo alle **invarianti strutturali storico-culturali**, nucleo essenziale del Piano Urbanistico Generale. Gli oggetti geometrici sono poligonali.

Riferimento alle "Linee Guida" DRAG/PUG

PARTE IV - Il Piano Urbanistico Generale, Parte Strutturale (PUG/S).

Regole di editing

Gli strati informativi delle discipline dei singoli sistemi di invarianti strutturali sono costituiti da areali sovrapponibili tra di loro, ogni parte del territorio può essere infatti interessata da nessuna, una o più invarianti allo stesso tempo. Lo strato informativo inerente i sistemi di Invarianti storico-culturali non copre necessariamente l'intero territorio comunale potendo esserci elementi non interessati da poligoni. Ad ogni areale individuato deve essere associato un insieme di attributi (informazioni) che lo identifichino e ne descrivano le caratteristiche.

Relazioni principali

La tabella non è coinvolta in relazioni rilevanti.

Campi

Chiavi primarie			
FILE_ID	Identificativo numerico univoco che contraddistingue ogni geometria nell'ambito della tabella.	Intero lungo	Obbligatorio
COD_ISTAT	Codice ISTAT del Comune al quale lo strato informativo si riferisce.	Stringa max 6 caratteri	Obbligatorio
Campi geometrici			
SHAPE	Campo geometrico poligonale relativo ad una singola istanza dello strato informativo; le geometrie sono 2D.	Tipo geometrico binario	Obbligatorio
Campi ulteriori			
DESCRIZION	Descrizione sintetica dell'invariante corrispondente alla singola geometria.	Stringa max 255 caratteri (testo libero)	Obbligatorio
RISCHI	Valutazione dei rischi a cui è soggetta l'invariante.	Stringa max 255 caratteri (testo libero)	Obbligatorio
OPPORTUN	Valutazione circa le potenzialità dell'ambito.	Stringa max 255 caratteri (testo libero)	Obbligatorio
RIFERIMENT	Riferimento al paragrafo o articolo degli "indirizzi e direttive strutturali" del PUG.	Stringa max 255 caratteri (testo libero)	Obbligatorio
DISCIPLINA	Sintesi della disciplina da applicarsi all'invariante.	Stringa max 255 caratteri (testo libero)	Obbligatorio

2.3 SIT_PUG43G_IS_PA

Descrizione

La tabella è di natura geometrica e contiene lo strato informativo relativo alle **invarianti**

strutturali paesistico-ambientali, nucleo essenziale del Piano Urbanistico Generale.
Gli oggetti geometrici sono poligonali.

Riferimento alle "Linee Guida" DRAG/PUG

PARTE IV - Il Piano Urbanistico Generale, Parte Strutturale (PUG/S).

Regole di editing

Gli strati informativi delle discipline dei singoli sistemi di invarianti strutturali sono costituiti da areali sovrapponibili tra di loro, ogni parte del territorio può essere infatti interessata da nessuna, una o più invarianti allo stesso tempo. Lo strato informativo inerente i sistemi di Invarianti paesistico-ambientali non copre necessariamente l'intero territorio comunale potendo esserci elementi non interessati da poligoni. Ad ogni areale individuato deve essere associato un insieme di attributi (informazioni) che lo identifichino e ne descrivano le caratteristiche.

Relazioni principali

La tabella non è coinvolta in relazioni rilevanti.

Campi

Chiavi primarie			
FILE_ID	Identificativo numerico univoco che contraddistingue ogni geometria nell'ambito della tabella.	Intero lungo	Obbligatorio
COD_ISTAT	Codice ISTAT del Comune al quale lo strato informativo si riferisce.	Stringa max 6 caratteri	Obbligatorio
Campi geometrici			
SHAPE	Campo geometrico poligonale relativo ad una singola istanza dello strato informativo; le geometrie sono 2D.	Tipo geometrico binario	Obbligatorio
Campi ulteriori			
DESCRIZION	Descrizione sintetica dell'invariante corrispondente alla singola geometria.	Stringa max 255 caratteri (testo libero)	Obbligatorio
RISCHI	Valutazione dei rischi a cui è soggetta l'invariante.	Stringa max 255 caratteri (testo libero)	Obbligatorio
OPPORTUN	Valutazione circa le potenzialità dell'ambito.	Stringa max 255 caratteri (testo libero)	Obbligatorio
RIFERIMENT	Riferimento al paragrafo o articolo degli "indirizzi e direttive strutturali" del PUG.	Stringa max 255 caratteri (testo libero)	Obbligatorio
DISCIPLINA	Sintesi della disciplina da applicarsi all'invariante.	Stringa max 255 caratteri (testo libero)	Obbligatorio

2.4 SIT_PUG44G_IS_AP

Descrizione

La tabella è di natura geometrica e contiene lo strato informativo relativo alle **invarianti strutturali attinenti aree protette, SIC, ZPS e IBA**, nucleo essenziale del Piano Urbanistico Generale.
Gli oggetti geometrici sono poligonali.

Riferimento alle "Linee Guida" DRAG/PUG

PARTE IV - Il Piano Urbanistico Generale, Parte Strutturale (PUG/S).

Regole di editing

Gli strati informativi delle discipline dei singoli sistemi di invarianti strutturali sono costituiti da areali sovrapponibili tra di loro, ogni parte del territorio può essere infatti interessata da nessuna, una o più invarianti allo stesso tempo. Lo strato informativo inerente i sistemi di Invarianti relative alle aree protette, SIC, ZPS non copre necessariamente l'intero territorio comunale potendo esserci elementi non interessati da poligoni. Ad ogni areale individuato deve essere associato un insieme di attributi (informazioni) che lo identifichino e ne descrivano le caratteristiche.

Relazioni principali

La tabella non è coinvolta in relazioni rilevanti.

Campi

Chiavi primarie			
FILE_ID	Identificativo numerico univoco che contraddistingue ogni geometria nell'ambito della tabella.	Intero lungo	Obbligatorio
COD_ISTAT	Codice ISTAT del Comune al quale lo strato informativo si riferisce.	Stringa max 6 caratteri	Obbligatorio
Campi geometrici			
SHAPE	Campo geometrico poligonale relativo ad una singola istanza dello strato informativo; le geometrie sono 2D.	Tipo geometrico binario	Obbligatorio
Campi ulteriori			
DESCRIZION	Descrizione sintetica dell'invariante corrispondente alla singola geometria.	Stringa max 255 caratteri (testo libero)	Obbligatorio
RISCHI	Valutazione dei rischi a cui è soggetta l'invariante.	Stringa max 255 caratteri (testo libero)	Obbligatorio
OPPORTUN	Valutazione circa le potenzialità dell'ambito.	Stringa max 255 caratteri (testo libero)	Obbligatorio
RIFERIMENT	Riferimento al paragrafo o articolo degli "indirizzi e direttive strutturali" del PUG.	Stringa max 255 caratteri (testo libero)	Obbligatorio
DISCIPLINA	Sintesi della disciplina da applicarsi all'invariante.	Stringa max 255 caratteri (testo libero)	Obbligatorio

2.5 SIT_PUG52G_IS**Descrizione**

La tabella è di natura geometrica e contiene lo strato informativo relativo ad una **sintesi complessiva delle invarianti strutturali** definite nell'ambito di un dato Comune, nucleo essenziale del Piano Urbanistico Generale.

Gli oggetti geometrici sono poligonali.

Riferimento alle "Linee Guida" DRAG/PUG

PARTE IV - Il Piano Urbanistico Generale, Parte Strutturale (PUG/S).

Regole di editing

Lo strato informativo di sintesi delle invarianti strutturali è costituito da areali non sovrapponibili tra di loro, tuttavia lo strato informativo non copre necessariamente l'intero territorio comunale potendo esserci elementi non interessati da poligoni. Lo strato informativo deriva dalla sovrapposizione dei diversi sistemi di invarianti strutturali, mettendoli in relazione tra loro e considerandone le interazioni. Ad ogni areale individuato deve essere associato un insieme di

attributi (informazioni) che lo identifichino e ne descrivano le caratteristiche.

Relazioni principali

La tabella è coinvolta in relazioni di decodifica con tabelle dei domini.

Campi

Chiavi primarie			
FILE_ID	Identificativo numerico univoco che contraddistingue ogni geometria nell'ambito della tabella.	Intero lungo	Obbligatorio
COD_ISTAT	Codice ISTAT del Comune al quale lo strato informativo si riferisce.	Stringa max 6 caratteri	Obbligatorio
Campi geometrici			
SHAPE	Campo geometrico poligonale relativo ad una singola istanza dello strato informativo; le geometrie sono 2D.	Tipo geometrico binario	Obbligatorio
Campi ulteriori			
INV_IS_GM	Vero se la geometria interseca invarianti di tipo geo-morfologico.	Booleano	Obbligatorio
INV_IS_SC	Vero se la geometria interseca invarianti di tipo storico-culturali.	Booleano	Obbligatorio
INV_IS_PA	Vero se la geometria interseca invarianti di tipo paesistico-ambientale.	Booleano	Obbligatorio
INV_IS_AP	Vero se la geometria interseca invarianti attinenti ad aree protette.	Booleano	Obbligatorio
DESCRIZION	Descrizione sintetica dell'invariante corrispondente alla singola geometria.	Stringa max 255 caratteri (testo libero)	Obbligatorio
RISCHI	Valutazione dei rischi a cui è soggetta l'invariante.	Stringa max 255 caratteri (testo libero)	Obbligatorio
OPPORTUN	Valutazione circa le potenzialità dell'ambito.	Stringa max 255 caratteri (testo libero)	Obbligatorio
RIFERIMENT	Riferimento al paragrafo o articolo degli "indirizzi e direttive strutturali" del PUG.	Stringa max 255 caratteri (testo libero)	Obbligatorio
INDIRIZZI	Sintesi della disciplina da applicarsi all'invariante.	Stringa max 255 caratteri (testo libero)	Obbligatorio

2.6 SIT_PUG45G_INF

Descrizione

La tabella è di natura geometrica e contiene lo strato informativo relativo alle **invarianti infrastrutturali** definite nell'ambito di un dato Comune, nucleo essenziale del Piano Urbanistico Generale.

Gli oggetti geometrici sono poligonali.

Riferimento alle "Linee Guida" DRAG/PUG

PARTE IV - Il Piano Urbanistico Generale, Parte Strutturale (PUG/S).

Regole di editing

Lo strato informativo delle invarianti infrastrutturali è costituito da areali, sovrapponibili tra di loro, e non copre necessariamente l'intero territorio comunale potendo esserci aree non interessate da

alcun elemento. Lo strato informativo deriva dalla sovrapposizione di un insieme di infrastrutture e di attrezzature. Le aree di pertinenza rappresentano la localizzazione delle invarianti infrastrutturali esistenti e di quelle di progetto se esattamente determinate. Le fasce di rispetto rappresentano l'intorno di un'area di pertinenza individuato in base alle norme vigenti per tipo di infrastruttura. La giacitura di massima è quella fascia in cui potrebbero trovare collocazione quelle infrastrutture/attrezzature di previsione per le quali non è possibile/opportuno stabilire la posizione esatta o quelle infrastrutture esistenti ma i cui contorni non sono esattamente individuabili (e.g., il percorso di un nuovo asse di collegamento stradale, un nodo ad elevata specializzazione). Le infrastrutture rappresentate dalla loro giacitura di massima non necessitano dell'individuazione di una fascia di rispetto. Ad ogni areale individuato deve essere associato un insieme di attributi (informazioni) che lo identifichino e ne descrivano le caratteristiche.

Relazioni principali

La tabella è coinvolta in relazioni di decodifica con tabelle dei domini.

Campi

Chiavi primarie			
FILE_ID	Identificativo numerico univoco che contraddistingue ogni geometria nell'ambito della tabella.	Intero lungo	Obbligatorio
COD_ISTAT	Codice ISTAT del Comune al quale lo strato informativo si riferisce.	Stringa max 6 caratteri	Obbligatorio
Campi geometrici			
SHAPE	Campo geometrico poligonale relativo ad una singola istanza dello strato informativo; le geometrie sono 2D.	Tipo geometrico binario	Obbligatorio
Campi ulteriori			
DENOMINAZ	Denominazione associata all'invariante.	Stringa max 255 caratteri (testo libero)	Obbligatorio
DESCRIZION	Descrizione sintetica dell'invariante.	Stringa max 255 caratteri (testo libero)	Obbligatorio
CLASSE	Codice del valore relativo all'attributo <i>classificazione</i> associato all'invariante. Si fa riferimento a valori codificati in un dominio assegnato.	Stringa max 10 caratteri (valori codificati - v. cap.3.1 pag.48)	Obbligatorio
CLASSE_SPE	Descrizione testuale di una classificazione non contemplata nei valori codificati (ha senso se CLASSE='altro').	Stringa max 255 caratteri (testo libero)	Non obbligatorio
TIPO	Codice del valore relativo all'attributo <i>tipologia</i> associato all'invariante. Si fa riferimento a valori codificati in un dominio assegnato.	Stringa max 10 caratteri (valori codificati - v. cap.3.2 pag.48)	Obbligatorio
STA_FATTO	Codice del valore relativo all'attributo <i>stato di fatto</i> associato all'invariante. Si fa riferimento a valori codificati in un dominio assegnato.	Stringa max 10 caratteri (valori codificati - v. cap.3.3 pag.48)	Obbligatorio
RIFERIMENT	Descrizione del riferimento al paragrafo o articolo degli "indirizzi e direttive strutturali" del PUG.	Stringa max 255 caratteri (testo libero)	Obbligatorio
INDIRIZZI	Sintesi della disciplina da applicare all'invariante.	Stringa max 255 caratteri (testo libero)	Obbligatorio

2.7 SIT_PUG49G_CT

Descrizione

La tabella è di natura geometrica e contiene lo strato informativo relativo ai **contesti territoriali** definiti nell'ambito di un dato Comune, nucleo essenziale del Piano Urbanistico Generale. Gli oggetti geometrici sono poligonali.

Riferimento alle "Linee Guida" DRAG/PUG

PARTE IV - Il Piano Urbanistico Generale, Parte Strutturale (PUG/S).

Regole di editing

Lo strato informativo dei contesti territoriali costituisce una partizione del territorio in unità elementari, pertanto l'intero territorio comunale (comprese le strade di rilevanza comunale e le aree interessate da invarianti) deve essere coperto da poligoni e questi non si possono sovrapporre tra loro. Ogni parte del territorio deve essere interessata da uno ed un solo contesto. Non è ammissibile uno strato informativo in cui vi siano areali a cui non è associato alcun attributo. Ad ogni areale individuato deve essere associato un insieme di attributi (informazioni) che lo identifichino e ne descrivano le caratteristiche.

Relazioni principali

La tabella è coinvolta in relazioni di decodifica con tabelle dei domini.

Campi

Chiavi primarie			
FILE_ID	Identificativo numerico univoco che contraddistingue ogni geometria nell'ambito della tabella.	Intero lungo	Obbligatorio
COD_ISTAT	Codice ISTAT del Comune al quale lo strato informativo si riferisce.	Stringa max 6 caratteri	Obbligatorio
Campi geometrici			
SHAPE	Campo geometrico poligonale relativo ad una singola istanza dello strato informativo; le geometrie sono 2D.	Tipo geometrico binario	Obbligatorio
Campi ulteriori			
AMBITO	Codice del valore relativo all'attributo <i>ambito</i> caratteristico dello strato informativo. Si fa riferimento a valori codificati in un dominio assegnato.	Stringa max 10 caratteri (valori codificati - v. cap.3.4 pag.48)	Obbligatorio
TIPO	Codice del valore relativo all'attributo <i>tipo</i> caratteristico dello strato informativo. Si fa riferimento a valori codificati in un dominio assegnato.	Stringa max 10 caratteri (valori codificati - v. cap.3.5 pag.48)	Obbligatorio
TIPO_SPEC	Descrizione di un tipo non contemplato nel dominio di valori codificati; ha senso se TIPO='altro'.	Stringa max 255 caratteri (testo libero)	Non obbligatorio
DENOMINAZ	Denominazione associata ad un singolo contesto, non ripetibile in uno stesso Comune.	Stringa max 255 caratteri (testo libero)	Obbligatorio
ZONE_PAI	Vero se il contesto interseca aree di pericolosità del PAI.	Booleano	Obbligatorio
ATE_PUTT	Vero se il contesto interseca ambiti territoriali estesi.	Booleano	Obbligatorio

INFR_ATTR	Valutazione circa la dotazione di infrastrutture e attrezzature che caratterizza il contesto.	Stringa max 255 caratteri (testo libero)	Obbligatorio
OPPORTUN	Valutazione circa le potenzialità del contesto.	Stringa max 255 caratteri (testo libero)	Obbligatorio
RISCHI	Valutazione circa i rischi a cui il contesto può essere soggetto.	Stringa max 255 caratteri (testo libero)	Obbligatorio
RIFERIMENT	Riferimento al paragrafo o articolo degli "indirizzi e direttive strutturali" del PUG.	Stringa max 255 caratteri (testo libero)	Obbligatorio
SALV_TRASF	Descrizione sintetica delle politiche di salvaguardia o trasformazione previste per il contesto.	Stringa max 255 caratteri (testo libero)	Obbligatorio
INV_IS_GM	Vero se il contesto interseca delle invarianti geo-morfo-idrologiche.	Booleano	Obbligatorio
INV_IS_SC	Vero se il contesto interseca delle invarianti storico-culturali.	Booleano	Obbligatorio
INV_IS_PA	Vero se il contesto interseca delle invarianti paesistico-ambientali.	Booleano	Obbligatorio
INV_AP	Vero se il contesto interseca delle invarianti relative ad aree protette.	Booleano	Obbligatorio

2.8 SIT_PUG63G_PREV_PROGRAMMATICHE

Descrizione

La tabella è di natura geometrica e contiene lo strato informativo relativo alle **previsioni programmatiche** definite nell'ambito di un dato Comune, nucleo essenziale del Piano Urbanistico Generale. Sono presenti informazioni anche relative al contesto in cui la previsione si inserisce.

Gli oggetti geometrici sono poligonali.

Riferimento alle "Linee Guida" DRAG/PUG

PARTE IV - Il Piano Urbanistico Generale, Parte Programmatica (PUG/P).

Regole di editing

Lo strato informativo inerente le Previsioni Programmatiche deriva dalla partizione in microunità dello strato informativo dei contesti già definito. Queste microunità individuano in particolar modo quelle porzioni del territorio sulle quali l'Amministrazione intende agire nel "breve periodo" (anche se per i contesti per i quali non sono previsti interventi di trasformazioni le previsioni possono essere valide a tempo indeterminato). Non devono necessariamente coprire l'intero territorio comunale. Non è ammissibile uno strato informativo in cui vi siano areali a cui non è associato alcun attributo. Ad ogni areale individuato deve essere associato un insieme di attributi (informazioni) che lo identifichino e ne descrivano

Relazioni principali

La tabella è coinvolta in relazioni di decodifica con tabelle dei domini.

Campi

Chiavi primarie			
FILE_ID	Identificativo numerico univoco che contraddistingue ogni geometria nell'ambito della tabella.	Intero lungo	Obbligatorio
COD_ISTAT	Codice ISTAT del Comune al quale lo	Stringa max 6 caratteri	Obbligatorio

	strato informativo si riferisce.		
Campi geometrici			
SHAPE	Campo geometrico poligonale relativo ad una singola istanza dello strato informativo; le geometrie sono 2D.	Tipo geometrico binario	Obbligatorio
Campi ulteriori			
DENOMINAZ	Denominazione associata ad una singola area soggetta a Previsione Programmatica, non ripetibile in uno stesso Comune.	Stringa max 255 caratteri (testo libero)	Obbligatorio
RIF_NORME	Riferimento al paragrafo o articolo degli "indirizzi e direttive programmatiche" del PUG.	Stringa max 255 caratteri (testo libero)	Obbligatorio
SALV_TRASF	Descrizione sintetica delle politiche di salvaguardia o trasformazione previste per l'area soggetta a Previsione Programmatica.	Stringa max 255 caratteri (testo libero)	Obbligatorio
RIF_DESCR	Riferimento all'eventuale paragrafo in cui viene descritta la singola area soggetta a Previsione Programmatica.	Stringa max 255 caratteri (testo libero)	Non obbligatorio
MOD_ATT	Codice del valore relativo all'attributo <i>modalità attuative</i> associato all'area soggetta a Previsione Programmatica. Si fa riferimento a valori codificati in un dominio assegnato.	Stringa max 10 caratteri (valori codificati - v. cap.3.6 pag.49)	Obbligatorio
AMB_APPL	Codice del valore relativo all'attributo <i>ambito di applicazione</i> associato all'area soggetta a Previsione Programmatica. Si fa riferimento a valori codificati in un dominio assegnato.	Stringa max 10 caratteri (valori codificati - v. cap.3.7 pag.49)	Obbligatorio
ARCO_VAL	Codice del valore relativo all'arco di validità associato all'area soggetta a Previsione Programmatica. Si fa riferimento a valori codificati in un dominio assegnato.	Stringa max 10 caratteri (valori codificati - v. cap.3.8 pag.49)	Obbligatorio
ARCO_VAL_S	Dettaglia una classificazione non contemplata nei valori codificati.	Stringa max 255 caratteri (testo libero)	Non obbligatorio
SUP_L_ED	Quantifica la superficie lorda già edificata presente nell'area (mq).	Numerico	Obbligatorio
SUP_L_U_ED	Quantifica la superficie lorda che si prevede di edificare nell'area (mq).	Numerico	Obbligatorio
VOL_L_ED	Quantifica la volumetria lorda già edificata presente nell'area (mc).	Numerico	Obbligatorio
VOL_L_U_ED	Quantifica la volumetria lorda che si prevede di edificare nell'area (mc).	Numerico	Obbligatorio
SUP_CEDUTA	Quantifica la superficie ceduta oltre quella prevista dal Decreto 1444/'68 (mq).	Numerico	Obbligatorio
VOL_CEDUTA	Quantifica la volumetria di alloggi residenziali sociali ceduta (mc) .	Numerico	Obbligatorio
S_ST_ESIST	Quantifica la superficie occupata da servizi di quartiere (mq).	Numerico	Obbligatorio
S_ST_PREV	Quantifica la superficie destinata alla	Numerico	Obbligatorio

	realizzazione di servizi di quartiere (mq).		
PEREQUAZ	Specifica se l'area è soggetta a perequazione.	Booleano	Obbligatorio
INFR_ATTR	Valutazione circa la dotazione di infrastrutture e attrezzature che caratterizza l'area soggetta a Previsione Programmatica.	Stringa max 255 caratteri (testo libero)	Non obbligatorio
INS_INFR	Specifica se nell'area si prevede l'inserimento di nuove infrastrutture.	Booleano	Obbligatorio
AMBITO_C	Codice del valore relativo all'attributo <i>ambito del contesto</i> in cui è inserita l'area soggetta a Previsione Programmatica. Si fa riferimento a valori codificati in un dominio assegnato.	Stringa max 10 caratteri (valori codificati - v. cap.3.4 pag.48)	Obbligatorio
TIPO_C	Codice del valore relativo all'attributo <i>tipologia</i> del contesto in cui è inserita l'area soggetta a Previsione Programmatica. Si fa riferimento a valori codificati in un dominio assegnato.	Stringa max 10 caratteri (valori codificati - v. cap.3.5 pag.48)	Obbligatorio
TIPO_SP_C	Dettaglia una tipologia di contesto in cui è inserita l'area soggetta a Previsione Programmatica non contemplato nel dominio di valori codificati.	Stringa max 255 caratteri (testo libero)	Non obbligatorio
DENOM_C	Specifica la denominazione caratterizzante il contesto in cui l'area soggetta a Previsione Programmatica è inserita.	Stringa max 255 caratteri (testo libero)	Obbligatorio

2.9 SIT_PUG01G_PAI_PG

Descrizione

La tabella è di natura geometrica e contiene lo strato informativo relativo alla **pericolosità geomorfologica**, afferente alla tavola di adeguamento al Piano di Assetto Idrogeologico redatto dalle Autorità di Bacino (AdB) che hanno competenza in Puglia.

Gli oggetti geometrici sono poligonali.

Riferimento alle "Linee Guida" DRAG/PUG

Appendice II - Promemoria sugli adeguamenti alle pianificazioni sovraordinate ed elenco dei pareri - L'adeguamento ai piani di assetto idrogeologico.

Regole di editing

La tavola di adeguamento al piano di assetto idrogeologico ha come base perimetrazioni individuate dalle Autorità di Bacino che hanno competenza sul territorio della Regione Puglia. L'adeguamento consiste nel recepire e prendere atto dei vincoli/limitazioni del PAI (con diverse modalità ed interventi non strutturali) e nel definire per ogni area perimetrata e classificata dal PAI le misure di salvaguardia e/o mitigazione che si intendono adottare in relazione allo stato di fatto e agli interventi proposti dal PUG. Ciascuno strato informativo che da origine alla tavola ha come elemento di partenza le aree individuate dal PAI, eventualmente già approvate come variante derivante da modifiche e/o integrazioni proposte dalle amministrazioni competenti

tramite i procedimenti previsti a tal fine dalle diverse AdB (ricordando che non vi è una sola AdB che ha competenza sul territorio della Regione Puglia). Questo strato sarà costituito da areali che riportano e mosaicano le aree perimetrata e classificate dall' AdB e le definiscono tramite attributi. Nel caso di PAI redatto da altra AdB la restituzione di strati informativi sarà il più possibile conforme a quella riportata, fermo restando le specifiche disposizioni dettate nei singoli PAI. Ad ogni areale individuato deve essere associato un insieme di attributi (informazioni) che lo identifichino e ne descrivano le caratteristiche.

Relazioni principali

La tabella è coinvolta solo in relazioni di decodifica dei valori degli attributi.

Campi

Chiavi primarie			
FILE_ID	Identificativo numerico univoco che contraddistingue ogni geometria nell'ambito della tabella.	Intero lungo	Obbligatorio
COD_ISTAT	Codice ISTAT del Comune al quale lo strato informativo si riferisce.	Stringa max 6 caratteri	Obbligatorio
Campi geometrici			
SHAPE	Campo geometrico poligonale relativo ad una singola istanza dello strato informativo; le geometrie sono 2D.	Tipo geometrico binario	Obbligatorio
Campi ulteriori			
CLASSE	Codice del valore relativo all'attributo <i>classificazione</i> per lo strato informativo. Si fa riferimento a valori codificati in un dominio assegnato.	Stringa max 10 caratteri (valori codificati - v. cap.3.9 pag.49)	Obbligatorio
MOD_RECEP	Descrizione delle azioni e modalità con cui il Comune ha recepito e preso atto dei vincoli/limitazioni del PAI.	Stringa max 255 caratteri (testo libero)	Obbligatorio
SALV_MITIG	Descrizione delle misure di salvaguardia o mitigazione a cui è soggetto l'elemento.	Stringa max 255 caratteri (testo libero)	Non obbligatorio
DESCRIZION	Descrizione associata al singolo elemento areale.	Stringa max 255 caratteri (testo libero)	Non obbligatorio

2.10 SIT_PUG03G_PAI_PI

Descrizione

La tabella è di natura geometrica e contiene lo strato informativo relativo alla **pericolosità idraulica**, afferente alla tavola di adeguamento al Piano di Assetto Idrogeologico redatto dalle Autorità di Bacino (AdB) che hanno competenza in Puglia. Gli oggetti geometrici sono poligonal.

Riferimento alle "Linee Guida" DRAG/PUG

Appendice II - Promemoria sugli adeguamenti alle pianificazioni sovraordinate ed elenco dei pareri - L'adeguamento ai piani di assetto idrogeologico.

Regole di editing

La tavola di adeguamento al piano di assetto idrogeologico ha come base perimetrazioni individuate dalle Autorità di Bacino che hanno competenza sul territorio della Regione Puglia. L'adeguamento consiste nel recepire e prendere atto dei vincoli/limitazioni del PAI (con diverse modalità ed interventi non strutturali) e nel definire per ogni area perimetrata e classificata dal

PAI le misure di salvaguardia e/o mitigazione che si intendono adottare in relazione allo stato di fatto e agli interventi proposti dal PUG. Ciascuno strato informativo che da origine alla tavola ha come elemento di partenza le aree individuate dal PAI, eventualmente già approvate come variante derivante da modifiche e/o integrazioni proposte dalle amministrazioni competenti tramite i procedimenti previsti a tal fine dalle diverse AdB (ricordando che non vi è una sola AdB che ha competenza sul territorio della Regione Puglia). Questo strato sarà costituito da areali che riportano e mosaicano le aree perimetrare e classificate dall' AdB e le definiscono tramite attributi. Nel caso di PAI redatto da altra AdB la restituzione di strati informativi sarà il più possibile conforme a quella riportata, fermo restando le specifiche disposizioni dettate nei singoli PAI. Ad ogni areale individuato deve essere associato un insieme di attributi (informazioni) che lo identifichino e ne descrivano le caratteristiche.

Relazioni principali

La tabella è coinvolta solo in relazioni di decodifica dei valori degli attributi.

Campi

Chiavi primarie			
FILE_ID	Identificativo numerico univoco che contraddistingue ogni geometria nell'ambito della tabella.	Intero lungo	Obbligatorio
COD_ISTAT	Codice ISTAT del Comune al quale lo strato informativo si riferisce.	Stringa max 6 caratteri	Obbligatorio
Campi geometrici			
SHAPE	Campo geometrico poligonale relativo ad una singola istanza dello strato informativo; le geometrie sono 2D.	Tipo geometrico binario	Obbligatorio
Campi ulteriori			
CLASSE	Codice del valore relativo all'attributo <i>classificazione</i> per lo strato informativo. Si fa riferimento a valori codificati in un dominio assegnato.	Stringa max 10 caratteri (valori codificati - v. cap.3.10 pag.49)	Obbligatorio
MOD_RECEP	Descrizione delle azioni e modalità con cui il Comune ha recepito e preso atto dei vincoli/limitazioni del PAI.	Stringa max 255 caratteri (testo libero)	Obbligatorio
SALV_MITIG	Descrizione delle misure di salvaguardia o mitigazione a cui è soggetto l'elemento.	Stringa max 255 caratteri (testo libero)	Non obbligatorio
DESCRIZION	Descrizione associata al singolo elemento areale.	Stringa max 255 caratteri (testo libero)	Non obbligatorio

2.11 SIT_PUG05G_PAI_R

Descrizione

La tabella è di natura geometrica e contiene lo strato informativo relativo al **rischio**, afferente alla tavola di adeguamento al Piano di Assetto Idrogeologico redatto dalle Autorità di Bacino (AdB) che hanno competenza in Puglia.

Gli oggetti geometrici sono poligonali.

Riferimento alle "Linee Guida" DRAG/PUG

Appendice II - Promemoria sugli adeguamenti alle pianificazioni sovraordinate ed elenco dei pareri - L'adeguamento ai piani di assetto idrogeologico.

Regole di editing

La tavola di adeguamento al piano di assetto idrogeologico ha come base perimetrazioni individuate dalle Autorità di Bacino che hanno competenza sul territorio della Regione Puglia. L'adeguamento consiste nell'individuare in ogni area perimetrata dal PAI come area a rischio la tipologia di elementi a rischio presenti, nel recepire e prendere atto dei vincoli/limitazioni del PAI (con diverse modalità ed interventi non strutturali) e nel definire per ogni area perimetrata le misure di salvaguardia e/o mitigazione che si intendono adottare in relazione allo stato di fatto e agli interventi proposti dal PUG. Ciascuno strato informativo che da origine alla tavola ha come elemento di partenza le aree individuate dal PAI, eventualmente già approvate come variante derivante da modifiche e/o integrazioni proposte dalle amministrazioni competenti tramite i procedimenti previsti a tal fine dalle diverse AdB (ricordando che non vi è una sola AdB che ha competenza sul territorio della Regione Puglia).

Nel caso del PAI redatto dall'Autorità di Bacino della Puglia si propone la restituzione di uno strato informativo inerente il rischio (R1/R2/R3/R4). Questi strati saranno costituiti da areali che riportano e mosaicano le aree perimetrare e classificate dall' AdB e le definiscono tramite attributi. Nel caso di PAI redatto da altra AdB la restituzione di strati informativi sarà il più possibile conforme a quella riportata, fermo restando le specifiche disposizioni dettate nei singoli PAI.

Ad ogni areale individuato deve essere associato un insieme di attributi (informazioni) che lo identifichino e ne descrivano le caratteristiche.

Relazioni principali

La tabella è coinvolta solo in relazioni di decodifica dei valori degli attributi.

Campi

Chiavi primarie			
FILE_ID	Identificativo numerico univoco che contraddistingue ogni geometria nell'ambito della tabella.	Intero lungo	Obbligatorio
COD_ISTAT	Codice ISTAT del Comune al quale lo strato informativo si riferisce.	Stringa max 6 caratteri	Obbligatorio
Campi geometrici			
SHAPE	Campo geometrico poligonale relativo ad una singola istanza dello strato informativo; le geometrie sono 2D.	Tipo geometrico binario	Obbligatorio
Campi ulteriori			
CLASSE	Codice del valore relativo all'attributo <i>classificazione</i> per lo strato informativo. Si fa riferimento a valori codificati in un dominio assegnato.	Stringa max 10 caratteri (valori codificati - v. cap.3.11 pag.49)	Obbligatorio
MOD_RECEP	Descrizione delle azioni e modalità con cui il Comune ha recepito e preso atto dei vincoli/limitazioni del PAI.	Stringa max 255 caratteri (testo libero)	Obbligatorio
SALV_MITIG	Descrizione delle misure di salvaguardia o mitigazione a cui è soggetto l'elemento.	Stringa max 255 caratteri (testo libero)	Non obbligatorio
DESCRIZION	Descrizione associata al singolo elemento areale.	Stringa max 255 caratteri (testo libero)	Non obbligatorio
AGGL_URB	Specifica se l'area si riferisce ad agglomerati urbani, comprese le zone di espansione urbanistica.	Booleano	Obbligatorio
AREE_PROD	Specifica se il poligono si riferisce ad aree su cui insistono insediamenti	Booleano	Obbligatorio

	produttivi, impianti tecnologici di rilievo, in particolare quelli definiti a rischio ai sensi di legge.		
INFR_RETE	Specifica se l'area include infrastrutture a rete o vie di comunicazione di rilevanza strategica, anche a livello locale.	Booleano	Obbligatorio
PATR_AMB	Specifica se l'area contiene patrimonio ambientale o beni culturali di interesse rilevante.	Booleano	Obbligatorio
AREE_SERV	Specifica se l'area contiene servizi pubblici o privati, di impianti sportivi o ricreativi, strutture ricettive e infrastrutture primarie.	Booleano	Obbligatorio
ALTRO_RISC	Specifica se all'area sono associati elementi di rischio non contemplati nei casi precedenti.	Booleano	Obbligatorio
DESC_ALT_R	Dettaglia il rischio la cui presenza è garantita dal campo precedente impostato a vero; ha senso solo in tale condizione.	Stringa max 255 caratteri (testo libero)	Non obbligatorio

2.12 SIT_PUG07G_PUTT_ATDGEOL

Descrizione

La tabella è di natura geometrica e contiene lo strato informativo relativo alle **emergenze geologiche**, afferente alla tavola di adeguamento al Piano Urbanistico Territoriale Tematico Paesaggio e Beni Ambientali (PUTT/PBA) redatto a livello Regionale. Gli oggetti geometrici sono poligonal.

Riferimento alle "Linee Guida" DRAG/PUG

Appendice II - Promemoria sugli adeguamenti alle pianificazioni sovraordinate ed elenco dei pareri - L'adeguamento al Piano Urbanistico Territoriale Tematico/Paesaggio.

Regole di editing

Gli strati informativi di adeguamento al piano urbanistico territoriale tematico/paesaggio hanno, nella maggior parte dei casi, come base le aree individuate dai PUTT/PBA come ATD, che vanno analizzate e verificate, nonché studi specifici. Ad ogni areale individuato deve essere associato un insieme di attributi (informazioni) che lo identifichino e ne descrivano le caratteristiche per le emergenze geologiche e le rispettive aree annesse.

Le geometrie corrispondenti ad aree annesse derivanti da intersezione di oggetti afferenti a strati distinti vanno acquisite in maniera identica in ciascuno degli strati coinvolti.

Relazioni principali

La tabella è coinvolta solo in relazioni di decodifica dei valori degli attributi.

Campi

Chiavi primarie			
FILE_ID	Identificativo numerico univoco che contraddistingue ogni geometria nell'ambito della tabella.	Intero lungo	Obbligatorio
COD_ISTAT	Codice ISTAT del Comune al quale lo strato informativo si riferisce.	Stringa max 6 caratteri	Obbligatorio

Campi geometrici			
SHAPE	Campo geometrico poligonale relativo ad una singola istanza dello strato informativo; le geometrie sono 2D.	Tipo geometrico binario	Obbligatorio
Campi ulteriori			
CLASSE	Codice del valore relativo all'attributo <i>classificazione</i> per lo strato informativo. Si fa riferimento a valori codificati in un dominio assegnato. Il valore mista può essere utilizzato in casi estremi solo per aree classificate come area annessa nell'attributo di tipo.	Stringa max 10 caratteri (valori codificati - v. cap.3.12 pag.50)	Obbligatorio
TIPO	Codice del valore relativo all'attributo <i>tipo</i> per lo strato informativo. Si fa riferimento a valori codificati in un dominio assegnato.	Stringa max 10 caratteri (valori codificati - v. cap.3.13 pag.50)	Obbligatorio
DESCRIZION	Descrizione associata al singolo elemento areale.	Stringa max 255 caratteri (testo libero)	Non obbligatorio
RIF_CL_INT	Codice del valore relativo all'attributo <i>riferimento alle classi intersecate</i> . Viene fatto riferimento a valori codificati in un dominio assegnato. Il campo va compilato solo per aree classificate come <i>area annessa</i> nell'attributo di tipo.	Stringa max 10 caratteri (valori codificati - v. cap.3.40 pag. 56)	Non obbligatorio
TIPO_FONTE	Descrizione testuale relativamente all'origine del dato inserito.	Stringa max 255 caratteri (testo libero)	Non obbligatorio

2.13 SIT_PUG10G_PUTT_ATDGROTT

Descrizione

La tabella è di natura geometrica e contiene lo strato informativo relativo a **grotte, doline, puli, vore, inghiottitoi**, afferente alla tavola di adeguamento al Piano Urbanistico Territoriale Tematico Paesaggio e Beni Ambientali (PUTT/PBA) redatto a livello regionale. Gli oggetti geometrici sono poligonali.

Riferimento alle "Linee Guida" DRAG/PUG

Appendice II - Promemoria sugli adeguamenti alle pianificazioni sovraordinate ed elenco dei pareri - L' adeguamento al Piano Urbanistico Territoriale Tematico/Paesaggio.

Regole di editing

Gli strati informativi di adeguamento al piano urbanistico territoriale tematico/paesaggio hanno, nella maggior parte dei casi, come base le aree individuate dai PUTT/PBA come ATD, che vanno analizzate e verificate, nonché studi specifici. Ad ogni areale individuato deve essere associato un insieme di attributi (informazioni) che lo identifichino e ne descrivano le caratteristiche per le grotte/doline, puli e vore, e le rispettive aree annesse.

Le geometrie corrispondenti ad aree annesse derivanti da intersezione di oggetti afferenti a strati distinti vanno acquisite in maniera identica in ciascuno degli strati coinvolti.

Relazioni principali

La tabella è coinvolta solo in relazioni di decodifica dei valori degli attributi.

Campi

Chiavi primarie			
FILE_ID	Identificativo numerico univoco che contraddistingue ogni geometria nell'ambito della tabella.	Intero lungo	Obbligatorio
COD_ISTAT	Codice ISTAT del Comune al quale lo strato informativo si riferisce.	Stringa max 6 caratteri	Obbligatorio
Campi geometrici			
SHAPE	Campo geometrico poligonale relativo ad una singola istanza dello strato informativo; le geometrie sono 2D.	Tipo geometrico binario	Obbligatorio
Campi ulteriori			
DENOMINAZ	Denominazione associata all'area (fa riferimento ad un nome o un codice univoco).	Stringa max 255 caratteri (testo libero)	Obbligatorio
CLASSE	Codice del valore relativo all'attributo <i>classificazione</i> per lo strato informativo. Si fa riferimento a valori codificati in un dominio assegnato. Il valore mista può essere utilizzato in casi estremi solo per aree classificate come area annessa nell'attributo di tipo.	Stringa max 10 caratteri (valori codificati - v. cap.3.18 pag.51)	Obbligatorio
TIPO	Codice del valore relativo all'attributo <i>tipo</i> per lo strato informativo. Si fa riferimento a valori codificati in un dominio assegnato.	Stringa max 10 caratteri (valori codificati - v. cap.3.13 pag.50)	Obbligatorio
MOD_PUTT	Codice del valore relativo all'attributo inerente le modifiche in rapporto al PUTT/PBA in vigore. Si fa riferimento a valori codificati in un dominio assegnato.	Stringa max 10 caratteri (valori codificati - v. cap.3.15 pag.50)	Non obbligatorio
RIF_CL_INT	Codice del valore relativo all'attributo <i>riferimento alle classi intersecate</i> . Viene fatto riferimento a valori codificati in un dominio assegnato. Il campo va compilato solo per aree classificate come <i>area ammessa</i> nell'attributo di tipo.	Stringa max 10 caratteri (valori codificati - v. cap.3.40 pag. 56)	Non obbligatorio
ID_CAT_GR	Riporta il numero che identifica la grotta in modo univoco nel catasto grotte della Puglia.	Stringa max 50 caratteri (testo libero)	Non obbligatorio
ID_PTCP	Riporta l'identificativo univoco della grotta secondo il Piano Territoriale di Coordinamento della provincia relativa (laddove il piano esiste e lo contempla).	Stringa max 50 caratteri (testo libero)	Non obbligatorio
TIPO_FONTE	Descrizione testuale relativamente all'origine del dato inserito.	Stringa max 255 caratteri (testo libero)	Non obbligatorio

2.14 SIT_PUG57G_PUTT_ATDGROTT_P**Descrizione**

La tabella è di natura geometrica e contiene lo strato informativo relativo a **grotte, doline, puli, vore, inghiottitoi**, afferente alla tavola di adeguamento al Piano Urbanistico Territoriale

Tematico Paesaggio e Beni Ambientali (PUTT/PBA) redatto a livello regionale.

Gli oggetti geometrici sono puntuali in quanto beni non individuabili in termini di estensioni areali; si tratta di un'eccezione particolare rappresentata dal collassamento in linea in quanto del singolo bene è possibile una localizzazione puntuale ma non un ingombro areale.

Questo strato non è obbligatorio.

Riferimento alle "Linee Guida" DRAG/PUG

Appendice II - Promemoria sugli adeguamenti alle pianificazioni sovraordinate ed elenco dei pareri – L' adeguamento al Piano Urbanistico Territoriale Tematico/Paesaggio.

Regole di editing

Gli strati informativi di adeguamento al piano urbanistico territoriale tematico/paesaggio hanno, nella maggior parte dei casi, come base le aree individuate dai PUTT/PBA come ATD, che vanno analizzate e verificate, nonché studi specifici. L'utilizzo di questo strato informativo (puntuale e non areale) è ammesso solo nei casi in cui non sia in alcun modo possibile il riconoscimento dell'area del bene; la restituzione delle aree annesse è comunque richiesta in formato areale, e verrà inserita nel corrispettivo strato areale.

Relazioni principali

La tabella è coinvolta solo in relazioni di decodifica dei valori degli attributi.

Campi

Chiavi primarie			
FILE_ID	Identificativo numerico univoco che contraddistingue ogni geometria nell'ambito della tabella.	Intero lungo	Obbligatorio
COD_ISTAT	Codice ISTAT del Comune al quale lo strato informativo si riferisce.	Stringa max 6 caratteri	Obbligatorio
Campi geometrici			
SHAPE	Campo geometrico puntuale relativo ad una singola istanza dello strato informativo; le geometrie sono 2D.	Tipo geometrico binario	Obbligatorio
Campi ulteriori			
DENOMINAZ	Denominazione associata a grotte/puli/doline/vore/inghiottitoi (fa riferimento ad un nome o un codice univoco).	Stringa max 255 caratteri (testo libero)	Obbligatorio
CLASSE	Codice del valore relativo all'attributo classificazione per lo strato informativo. Si fa riferimento a valori codificati in un dominio assegnato.	Stringa max 10 caratteri (valori codificati - v. cap.3.18 pag.51)	Obbligatorio
MOD_PUTT	Codice del valore relativo all'attributo inerente le modifiche in rapporto al PUTT/PBA in vigore. Si fa riferimento a valori codificati in un dominio assegnato.	Stringa max 10 caratteri (valori codificati - v. cap.3.17 pag.51)	Non obbligatorio
ID_CAT_GR	Riporta il numero che identifica la grotta in modo univoco nel catasto grotte della Puglia.	Stringa max 50 caratteri (testo libero)	Non obbligatorio
ID_PTCP	Riporta l'identificativo univoco della grotta secondo il Piano Territoriale di Coordinamento della provincia relativa (laddove il piano esiste e lo contempla).	Stringa max 50 caratteri (testo libero)	Non obbligatorio
TIPO_FONTE	Descrizione testuale relativamente all'origine del dato inserito.	Stringa max 255 caratteri (testo libero)	Non obbligatorio

2.15 SIT_PUG13G_PUTT_ATDCOSTE

Descrizione

La tabella è di natura geometrica e contiene lo strato informativo relativo alle **coste**, afferente alla tavola di adeguamento al Piano Urbanistico Territoriale Tematico Paesaggio e Beni Ambientali (PUTT/PBA) redatto a livello regionale.
Gli oggetti geometrici sono poligonali.

Riferimento alle "Linee Guida" DRAG/PUG

Appendice II - Promemoria sugli adeguamenti alle pianificazioni sovraordinate ed elenco dei pareri – L'adeguamento al Piano Urbanistico Territoriale Tematico/Paesaggio.

Regole di editing

Ad ogni areale individuato deve essere associato un insieme di attributi (informazioni) che lo identifichino e ne descrivano le caratteristiche per le coste e le rispettive aree annesse.

Relazioni principali

La tabella è coinvolta solo in relazioni di decodifica dei valori degli attributi.
Le geometrie corrispondenti ad aree annesse derivanti da intersezione di oggetti afferenti a strati distinti vanno acquisite in maniera identica in ciascuno degli strati coinvolti.

Campi

Chiavi primarie			
FILE_ID	Identificativo numerico univoco che contraddistingue ogni geometria nell'ambito della tabella.	Intero lungo	Obbligatorio
COD_ISTAT	Codice ISTAT del Comune al quale lo strato informativo si riferisce.	Stringa max 6 caratteri	Obbligatorio
Campi geometrici			
SHAPE	Campo geometrico poligonale relativo ad una singola istanza dello strato informativo; le geometrie sono 2D.	Tipo geometrico binario	Obbligatorio
Campi ulteriori			
CLASSE	Codice del valore relativo all'attributo <i>classificazione</i> per lo strato informativo. Si fa riferimento a valori codificati in un dominio assegnato. Il valore mista può essere utilizzato in casi estremi solo per aree classificate come area annessa nell'attributo di tipo.	Stringa max 10 caratteri (valori codificati - v. cap.3.19 pag.51)	Obbligatorio
TIPO	Codice del valore relativo all'attributo <i>tipo</i> per lo strato informativo. Si fa riferimento a valori codificati in un dominio assegnato.	Stringa max 10 caratteri (valori codificati - v. cap.3.20 pag.51)	Obbligatorio
DESCRIZION	Descrizione associata al singolo elemento areale.	Stringa max 255 caratteri (testo libero)	Non obbligatorio
RIF_CL_INT	Codice del valore relativo all'attributo <i>riferimento alle classi intersecate</i> . Viene fatto riferimento a valori codificati in un dominio assegnato. Il campo va compilato solo per aree classificate come <i>area annessa</i> nell'attributo di tipo.	Stringa max 10 caratteri (valori codificati - v. cap.3.40 pag. 56)	Non obbligatorio

TIPO_FONTE	Descrizione testuale relativamente all'origine del dato inserito.	Stringa max 255 caratteri (testo libero)	Non obbligatorio
DESC_CI	Descrizione della tipologia di costa secondo la classificazione della Carta Idrogeomorfologica. Si fa riferimento a valori codificati in un dominio assegnato.	Stringa max 10 caratteri (valori codificati - v. cap.3.21 pag. 51)	Non obbligatorio
ID_PCC	Identificativo dell'elemento secondo il Piano Comunale delle Coste, se realizzato e informatizzato.	Stringa max 50 caratteri (testo libero)	Non obbligatorio

2.16 SIT_PUG74G_PUTT_ATDIDRO_BACINO

Descrizione

La tabella è di natura geometrica e contiene lo strato informativo relativo all'**idrologia superficiale**, afferente alla tavola di adeguamento al Piano Urbanistico Territoriale Tematico Paesaggio e Beni Ambientali (PUTT/PBA) redatto a livello regionale.

Gli oggetti geometrici sono poligonali e si riferiscono ad oggetti territoriali afferenti alla categoria dei **bacini, invasi e laghi**.

Riferimento alle "Linee Guida" DRAG/PUG

Appendice II - Promemoria sugli adeguamenti alle pianificazioni sovraordinate ed elenco dei pareri – L'adeguamento al Piano Urbanistico Territoriale Tematico/Paesaggio.

Regole di editing

Gli strati informativi di adeguamento al piano urbanistico territoriale tematico/paesaggio hanno, nella maggior parte dei casi, come base le aree individuate dai PUTT/PBA come ATD, che vanno analizzate e verificate nonché studi specifici. Ad ogni areale individuato deve essere associato un insieme di attributi (informazioni) che lo identifichino e ne descrivano le caratteristiche per l'idrologia superficiale e le rispettive aree annesse.

Le geometrie corrispondenti ad aree annesse derivanti da intersezione di oggetti afferenti a strati distinti vanno acquisite in maniera identica in ciascuno degli strati coinvolti.

Relazioni principali

La tabella è coinvolta solo in relazioni di decodifica dei valori degli attributi.

Campi

Chiavi primarie			
FILE_ID	Identificativo numerico univoco che contraddistingue ogni geometria nell'ambito della tabella.	Intero lungo	Obbligatorio
COD_ISTAT	Codice ISTAT del Comune al quale lo strato informativo si riferisce.	Stringa max 6 caratteri	Obbligatorio
Campi geometrici			
SHAPE	Campo geometrico poligonale relativo ad una singola istanza dello strato informativo; le geometrie sono 2D.	Tipo geometrico binario	Obbligatorio
Campi ulteriori			
DENOMINAZ	Denominazione associata all'area (fa riferimento ad un nome o un codice univoco)	Stringa max 255 caratteri (testo libero)	Obbligatorio
CLASSE	Codice del valore relativo all'attributo <i>classificazione</i> per lo strato informativo.	Stringa max 10 caratteri (valori codificati - v.	Obbligatorio

	Si fa riferimento a valori codificati in un dominio assegnato. Il valore mista può essere utilizzato in casi estremi solo per aree classificate come area annessa nell'attributo di tipo.	cap.3.22 pag.52)	
TIPO	Codice del valore relativo all'attributo <i>tipo</i> per lo strato informativo. Si fa riferimento a valori codificati in un dominio assegnato.	Stringa max 10 caratteri (valori codificati - v. cap.3.20 pag.51)	Obbligatorio
DESCRIZION	Descrizione associata al singolo elemento areale.	Stringa max 255 caratteri (testo libero)	Non obbligatorio
RIF_CL_INT	Codice del valore relativo all'attributo <i>riferimento alle classi intersecate</i> . Viene fatto riferimento a valori codificati in un dominio assegnato. Il campo va compilato solo per aree classificate come <i>area annessa</i> nell'attributo di tipo.	Stringa max 10 caratteri (valori codificati - v. cap.3.40 pag. 56)	Non obbligatorio
TIPO_FONTE	Descrizione testuale relativamente all'origine del dato inserito	Stringa max 255 caratteri (testo libero)	Non obbligatorio
DESC_CI	Descrizione della tipologia di costa secondo la classificazione della Carta Idrogeomorfologica. Si fa riferimento a valori codificati in un dominio assegnato.	Stringa max 10caratteri (valori codificati - v. cap3.23 pag.52)	Non obbligatorio

2.17 SIT_PUG15G_PUTT_ATDIDRO_CORSO

Descrizione

La tabella è di natura geometrica e contiene lo strato informativo relativo all'**idrologia superficiale**, afferente alla tavola di adeguamento al Piano Urbanistico Territoriale Tematico Paesaggio e Beni Ambientali (PUTT/PBA) redatto a livello regionale.

Gli oggetti geometrici sono poligonali.

Riferimento alle "Linee Guida" DRAG/PUG

Appendice II - Promemoria sugli adeguamenti alle pianificazioni sovraordinate ed elenco dei pareri – L'adeguamento al Piano Urbanistico Territoriale Tematico/Paesaggio.

Regole di editing

Gli strati informativi di adeguamento al piano urbanistico territoriale tematico/paesaggio hanno, nella maggior parte dei casi, come base le aree individuate dai PUTT/PBA come ATD, che vanno analizzate e verificate, nonché studi specifici. Ad ogni areale individuato deve essere associato un insieme di attributi (informazioni) che lo identifichino.

Le geometrie corrispondenti ad aree annesse derivanti da intersezione di oggetti afferenti a strati distinti vanno acquisite in maniera identica in ciascuno degli strati coinvolti.

Relazioni principali

La tabella è coinvolta solo in relazioni di decodifica dei valori degli attributi.

Campi

Chiavi primarie			
FILE_ID	Identificativo numerico univoco che contraddistingue ogni geometria nell'ambito della tabella.	Intero lungo	Obbligatorio

COD_ISTAT	Codice ISTAT del Comune al quale lo strato informativo si riferisce.	Stringa max 6 caratteri	Obbligatorio
Campi geometrici			
SHAPE	Campo geometrico poligonale relativo ad una singola istanza dello strato informativo; le geometrie sono 2D.	Tipo geometrico binario	Obbligatorio
Campi ulteriori			
DENOMINAZ	Denominazione associata all'area (fa riferimento ad un nome o un codice univoco).	Stringa max 255 caratteri (testo libero)	Obbligatorio
CLASSE	Codice del valore relativo all'attributo <i>classificazione</i> per lo strato informativo. Si fa riferimento a valori codificati in un dominio assegnato. Il valore mista può essere utilizzato in casi estremi solo per aree classificate come area annessa nell'attributo di tipo.	Stringa max 10 caratteri (valori codificati - v. cap.3.24 pag.52)	Obbligatorio
PROPRIETA'	Codice del valore relativo all'attributo <i>proprietà</i> per lo strato informativo. Si fa riferimento a valori codificati in un dominio assegnato.	Stringa max 10 caratteri (valori codificati - v. cap.3.28 pag.53)	Obbligatorio
TIPO	Codice del valore relativo all'attributo <i>tipo</i> per lo strato informativo. Si fa riferimento a valori codificati in un dominio assegnato.	Stringa max 10 caratteri (valori codificati - v. cap.3.13 pag.50)	Obbligatorio
MOD_PUTT	Codice del valore relativo all'attributo inerente le modifiche in rapporto al PUTT/PBA in vigore. Si fa riferimento a valori codificati in un dominio assegnato.	Stringa max 10 caratteri (valori codificati - v. cap.3.15 pag.50)	Non obbligatorio
RIF_CL_INT	Codice del valore relativo all'attributo <i>riferimento alle classi intersecate</i> . Viene fatto riferimento a valori codificati in un dominio assegnato. Il campo va compilato solo per aree classificate come <i>area annessa</i> nell'attributo di tipo.	Stringa max 10 caratteri (valori codificati - v. cap.3.40 pag. 56)	Non obbligatorio
TIPO_FONTE	Descrizione testuale relativamente all'origine del dato inserito.	Stringa max 255 caratteri (testo libero)	Non obbligatorio
DESC_CI	Descrizione della tipologia di costa secondo la classificazione della Carta Idrogeomorfologica. Si fa riferimento a valori codificati in un dominio assegnato.	Stringa max 10caratteri (valori codificati - v. cap3.25 pag.52)	Non obbligatorio

2.18 SIT_PUG58G_PUTT_ATDIDRO_L

Descrizione

La tabella è di natura geometrica e contiene lo strato informativo relativo all'**idrologia superficiale**, afferente alla tavola di adeguamento al Piano Urbanistico Territoriale Tematico Paesaggio e Beni Ambientali (PUTT/PBA) redatto a livello regionale.

Gli oggetti geometrici sono lineari in quanto beni non individuabili in termini di estensioni areali; si tratta di un'eccezione particolare rappresentata dal collassamento in linea in quanto del singolo bene è possibile definire un tracciato lineare ma non un ingombro areale.

Questo strato non è obbligatorio.

Riferimento alle "Linee Guida" DRAG/PUG

Appendice II - Promemoria sugli adeguamenti alle pianificazioni sovraordinate ed elenco dei pareri – L'adeguamento al Piano Urbanistico Territoriale Tematico/Paesaggio.

Regole di editing

Gli strati informativi di adeguamento al piano urbanistico territoriale tematico/paesaggio hanno, nella maggior parte dei casi, come base le aree individuate dai PUTT/PBA come ATD, che vanno analizzate e verificate, nonché studi specifici. L'utilizzo di questo strato informativo (lineare e non areale) è ammesso solo nei casi in cui non sia in alcun modo possibile il riconoscimento dell'area del bene; la restituzione delle aree annesse è comunque richiesta in formato areale, e verrà inserita nel corrispettivo strato areale. Ad ogni linea individuata deve essere associata un insieme di attributi che lo identifichino e ne descrivano le caratteristiche per l'idrologia superficiale.

Relazioni principali

La tabella è coinvolta solo in relazioni di decodifica dei valori degli attributi.

Campi

Chiavi primarie			
FILE_ID	Identificativo numerico univoco che contraddistingue ogni geometria nell'ambito della tabella.	Intero lungo	Obbligatorio
COD_ISTAT	Codice ISTAT del Comune al quale lo strato informativo si riferisce.	Stringa max 6 caratteri	Obbligatorio
Campi geometrici			
SHAPE	Campo geometrico lineare relativo ad una singola istanza dello strato informativo; le geometrie sono 2D.	Tipo geometrico binario	Obbligatorio
Campi ulteriori			
DENOMINAZ	Denominazione associata al bene idrogeologico (fa riferimento ad un nome o un codice univoco)	Stringa max 255 caratteri (testo libero)	Obbligatorio
CLASSE	Codice del valore relativo all'attributo <i>classificazione</i> per lo strato informativo. Si fa riferimento a valori codificati in un dominio assegnato.	Stringa max 10 caratteri (valori codificati - v. cap.3.26 pag.52)	Obbligatorio
PROPRIETA'	Codice del valore relativo all'attributo <i>proprietà</i> per lo strato informativo. Si fa riferimento a valori codificati in un dominio assegnato	Stringa max 10 caratteri (valori codificati - v. cap.3.28 pag.53)	Obbligatorio
MOD_PUTT	Codice del valore relativo all'attributo inerente le modifiche in rapporto al PUTT/PBA in vigore. Si fa riferimento a valori codificati in un dominio assegnato.	Stringa max 10 caratteri (valori codificati - v. cap.3.16 pag.50)	Non obbligatorio
TIPO_FONTE	Descrizione testuale relativamente all'origine del dato inserito	Stringa max 255 caratteri (testo libero)	Non obbligatorio
DESC_CI	Descrizione della tipologia di costa secondo la classificazione della Carta Idrogeomorfologica. Si fa riferimento a valori codificati in un dominio assegnato.	Stringa max 10 caratteri (valori codificati - v. cap.3.27 pag.53)	Non obbligatorio

2.19 SIT_PUG70G_PUTT_ATDIDRO_P

Descrizione

La tabella è di natura geometrica e contiene lo strato informativo delle *sorgenti* (elementi puntuali) nell'ambito dell'**idrologia superficiale**, con riferimento alla tavola di adeguamento al Piano Urbanistico Territoriale Tematico Paesaggio e Beni Ambientali (PUTT/PBA) redatto a livello regionale.

Gli oggetti geometrici sono puntuali e riferiti esclusivamente alla tipologia idrologica delle **sorgenti**, per cui assumendo ciò si omettono ulteriori attributi qualificativi di categorie specifiche.

Riferimento alle "Linee Guida" DRAG/PUG

Appendice II - Promemoria sugli adeguamenti alle pianificazioni sovraordinate ed elenco dei pareri – L'adeguamento al Piano Urbanistico Territoriale Tematico/Paesaggio.

Regole di editing

Gli strati informativi di adeguamento al piano urbanistico territoriale tematico/paesaggio hanno, nella maggior parte dei casi, come base le aree individuate dai PUTT/PBA come ATD, che vanno analizzate e verificate, nonché studi specifici. L'utilizzo di questo strato informativo (puntuale e non areale) è ammesso solo nei casi in cui non sia in alcun modo possibile il riconoscimento dell'area del bene; la restituzione delle aree annesse è comunque richiesta in formato areale, e verrà inserita nel corrispettivo strato areale. Ad ogni punto individuato deve essere associato un insieme di attributi che lo identifichino e ne descrivano le caratteristiche per l'idrologia superficiale.

Relazioni principali

La tabella è coinvolta solo in relazioni di decodifica dei valori degli attributi.

Campi

Chiavi primarie			
FILE_ID	Identificativo numerico univoco che contraddistingue ogni geometria nell'ambito della tabella.	Intero lungo	Obbligatorio
COD_ISTAT	Codice ISTAT del Comune al quale lo strato informativo si riferisce.	Stringa max 6 caratteri	Obbligatorio
Campi geometrici			
SHAPE	Campo geometrico puntuale relativo ad una singola istanza dello strato informativo; le geometrie sono 2D.	Tipo geometrico binario	Obbligatorio
Campi ulteriori			
DENOMINAZ	Denominazione associata al bene idrogeologico (fa riferimento ad un nome o un codice univoco).	Stringa max 255 caratteri (testo libero)	Obbligatorio
DESCRIZION	Descrizione associata al singolo elemento puntuale.	Stringa max 255 caratteri (testo libero)	Non obbligatorio
TIPO_FONTE	Descrizione testuale relativamente all'origine del dato inserito.	Stringa max 255 caratteri (testo libero)	Non obbligatorio

2.20 SIT_PUG19G_PUTT_ATDVECRI

Descrizione

La tabella è di natura geometrica e contiene lo strato informativo relativo ai **versanti e ai crinali**, afferente alla tavola di adeguamento al Piano Urbanistico Territoriale Tematico Paesaggio e Beni

Ambientali (PUTT/PBA) redatto a livello regionale.
Gli oggetti geometrici sono poligonali.

Riferimento alle "Linee Guida" DRAG/PUG

Appendice II - Promemoria sugli adeguamenti alle pianificazioni sovraordinate ed elenco dei pareri – L'adeguamento al Piano Urbanistico Territoriale Tematico/Paesaggio.

Regole di editing

Ad ogni areale individuato deve essere associato un insieme di attributi (informazioni) che lo identifichino e ne descrivano le caratteristiche per i versanti/crinali.

Le geometrie corrispondenti ad aree annesse derivanti da intersezione di oggetti afferenti a strati distinti vanno acquisite in maniera identica in ciascuno degli strati coinvolti.

Relazioni principali

La tabella è coinvolta solo in relazioni di decodifica dei valori degli attributi.

Campi

Chiavi primarie			
FILE_ID	Identificativo numerico univoco che contraddistingue ogni geometria nell'ambito della tabella.	Intero lungo	Obbligatorio
COD_ISTAT	Codice ISTAT del Comune al quale lo strato informativo si riferisce.	Stringa max 6 caratteri	Obbligatorio
Campi geometrici			
SHAPE	Campo geometrico poligonale relativo ad una singola istanza dello strato informativo; le geometrie sono 2D.	Tipo geometrico binario	Obbligatorio
Campi ulteriori			
CLASSE	Codice del valore relativo all'attributo <i>classificazione</i> per lo strato informativo. Si fa riferimento a valori codificati in un dominio assegnato. Il valore mista può essere utilizzato in casi estremi solo per aree classificate come area annessa nell'attributo di tipo.	Stringa max 10 caratteri (valori codificati - v. cap.3.29 pag.53)	Obbligatorio
TIPO	Codice del valore relativo all'attributo <i>tipo</i> per lo strato informativo. Si fa riferimento a valori codificati in un dominio assegnato.	Stringa max 10 caratteri (valori codificati - v. cap.3.30 pag.53)	Obbligatorio
DESCRIZION	Descrizione associata al singolo elemento areale.	Stringa max 255 caratteri (testo libero)	Non obbligatorio
RIF_CL_INT	Codice del valore relativo all'attributo <i>riferimento alle classi intersecate</i> . Viene fatto riferimento a valori codificati in un dominio assegnato. Il campo va compilato solo per aree classificate come <i>area annessa</i> nell'attributo di tipo.	Stringa max 10 caratteri (valori codificati - v. cap.3.40 pag. 56)	Non obbligatorio
TIPO_FONTE	Descrizione testuale relativamente all'origine del dato inserito.	Stringa max 255 caratteri (testo libero)	Non obbligatorio

2.21 SIT_PUG72G_PUTT_ATDVECRI_L

Descrizione

La tabella è di natura geometrica e contiene lo strato informativo relativo ai **versanti e ai crinali**, afferente alla tavola di adeguamento al Piano Urbanistico Territoriale Tematico Paesaggio e Beni Ambientali (PUTT/PBA) redatto a livello regionale.

Gli oggetti geometrici sono lineari in quanto beni non individuabili in termini di estensioni areali; si tratta di un'eccezione particolare rappresentata dal collassamento in linea in quanto del singolo bene è possibile definire un tracciato lineare ma non un ingombro areale.

Questo strato non è obbligatorio.

Riferimento alle "Linee Guida" DRAG/PUG

Appendice II - Promemoria sugli adeguamenti alle pianificazioni sovraordinate ed elenco dei pareri – L'adeguamento al Piano Urbanistico Territoriale Tematico/Paesaggio.

Regole di editing

L'utilizzo di questo strato informativo (lineare e non areale) è ammesso solo nei casi in cui non sia in alcun modo possibile il riconoscimento dell'area del bene; la restituzione delle aree annesse è comunque richiesta in formato areale, e verrà inserita nel corrispettivo strato areale. Ad ogni linea individuata deve essere associata un insieme di attributi che lo identifichino e ne descrivano le caratteristiche per i versanti/crinali.

Relazioni principali

La tabella è coinvolta solo in relazioni di decodifica dei valori degli attributi.

Campi

Chiavi primarie			
FILE_ID	Identificativo numerico univoco che contraddistingue ogni geometria nell'ambito della tabella.	Intero lungo	Obbligatorio
COD_ISTAT	Codice ISTAT del Comune al quale lo strato informativo si riferisce.	Stringa max 6 caratteri	Obbligatorio
Campi geometrici			
SHAPE	Campo geometrico lineare relativo ad una singola istanza dello strato informativo; le geometrie sono 2D.	Tipo geometrico binario	Obbligatorio
Campi ulteriori			
DESCRIZION	Descrizione associata al singolo elemento areale.	Stringa max 255 caratteri (testo libero)	Obbligatorio
TIPO_FONTE	Descrizione testuale relativamente all'origine del dato inserito.	Stringa max 255 caratteri (testo libero)	Non obbligatorio

2.22 SIT_PUG22G_PUTT_ATDBOMA

Descrizione

La tabella è di natura geometrica e contiene lo strato informativo relativo ai **boschi e alle macchie**, afferente alla tavola di adeguamento al Piano Urbanistico Territoriale Tematico Paesaggio e Beni Ambientali (PUTT/PBA) redatto a livello regionale.

Gli oggetti geometrici sono poligonali.

Riferimento alle "Linee Guida" DRAG/PUG

Appendice II - Promemoria sugli adeguamenti alle pianificazioni sovraordinate ed elenco dei pareri – L'adeguamento al Piano Urbanistico Territoriale Tematico/Paesaggio.

Regole di editing

Gli strati informativi di adeguamento al piano urbanistico territoriale tematico/paesaggio hanno, nella maggior parte dei casi, come base le aree individuate dai PUTT/PBA come ATD, che vanno analizzate e verificate, nonché studi specifici. Ad ogni areale individuato deve essere associato un insieme di attributi (informazioni) che lo identifichino e ne descrivano le caratteristiche per i boschi/macchie e le rispettive aree annesse.

Le geometrie corrispondenti ad aree annesse derivanti da intersezione di oggetti afferenti a strati distinti vanno acquisite in maniera identica in ciascuno degli strati coinvolti.

Relazioni principali

La tabella è coinvolta solo in relazioni di decodifica dei valori degli attributi.

Campi

Chiavi primarie			
FILE_ID	Identificativo numerico univoco che contraddistingue ogni geometria nell'ambito della tabella.	Intero lungo	Obbligatorio
COD_ISTAT	Codice ISTAT del Comune al quale lo strato informativo si riferisce.	Stringa max 6 caratteri	Obbligatorio
Campi geometrici			
SHAPE	Campo geometrico poligonale relativo ad una singola istanza dello strato informativo; le geometrie sono 2D.	Tipo geometrico binario	Obbligatorio
Campi ulteriori			
DENOMINAZ	Denominazione associata all'area (fa riferimento ad un nome o un codice univoco).	Stringa max 255 caratteri (testo libero)	Obbligatorio
CLASSE	Codice del valore relativo all'attributo <i>classificazione</i> per lo strato informativo. Si fa riferimento a valori codificati in un dominio assegnato. Il valore mista può essere utilizzato in casi estremi solo per aree classificate come area annessa nell'attributo di tipo.	Stringa max 10 caratteri (valori codificati - v. cap.3.31 pag.53)	Obbligatorio
TIPO	Codice del valore relativo all'attributo <i>tipo</i> per lo strato informativo. Si fa riferimento a valori codificati in un dominio assegnato.	Stringa max 10 caratteri (valori codificati - v. cap.3.13 pag.50)	Obbligatorio
MOD_PUTT	Codice del valore relativo all'attributo inerente le modifiche in rapporto al PUTT/PBA in vigore. Si fa riferimento a valori codificati in un dominio assegnato.	Stringa max 10 caratteri (valori codificati - v. cap.3.15 pag.50)	Non obbligatorio
RIF_CL_INT	Codice del valore relativo all'attributo <i>riferimento alle classi intersecate</i> . Viene fatto riferimento a valori codificati in un dominio assegnato. Il campo va compilato solo per aree classificate come <i>area annessa</i> nell'attributo di tipo.	Stringa max 10 caratteri (valori codificati - v. cap.3.40 pag. 56)	Non obbligatorio
TIPO_FONTE	Descrizione testuale relativamente	Stringa max 255 caratteri	Non obbligatorio

	all'origine del dato inserito..	(testo libero)	
--	---------------------------------	----------------	--

2.23 SIT_PUG24G_PUTT_ATDNATUR

Descrizione

La tabella è di natura geometrica e contiene lo strato informativo relativo alle **aree naturalistiche**, afferente alla tavola di adeguamento al Piano Urbanistico Territoriale Tematico Paesaggio e Beni Ambientali (PUTT/PBA) redatto a livello regionale.

Gli oggetti geometrici sono poligonali.

Riferimento alle "Linee Guida" DRAG/PUG

Appendice II - Promemoria sugli adeguamenti alle pianificazioni sovraordinate ed elenco dei pareri - L'adeguamento al Piano Urbanistico Territoriale Tematico/Paesaggio.

Regole di editing

Gli strati informativi di adeguamento al piano urbanistico territoriale tematico/paesaggio hanno, nella maggior parte dei casi, come base le aree individuate dai PUTT/PBA come ATD, che vanno analizzate e verificate, nonché studi specifici. Ad ogni areale individuato deve essere associato un insieme di attributi (informazioni) che lo identifichino e ne descrivano le caratteristiche per le aree naturalistiche e le rispettive aree annesse.

Le geometrie corrispondenti ad aree annesse derivanti da intersezione di oggetti afferenti a strati distinti vanno acquisite in maniera identica in ciascuno degli strati coinvolti.

Relazioni principali

La tabella è coinvolta solo in relazioni di decodifica dei valori degli attributi.

Campi

Chiavi primarie			
FILE_ID	Identificativo numerico univoco che contraddistingue ogni geometria nell'ambito della tabella.	Intero lungo	Obbligatorio
COD_ISTAT	Codice ISTAT del Comune al quale lo strato informativo si riferisce.	Stringa max 6 caratteri	Obbligatorio
Campi geometrici			
SHAPE	Campo geometrico poligonale relativo ad una singola istanza dello strato informativo; le geometrie sono 2D.	Tipo geometrico binario	Obbligatorio
Campi ulteriori			
DENOMINAZ	Denominazione associata all'area (fa riferimento ad un nome o un codice univoco).	Stringa max 255 caratteri (testo libero)	Obbligatorio
CLASSE	Codice del valore relativo all'attributo <i>classificazione</i> per lo strato informativo. Si fa riferimento a valori codificati in un dominio assegnato. Il valore mista può essere utilizzato in casi estremi solo per aree classificate come area annessa nell'attributo di tipo.	Stringa max 10 caratteri (valori codificati - v. cap.3.32 pag.53)	Obbligatorio
TIPO	Codice del valore relativo all'attributo <i>tipo</i> per lo strato informativo. Si fa riferimento a valori codificati in un dominio assegnato.	Stringa max 10 caratteri (valori codificati - v. cap.3.13 pag.50)	Obbligatorio
MOD_PUTT	Codice del valore relativo all'attributo	Stringa max 10 caratteri	Non obbligatorio

	inerente le modifiche in rapporto al PUTT/PBA in vigore. Si fa riferimento a valori codificati in un dominio assegnato.	(valori codificati - v. cap.3.15 pag.50)	
RIF_CL_INT	Codice del valore relativo all'attributo <i>riferimento alle classi intersecate</i> . Viene fatto riferimento a valori codificati in un dominio assegnato. Il campo va compilato solo per aree classificate come <i>area annessa</i> nell'attributo di tipo.	Stringa max 10 caratteri (valori codificati - v. cap.3.40 pag. 56)	Non obbligatorio
TIPO_FONTE	Descrizione testuale relativamente all'origine del dato inserito.	Stringa max 255 caratteri (testo libero)	Non obbligatorio

2.24 SIT_PUG26G_PUTT_ATDBEDI

Descrizione

La tabella è di natura geometrica e contiene lo strato informativo relativo ai **beni diffusi nel paesaggio agrario**, afferente alla tavola di adeguamento al Piano Urbanistico Territoriale Tematico Paesaggio e Beni Ambientali (PUTT/PBA) redatto a livello regionale. Gli oggetti geometrici sono poligonali in quanto si tratta di area di beni.

Riferimento alle "Linee Guida" DRAG/PUG

Appendice II - Promemoria sugli adeguamenti alle pianificazioni sovraordinate ed elenco dei pareri – L'adeguamento al Piano Urbanistico Territoriale Tematico/Paesaggio.

Regole di editing

Ad ogni areale individuato deve essere associato un insieme di attributi (informazioni) che lo identifichino e ne descrivano le caratteristiche per i beni diffusi nel paesaggio agrario.

Le geometrie corrispondenti ad aree annesse derivanti da intersezione di oggetti afferenti a strati distinti vanno acquisite in maniera identica in ciascuno degli strati coinvolti.

Relazioni principali

La tabella è coinvolta solo in relazioni di decodifica dei valori degli attributi.

Campi

Chiavi primarie			
FILE_ID	Identificativo numerico univoco che contraddistingue ogni geometria nell'ambito della tabella.	Intero lungo	Obbligatorio
COD_ISTAT	Codice ISTAT del Comune al quale lo strato informativo si riferisce.	Stringa max 6 caratteri	Obbligatorio
Campi geometrici			
SHAPE	Campo geometrico poligonale relativo ad una singola istanza dello strato informativo; le geometrie sono 2D.	Tipo geometrico binario	Obbligatorio
Campi ulteriori			
CLASSE	Codice del valore relativo all'attributo <i>classificazione</i> per lo strato informativo. Si fa riferimento a valori codificati in un dominio assegnato.	Stringa max 10 caratteri (valori codificati - v. cap.3.33 pag.54)	Obbligatorio
DESCRIZION	Descrizione associata al singolo elemento areale.	Stringa max 255 caratteri (testo libero)	Non obbligatorio
RIF_CL_INT	Codice del valore relativo all'attributo	Stringa max 10 caratteri	Non obbligatorio

	<i>riferimento alle classi intersecate</i> . Viene fatto riferimento a valori codificati in un dominio assegnato. Il campo va compilato solo per aree classificate come <i>area annessa</i> nell'attributo di tipo.	(valori codificati - v. cap.3.40 pag. 56)	
TIPO_FONTE	Descrizione testuale relativamente all'origine del dato inserito.	Stringa max 255 caratteri (testo libero)	Non obbligatorio

2.25 SIT_PUG71G_PUTT_ATDBEDI_L

Descrizione

La tabella è di natura geometrica e contiene lo strato informativo relativo ai **beni diffusi nel paesaggio agrario**, afferente alla tavola di adeguamento al Piano Urbanistico Territoriale Tematico Paesaggio e Beni Ambientali (PUTT/PBA) redatto a livello regionale.

Gli oggetti geometrici sono lineari in quanto beni non individuabili in termini di estensioni areali; si tratta di un'eccezione particolare rappresentata dal collassamento in linea in quanto del singolo bene è possibile definire un tracciato lineare ma non un ingombro areale.

Questo strato non è obbligatorio.

Riferimento alle "Linee Guida" DRAG/PUG

Appendice II - Promemoria sugli adeguamenti alle pianificazioni sovraordinate ed elenco dei pareri – L'adeguamento al Piano Urbanistico Territoriale Tematico/Paesaggio.

Regole di editing

L'utilizzo di questo strato informativo (lineare e non areale) è ammesso solo nei casi in cui non sia in alcun modo possibile il riconoscimento dell'area del bene; la restituzione delle aree annesse è comunque richiesta in formato areale, e verrà inserita nel corrispettivo strato areale. Ad ogni linea individuata deve essere associata un insieme di attributi che lo identifichino e ne descrivano le caratteristiche per i beni diffusi nel paesaggio agrario.

Relazioni principali

La tabella è coinvolta solo in relazioni di decodifica dei valori degli attributi.

Campi

Chiavi primarie			
FILE_ID	Identificativo numerico univoco che contraddistingue ogni geometria nell'ambito della tabella.	Intero lungo	Obbligatorio
COD_ISTAT	Codice ISTAT del Comune al quale lo strato informativo si riferisce.	Stringa max 6 caratteri	Obbligatorio
Campi geometrici			
SHAPE	Campo geometrico lineare relativo ad una singola istanza dello strato informativo; le geometrie sono 2D.	Tipo geometrico binario	Obbligatorio
Campi ulteriori			
CLASSE	Codice del valore relativo all'attributo <i>classificazione</i> per lo strato informativo. Si fa riferimento a valori codificati in un dominio assegnato.	Stringa max 10 caratteri (valori codificati - v. cap.3.33 pag.54)	Obbligatorio
DESCRIZION	Descrizione associata al singolo elemento areale.	Stringa max 255 caratteri (testo libero)	Non obbligatorio
TIPO_FONTE	Descrizione testuale relativamente all'origine del dato inserito.	Stringa max 255 caratteri (testo libero)	Non obbligatorio

2.26 SIT_PUG28G_PUTT_ATDBECU

Descrizione

La tabella è di natura geometrica e contiene lo strato informativo relativo ai **beni culturali**, afferente alla tavola di adeguamento al Piano Urbanistico Territoriale Tematico Paesaggio e Beni Ambientali (PUTT/PBA) redatto a livello regionale.

Gli oggetti geometrici sono poligonali.

Riferimento alle "Linee Guida" DRAG/PUG

Appendice II - Promemoria sugli adeguamenti alle pianificazioni sovraordinate ed elenco dei pareri - L'adeguamento al Piano Urbanistico Territoriale Tematico/Paesaggio.

Regole di editing

Gli strati informativi di adeguamento al piano urbanistico territoriale tematico/paesaggio hanno, nella maggior parte dei casi, come base le aree individuate dai PUTT/PBA come ATD, che vanno analizzate e verificate, nonché studi specifici. Ad ogni areale individuato deve essere associato un insieme di attributi (informazioni) che lo identifichino e ne descrivano le caratteristiche per i beni culturali e le rispettive aree annesse.

Le geometrie corrispondenti ad aree annesse derivanti da intersezione di oggetti afferenti a strati distinti vanno acquisite in maniera identica in ciascuno degli strati coinvolti.

Relazioni principali

La tabella è coinvolta solo in relazioni di decodifica dei valori degli attributi.

Campi

Chiavi primarie			
FILE_ID	Identificativo numerico univoco che contraddistingue ogni geometria nell'ambito della tabella.	Intero lungo	Obbligatorio
COD_ISTAT	Codice ISTAT del Comune al quale lo strato informativo si riferisce.	Stringa max 6 caratteri	Obbligatorio
Campi geometrici			
SHAPE	Campo geometrico poligonale relativo ad una singola istanza dello strato informativo; le geometrie sono 2D.	Tipo geometrico binario	Obbligatorio
Campi ulteriori			
DENOMINAZ	Denominazione associata al bene culturale (fa riferimento ad un nome o un codice univoco).	Stringa max 255 caratteri (testo libero)	Obbligatorio
CATEGORIA	Codice del valore relativo all'attributo <i>categoria</i> per lo strato informativo. Si fa riferimento a valori codificati in un dominio assegnato.	Stringa max 10 caratteri (valori codificati - v. cap.3.34 pag.54)	Obbligatorio
PERIM	Codice del valore relativo all'attributo <i>natura della perimetrazione</i> , che ha senso nel caso di bene appartenente alla categoria di segnalazione.	Stringa max 10 caratteri (valori codificati - v. cap.3.35 pag.54)	Non obbligatorio
CLASSE	Codice del valore relativo all'attributo <i>classificazione</i> per lo strato informativo. Si fa riferimento a valori codificati in un dominio assegnato. Il valore mista può essere utilizzato in casi estremi solo per aree classificate come area annessa	Stringa max 10 caratteri (valori codificati - v. cap.3.36 pag.54)	Obbligatorio

	nell'attributo di tipo.		
TIPO	Codice del valore relativo all'attributo <i>tipo</i> per lo strato informativo. Si fa riferimento a valori codificati in un dominio assegnato.	Stringa max 10 caratteri (valori codificati - v. cap.3.13 pag.50)	Obbligatorio
MOD_PUTT	Codice del valore relativo all'attributo inerente le modifiche in rapporto al PUTT/PBA in vigore. Si fa riferimento a valori codificati in un dominio assegnato.	Stringa max 10 caratteri (valori codificati - v. cap.3.15 pag.50)	Non obbligatorio
RIF_CL_INT	Codice del valore relativo all'attributo <i>riferimento alle classi intersecate</i> . Viene fatto riferimento a valori codificati in un dominio assegnato. Il campo va compilato solo per aree classificate come <i>area annessa</i> nell'attributo di tipo.	Stringa max 10 caratteri (valori codificati - v. cap.3.40 pag. 56)	Non obbligatorio
TIPO_FONTE	Descrizione testuale relativamente all'origine del dato inserito.	Stringa max 255 caratteri (testo libero)	Non obbligatorio
ID_CB_SITO	Identificativo dell'elemento secondo la Carta dei Beni Culturali.	Stringa max 50 caratteri (testo libero)	Non obbligatorio
ID_CB_VINCOLO	Identificativo dell'elemento secondo la Carta dei Beni Culturali.	Stringa max 50 caratteri (testo libero)	Non obbligatorio
ID_PCT	Identificativo dell'elemento secondo il Piano Comunale dei Tratturi, se realizzato ed informatizzato.	Stringa max 50 caratteri (testo libero)	Non obbligatorio

2.27 SIT_PUG60G_PUTT_ATDBECU_P

Descrizione

La tabella è di natura geometrica e contiene lo strato informativo relativo ai **beni culturali**, afferente alla tavola di adeguamento al Piano Urbanistico Territoriale Tematico Paesaggio e Beni Ambientali (PUTT/PBA) redatto a livello regionale.

Gli oggetti geometrici sono puntuali in quanto beni non individuabili in termini di estensioni areali; si tratta di un'eccezione particolare rappresentata dal collassamento in linea in quanto del singolo bene è possibile una localizzazione puntuale ma non un ingombro areale.

Questo strato non è obbligatorio.

Riferimento alle "Linee Guida" DRAG/PUG

Appendice II - Promemoria sugli adeguamenti alle pianificazioni sovraordinate ed elenco dei pareri – L'adeguamento al Piano Urbanistico Territoriale Tematico/Paesaggio.

Regole di editing

Gli strati informativi di adeguamento al piano urbanistico territoriale tematico/paesaggio hanno, nella maggior parte dei casi, come base le aree individuate dai PUTT/PBA come ATD, che vanno analizzate e verificate, nonché studi specifici. L'utilizzo di questo strato informativo (puntuale e non areale) è ammesso solo nei casi di segnalazioni archeologiche (raramente architettoniche) quando non è in alcun modo possibile il riconoscimento dell'area del bene; la restituzione delle aree annesse è comunque richiesta in formato areale, e verrà inserita nel corrispettivo strato areale. Ad ogni punto individuato deve essere associato un insieme di attributi (informazioni) che lo identifichino e ne descrivano le caratteristiche per i beni culturali.

Relazioni principali

La tabella è coinvolta solo in relazioni di decodifica dei valori degli attributi.

Campi

Chiavi primarie			
FILE_ID	Identificativo numerico univoco che contraddistingue ogni geometria nell'ambito della tabella.	Intero lungo	Obbligatorio
COD_ISTAT	Codice ISTAT del Comune al quale lo strato informativo si riferisce.	Stringa max 6 caratteri	Obbligatorio
Campi geometrici			
SHAPE	Campo geometrico poligonale relativo ad una singola istanza dello strato informativo; le geometrie sono 2D.	Tipo geometrico binario	Obbligatorio
Campi ulteriori			
DENOMINAZ	Denominazione associata al bene culturale (fa riferimento ad un nome o un codice univoco).	Stringa max 255 caratteri (testo libero)	Obbligatorio
CATEGORIA	Codice del valore relativo all'attributo <i>categoria</i> per lo strato informativo. Si fa riferimento a valori codificati in un dominio assegnato.	Stringa max 10 caratteri (valori codificati - v. cap.3.37 pag.55)	Obbligatorio
CLASSE	Codice del valore relativo all'attributo <i>classificazione</i> per lo strato informativo. Si fa riferimento a valori codificati in un dominio assegnato.	Stringa max 10 caratteri (valori codificati - v. cap.3.36 pag.54)	Obbligatorio
MOD_PUTT	Codice del valore relativo all'attributo inerente le modifiche in rapporto al PUTT/PBA in vigore. Si fa riferimento a valori codificati in un dominio assegnato.	Stringa max 10 caratteri (valori codificati - v. cap.3.17 pag.51)	Non obbligatorio
TIPO_FONTE	Descrizione testuale relativamente all'origine del dato inserito.	Stringa max 255 caratteri (testo libero)	Non obbligatorio
ID_CB_SITO	Identificativo dell'elemento secondo la Carta dei Beni Culturali.	Stringa max 50 caratteri (testo libero)	Non obbligatorio

2.28 SIT_PUG77G_PUTT_ATDBECU_L**Descrizione**

La tabella è di natura geometrica e contiene lo strato informativo relativo ai **beni culturali**, afferente alla tavola di adeguamento al Piano Urbanistico Territoriale Tematico Paesaggio e Beni Ambientali (PUTT/PBA) redatto a livello regionale.

Gli oggetti geometrici sono lineari in quanto beni non individuabili in termini di estensioni areali; si tratta di un'eccezione particolare rappresentata dal collassamento in linea in quanto del singolo bene è possibile definire un tracciato lineare ma non un ingombro areale.

Questo strato non è obbligatorio.

Riferimento alle "Linee Guida" DRAG/PUG

Appendice II - Promemoria sugli adeguamenti alle pianificazioni sovraordinate ed elenco dei pareri – L'adeguamento al Piano Urbanistico Territoriale Tematico/Paesaggio.

Regole di editing

Gli strati informativi di adeguamento al piano urbanistico territoriale tematico/paesaggio hanno,

nella maggior parte dei casi, come base le aree individuate dai PUTT/PBA come ATD, che vanno analizzate e verificate, nonché studi specifici. L'utilizzo di questo strato informativo (lineare e non areale) è ammesso solo nei casi di segnalazioni archeologiche o architettoniche quando non è in alcun modo possibile il riconoscimento dell'area del bene; la restituzione delle aree annesse è comunque richiesta in formato areale, e verrà inserita nel corrispettivo strato areale. Ad ogni linea individuata deve essere associato un insieme di attributi (informazioni) che lo identifichino e ne descrivano le caratteristiche per i beni culturali.

Relazioni principali

La tabella è coinvolta solo in relazioni di decodifica dei valori degli attributi.

Campi

Chiavi primarie			
FILE_ID	Identificativo numerico univoco che contraddistingue ogni geometria nell'ambito della tabella.	Intero lungo	Obbligatorio
COD_ISTAT	Codice ISTAT del Comune al quale lo strato informativo si riferisce.	Stringa max 6 caratteri	Obbligatorio
Campi geometrici			
SHAPE	Campo geometrico poligonale relativo ad una singola istanza dello strato informativo; le geometrie sono 2D.	Tipo geometrico binario	Obbligatorio
Campi ulteriori			
DENOMINAZ	Denominazione associata al bene culturale (fa riferimento ad un nome o un codice univoco).	Stringa max 255 caratteri (testo libero)	Obbligatorio
CATEGORIA	Codice del valore relativo all'attributo <i>categoria</i> per lo strato informativo. Si fa riferimento a valori codificati in un dominio assegnato.	Stringa max 10 caratteri (valori codificati - v. cap.3.37 pag.55)	Obbligatorio
CLASSE	Codice del valore relativo all'attributo <i>classificazione</i> per lo strato informativo. Si fa riferimento a valori codificati in un dominio assegnato.	Stringa max 10 caratteri (valori codificati - v. cap.3.36 pag.54)	Obbligatorio
MOD_PUTT	Codice del valore relativo all'attributo inerente le modifiche in rapporto al PUTT/PBA in vigore. Si fa riferimento a valori codificati in un dominio assegnato.	Stringa max 10 caratteri (valori codificati - v. cap.3.16 pag.50)	Non obbligatorio
TIPO_FONTE	Descrizione testuale relativamente all'origine del dato inserito.	Stringa max 255 caratteri (testo libero)	Non obbligatorio
ID_CB_SITO	Identificativo dell'elemento secondo la Carta dei Beni Culturali.	Stringa max 50 caratteri (testo libero)	Non obbligatorio
ID_PCT	Identificativo dell'elemento secondo il Piano Comunale dei Tratturi, se realizzato ed informatizzato.	Stringa max 50 caratteri (testo libero)	Non obbligatorio

2.29 SIT_PUG31G_PUTT_ATDPAGRI

Descrizione

La tabella è di natura geometrica e contiene lo strato informativo relativo al **paesaggio agrario**, afferente alla tavola di adeguamento al Piano Urbanistico Territoriale Tematico Paesaggio e Beni Ambientali (PUTT/PBA) redatto a livello regionale.

Gli oggetti geometrici sono poligonali.

Riferimento alle "Linee Guida" DRAG/PUG

Appendice II - Promemoria sugli adeguamenti alle pianificazioni sovraordinate ed elenco dei pareri – L'adeguamento al Piano Urbanistico Territoriale Tematico/Paesaggio.

Regole di editing

Ad ogni areale individuato deve essere associato un insieme di attributi (informazioni) che lo identifichino e ne descrivano le caratteristiche per il paesaggio agrario.

Le geometrie corrispondenti ad aree annesse derivanti da intersezione di oggetti afferenti a strati distinti vanno acquisite in maniera identica in ciascuno degli strati coinvolti.

Relazioni principali

La tabella è coinvolta solo in relazioni di decodifica dei valori degli attributi.

Campi

Chiavi primarie			
FILE_ID	Identificativo numerico univoco che contraddistingue ogni geometria nell'ambito della tabella.	Intero lungo	Obbligatorio
COD_ISTAT	Codice ISTAT del Comune al quale lo strato informativo si riferisce.	Stringa max 6 caratteri	Obbligatorio
Campi geometrici			
SHAPE	Campo geometrico poligonale relativo ad una singola istanza dello strato informativo; le geometrie sono 2D.	Tipo geometrico binario	Obbligatorio
Campi ulteriori			
CLASSE	Codice del valore relativo all'attributo <i>classificazione</i> per lo strato informativo. Si fa riferimento a valori codificati in un dominio assegnato. Il valore mista può essere utilizzato in casi estremi solo per aree classificate come area annessa nell'attributo di tipo.	Stringa max 10 caratteri (valori codificati - v. cap.3.38 pag.55)	Obbligatorio
DESCRIZION	Descrizione associata al singolo elemento areale.	Stringa max 255 caratteri (testo libero)	Non obbligatorio
RIF_CL_INT	Codice del valore relativo all'attributo <i>riferimento alle classi intersecate</i> . Viene fatto riferimento a valori codificati in un dominio assegnato. Il campo va compilato solo per aree classificate come <i>area annessa</i> nell'attributo di tipo.	Stringa max 10 caratteri (valori codificati - v. cap.3.40 pag. 56)	Non obbligatorio
TIPO_FONTE	Descrizione testuale relativamente all'origine del dato inserito.	Stringa max 255 caratteri (testo libero)	Non obbligatorio

2.30 SIT_PUG33G_PUTT_ATDCIVIC

Descrizione

La tabella è di natura geometrica e contiene lo strato informativo relativo agli **usi civici**, afferente alla tavola di adeguamento al Piano Urbanistico Territoriale Tematico Paesaggio e Beni Ambientali (PUTT/PBA) redatto a livello regionale.

Gli oggetti geometrici sono poligonali.

Riferimento alle "Linee Guida" DRAG/PUG

Appendice II - Promemoria sugli adeguamenti alle pianificazioni sovraordinate ed elenco dei pareri - L'adeguamento al Piano Urbanistico Territoriale Tematico/Paesaggio.

Regole di editing

Gli strati informativi di adeguamento al piano urbanistico territoriale tematico/paesaggio hanno, nella maggior parte dei casi, come base le aree individuate dai PUTT/PBA come ATD, che vanno analizzate e verificate, nonché studi specifici. Ad ogni areale individuato deve essere associato un insieme di attributi (informazioni) che lo identifichino e ne descrivano le caratteristiche per gli usi civici.

Le geometrie corrispondenti ad aree annesse derivanti da intersezione di oggetti afferenti a strati distinti vanno acquisite in maniera identica in ciascuno degli strati coinvolti.

Relazioni principali

La tabella è coinvolta solo in relazioni di decodifica dei valori degli attributi.

Campi

Chiavi primarie			
FILE_ID	Identificativo numerico univoco che contraddistingue ogni geometria nell'ambito della tabella.	Intero lungo	Obbligatorio
COD_ISTAT	Codice ISTAT del Comune al quale lo strato informativo si riferisce.	Stringa max 6 caratteri	Obbligatorio
Campi geometrici			
SHAPE	Campo geometrico poligonale relativo ad una singola istanza dello strato informativo; le geometrie sono 2D.	Tipo geometrico binario	Obbligatorio
Campi ulteriori			
CLASSE	Codice del valore relativo all'attributo <i>classificazione</i> per lo strato informativo. Si fa riferimento a valori codificati in un dominio assegnato. Il valore mista può essere utilizzato in casi estremi solo per aree classificate come area annessa nell'attributo di tipo.	Stringa max 10 caratteri (valori codificati - v. cap.3.39 pag.56)	Obbligatorio
MOD_PUTT	Codice del valore relativo all'attributo inerente le modifiche in rapporto al PUTT/PBA in vigore. Si fa riferimento a valori codificati in un dominio assegnato.	Stringa max 10 caratteri (valori codificati - v. cap.3.15 pag.50)	Non obbligatorio
DESCRIZION	Descrizione associata al singolo elemento areale.	Stringa max 255 caratteri (testo libero)	Non obbligatorio
RIF_CL_INT	Codice del valore relativo all'attributo <i>riferimento alle classi intersecate</i> . Viene fatto riferimento a valori codificati in un dominio assegnato. Il campo va compilato solo per aree classificate come <i>area annessa</i> nell'attributo di tipo.	Stringa max 10 caratteri (valori codificati - v. cap.3.40 pag. 56)	Non obbligatorio
TIPO_FONTE	Descrizione testuale relativamente all'origine del dato inserito.	Stringa max 255 caratteri (testo libero)	Non obbligatorio
ATTO	Riferimenti all'atto relativo al bene in questione.	Stringa max 255 caratteri (testo libero)	Non obbligatorio
PERIZIA	Riferimenti alla perizia relativa al bene in questione.	Stringa max 255 caratteri (testo libero)	Non obbligatorio

2.31 SIT_PUG69G_PUTT_ATDAREEPA

Descrizione

La tabella è di natura geometrica e contiene lo strato informativo relativo alle **aree panoramiche**, afferente alla tavola di adeguamento al Piano Urbanistico Territoriale Tematico Paesaggio e Beni Ambientali (PUTT/PBA) redatto a livello regionale.

Gli oggetti geometrici sono poligonali.

Riferimento alle "Linee Guida" DRAG/PUG

Appendice II - Promemoria sugli adeguamenti alle pianificazioni sovraordinate ed elenco dei pareri - L'adeguamento al Piano Urbanistico Territoriale Tematico/Paesaggio.

Regole di editing

Ad ogni areale individuato deve essere associato un insieme di attributi (informazioni) che lo identifichino e ne descrivano le caratteristiche per le aree panoramiche.

Relazioni principali

La tabella non è coinvolta in alcuna relazione.

Campi

Chiavi primarie			
FILE_ID	Identificativo numerico univoco che contraddistingue ogni geometria nell'ambito della tabella.	Intero lungo	Obbligatorio
COD_ISTAT	Codice ISTAT del Comune al quale lo strato informativo si riferisce.	Stringa max 6 caratteri	Obbligatorio
Campi geometrici			
SHAPE	Campo geometrico poligonale relativo ad una singola istanza dello strato informativo; le geometrie sono 2D.	Tipo geometrico binario	Obbligatorio
Campi ulteriori			
DENOMINAZ	Denominazione associata al singolo punto panoramico (fa riferimento ad un nome o un codice univoco).	Stringa max 255 caratteri (testo libero)	Obbligatorio
DESCRIZION	Descrizione associata al singolo elemento puntuale.	Stringa max 255 caratteri (testo libero)	Non obbligatorio
TIPO_FONTE	Descrizione testuale relativamente all'origine del dato inserito.	Stringa max 255 caratteri (testo libero)	Non obbligatorio

2.32 SIT_PUG35G_PUTT_ATDPUPA

Descrizione

La tabella è di natura geometrica e contiene lo strato informativo relativo ai **punti panoramici** acquisibili solo come punti, afferente alla tavola di adeguamento al Piano Urbanistico Territoriale Tematico Paesaggio e Beni Ambientali (PUTT/PBA) redatto a livello regionale.

Gli oggetti geometrici sono puntuali.

Riferimento alle "Linee Guida" DRAG/PUG

Appendice II - Promemoria sugli adeguamenti alle pianificazioni sovraordinate ed elenco dei pareri - L'adeguamento al Piano Urbanistico Territoriale Tematico/Paesaggio.

Regole di editing

Ad ogni punto individuato deve essere associato un insieme di attributi (informazioni) che lo identifichino e ne descrivano le caratteristiche per i punti panoramici.

Relazioni principali

La tabella non è coinvolta in alcuna relazione.

Campi

Chiavi primarie			
FILE_ID	Identificativo numerico univoco che contraddistingue ogni geometria nell'ambito della tabella.	Intero lungo	Obbligatorio
COD_ISTAT	Codice ISTAT del Comune al quale lo strato informativo si riferisce.	Stringa max 6 caratteri	Obbligatorio
Campi geometrici			
SHAPE	Campo geometrico puntuale relativo ad una singola istanza dello strato informativo; le geometrie sono 2D.	Tipo geometrico binario	Obbligatorio
Campi ulteriori			
DENOMINAZ	Denominazione associata al singolo punto panoramico (fa riferimento ad un nome o un codice univoco).	Stringa max 255 caratteri (testo libero)	Obbligatorio
DESCRIZION	Descrizione associata al singolo elemento puntuale.	Stringa max 255 caratteri (testo libero)	Non obbligatorio
TIPO_FONTE	Descrizione testuale relativamente all'origine del dato inserito.	Stringa max 255 caratteri (testo libero)	Non obbligatorio

2.33 SIT_PUG36G_PUTT_ATDSTRAP**Descrizione**

La tabella è di natura geometrica e contiene lo strato informativo relativo alle **strade panoramiche**, afferente alla tavola di adeguamento al Piano Urbanistico Territoriale Tematico Paesaggio e Beni Ambientali (PUTT/PBA) redatto a livello regionale.

Gli oggetti geometrici sono lineari.

Riferimento alle "Linee Guida" DRAG/PUG

Appendice II - Promemoria sugli adeguamenti alle pianificazioni sovraordinate ed elenco dei pareri – L'adeguamento al Piano Urbanistico Territoriale Tematico/Paesaggio.

Regole di editing

Ad ogni linea individuata deve essere associata un insieme di attributi (informazioni) che la identifichino e ne descrivano le caratteristiche per le strade panoramiche.

Relazioni principali

La tabella non è coinvolta in alcuna relazione

Campi

Chiavi primarie			
FILE_ID	Identificativo numerico univoco che contraddistingue ogni geometria nell'ambito della tabella.	Intero lungo	Obbligatorio

COD_ISTAT	Codice ISTAT del Comune al quale lo strato informativo si riferisce.	Stringa max 6 caratteri	Obbligatorio
Campi geometrici			
SHAPE	Campo geometrico lineare relativo ad una singola istanza dello strato informativo; le geometrie sono 2D.	Tipo geometrico binario	Obbligatorio
Campi ulteriori			
DENOMINAZ	Denominazione associata alla singola strada panoramica (fa riferimento ad un nome o un codice univoco).	Stringa max 255 caratteri (testo libero)	Obbligatorio
DESCRIZION	Descrizione associata al singolo elemento lineare.	Stringa max 255 caratteri (testo libero)	Non obbligatorio
TIPO_FONTE	Descrizione testuale relativamente all'origine del dato inserito.	Stringa max 255 caratteri (testo libero)	Non obbligatorio

2.34 SIT_PUG37G_PUTT_ATE

Descrizione

La tabella è di natura geometrica e contiene lo strato informativo relativo agli **ambiti territoriali estesi**, afferente alla tavola di adeguamento al Piano Urbanistico Territoriale Tematico Paesaggio e Beni Ambientali (PUTT/PBA) redatto a livello regionale. Gli oggetti geometrici sono poligonali.

Riferimento alle "Linee Guida" DRAG/PUG

Appendice II - Promemoria sugli adeguamenti alle pianificazioni sovraordinate ed elenco dei pareri – L'adeguamento al Piano Urbanistico Territoriale Tematico/Paesaggio.

Regole di editing

La tavola di adeguamento al PUTT/PBA ha come base le aree individuate dai PUTT/PBA come Ambiti territoriali estesi. Non è sufficiente la digitalizzazione delle perimetrazioni degli ATE cartografati nel PUTT/PBA ma è anche necessario che queste vengano verificate e riperimate a scala di maggior dettaglio, aggiornate ed eventualmente integrate. Ad ogni areale individuato deve essere associato un insieme di attributi (informazioni) che lo identifichino e ne descrivano le caratteristiche.

Relazioni principali

La tabella è coinvolta solo in relazioni di decodifica dei valori degli attributi.

Campi

Chiavi primarie			
FILE_ID	Identificativo numerico univoco che contraddistingue ogni geometria nell'ambito della tabella.	Intero lungo	Obbligatorio
COD_ISTAT	Codice ISTAT del Comune al quale lo strato informativo si riferisce.	Stringa max 6 caratteri	Obbligatorio
Campi geometrici			
SHAPE	Campo geometrico poligonale relativo ad una singola istanza dello strato informativo; le geometrie sono 2D.	Tipo geometrico binario	Obbligatorio
Campi ulteriori			
CLASSE	Codice del valore relativo all'attributo <i>classificazione</i> per lo strato informativo. Si fa riferimento a valori codificati in un	Stringa max 10 caratteri (valori codificati - v. cap.3.41 pag.56)	Obbligatorio

	dominio assegnato.		
MOD_PUTT	Codice del valore relativo all'attributo inerente le modifiche in rapporto al PUTT/PBA in vigore. Si fa riferimento a valori codificati in un dominio assegnato.	Stringa max 10 caratteri (valori codificati - v. cap.3.14 pag.50)	Non obbligatorio

2.35 SIT_PUG39G_PUTT_TC

Descrizione

La tabella è di natura geometrica e contiene lo strato informativo relativo ai **territori costruiti**, afferente alla tavola di adeguamento al Piano Urbanistico Territoriale Tematico Paesaggio e Beni Ambientali (PUTT/PBA) redatto a livello regionale.

Gli oggetti geometrici sono poligonal.

Riferimento alle "Linee Guida" DRAG/PUG

Appendice II - Promemoria sugli adeguamenti alle pianificazioni sovraordinate ed elenco dei pareri - L'adeguamento al Piano Urbanistico Territoriale Tematico/Paesaggio.

Regole di editing

Le aree devono essere perimetrate tenendo conto dell'art. 1.03 comma 5 delle NTA del PUTT/P. Ad ogni areale individuato deve essere associato un insieme di attributi (informazioni) che lo identifichino e ne descrivano le caratteristiche.

Relazioni principali

La tabella è coinvolta solo in relazioni di decodifica dei valori degli attributi.

Campi

Chiavi primarie			
FILE_ID	Identificativo numerico univoco che contraddistingue ogni geometria nell'ambito della tabella.	Intero lungo	Obbligatorio
COD_ISTAT	Codice ISTAT del Comune al quale lo strato informativo si riferisce.	Stringa max 6 caratteri	Obbligatorio
Campi geometrici			
SHAPE	Campo geometrico poligonale relativo ad una singola istanza dello strato informativo; le geometrie sono 2D.	Tipo geometrico binario	Obbligatorio
Campi ulteriori			
CLASSE	Codice del valore relativo all'attributo <i>classificazione</i> per lo strato informativo. Si fa riferimento a valori codificati in un dominio assegnato.	Stringa max 10 caratteri (valori codificati - v. cap.3.42 pag.56)	Obbligatorio

2.36 SIT_PUG79G_VINCOLI

Descrizione

La tabella è di natura geometrica e contiene lo strato informativo relativo alle aree vincolate secondo differenti tipologie di vincoli (vedi dominio associato).

Gli oggetti geometrici sono poligonal.

Relazioni principali

La tabella è coinvolta solo in relazioni di decodifica dei valori degli attributi.

Campi

Chiavi primarie			
FILE_ID	Identificativo numerico univoco che contraddistingue ogni geometria nell'ambito della tabella.	Intero lungo	Obbligatorio
COD_ISTAT	Codice ISTAT del Comune al quale lo strato informativo si riferisce.	Stringa max 6 caratteri	Obbligatorio
Campi geometrici			
SHAPE	Campo geometrico poligonale relativo ad una singola istanza dello strato informativo; le geometrie sono 2D.	Tipo geometrico binario	Obbligatorio
Campi ulteriori			
TIPO	Codice del valore relativo all'attributo <i>tipo</i> per lo strato informativo. Si fa riferimento a valori codificati in un dominio assegnato.	Stringa max 12 caratteri (valori codificati - v. cap.3.43 pag.56)	Obbligatorio
DESCRIZION	Descrizione associata al singolo elemento areale.	Stringa max 255 caratteri (testo libero)	Non obbligatorio
RIF_NORME	Riferimento alle normative che definiscono il vincolo.	Stringa max 255 caratteri (testo libero)	Non obbligatorio
RIF_CAT	Riferimento alle particelle catastali che identificano il vincolo.	Stringa max 255 caratteri (testo libero)	Non obbligatorio
TIPO_FONTE	Descrizione testuale relativamente all'origine del dato inserito	Stringa max 255 caratteri (testo libero)	Non obbligatorio
ID_CB_VINCOLO	Identificativo dell'elemento secondo la Carta dei Beni Culturali.	Stringa max 50 caratteri (testo libero)	Non obbligatorio

3 Contenuto delle tabelle dei domini codificati

3.1 SIT_PUG46T_C_CLASSE_INF

Codice	Descrizione
01	infrastruttura per la mobilità di merci e persone
02	infrastruttura igienico-sanitaria
03	infrastruttura tecnologica
04	attrezzatura e dotazione di interesse collettivo
05	nodo ad elevata specializzazione funzionale
06	altro

3.2 SIT_PUG47T_C_TIPO_INF

Codice	Descrizione
01	area di pertinenza – superficie esatta dell'infrastruttura
02	fascia di rispetto – estesa secondo le norme vigenti in base alla infrastruttura a cui si riferisce
03	giacitura di massima – per elementi non esattamente individuati

3.3 SIT_PUG48T_C_STA_FATTO_INF

Codice	Descrizione
01	esistente, in funzione/aperta all'uso
02	esistente, non in funzione
03	di previsione superficie disponibile
04	di previsione superficie non disponibile

3.4 SIT_PUG50T_C_AMBITO

Codice	Descrizione
U	urbano
R	rurale

3.5 SIT_PUG51T_C_TIPO_CT

Codice	Descrizione
U1	urbano da tutelare
U2	consolidato e da consolidare, mantenere e qualificare
U3	periferico e marginale da riqualificare
U4	in formazione in modalità accentrate o diffuse da completare e consolidare
U5	da destinare a insediamenti di nuovo impianto
U6	altra tipologia di contesto urbano
R1	periurbano da riqualificare
R2	multifunzionale da tutelare

R3	marginale da rifunzionalizzare
R4	a prevalente funzione agricola da tutelare e rafforzare
R5	a prevalente valore ambientale e paesaggistico
R6	altra tipologia di contesto rurale

3.6 SIT_PUG64T_C_MOD_ATT_PP

Codice	Descrizione
01	attuazione diretta
02	attuazione diretta condizionata
03	attuazione indiretta tramite uno o più PUE
04	attuazione indiretta tramite procedura selettiva

3.7 SIT_PUG65T_C_AMB_APPL_PP

Codice	Descrizione
01	relative alle trasformazioni
02	relative alla gestione dell'esistente

3.8 SIT_PUG66T_C_ARCO_VAL_PP

Codice	Descrizione
01	fino ad un massimo di 5 anni
02	fino ad un massimo di 10 anni
03	indeterminato
04	condizionato

3.9 SIT_PUG02T_C_CLASSE_PAI_PG

Codice	Descrizione
PG1	area a pericolosità geomorfologica media e moderata
PG2	area a pericolosità geomorfologica elevata
PG3	area a pericolosità geomorfologica molto elevata

3.10 SIT_PUG04T_C_CLASSE_PAI_PI

Codice	Descrizione
AP	area ad alta pericolosità idraulica
MP	area a media pericolosità idraulica
BP	area a bassa pericolosità idraulica

3.11 SIT_PUG06T_C_CLASSE_PAI_R

Codice	Descrizione
R1	area a rischio moderato
R2	area a rischio medio

R3	area a rischio elevato
R4	area a rischio molto elevato

3.12 SIT_PUG08T_C_CLASSE_ATDGEOL

Codice	Descrizione
01	elemento strutturale
02	elemento litologico
03	elemento fossilifero
04	mista

3.13 SIT_PUG09T_C_TIPO_PUTT

Codice	Descrizione
01	area di pertinenza
02	area annessa

3.14 SIT_PUG12T_C_MOD_PUTT

Codice	Descrizione
01	recepito dallo strato informativo esistente senza modifiche
02	riperimetrazione dovuta esclusivamente alla scala di maggior dettaglio
0201	riperimetrazione dovuta esclusivamente alla scala di maggior dettaglio con modifica del livello di valore paesaggistico
03	modifica sostanziale della perimetrazione
0301	modifica sostanziale della perimetrazione con modifica del livello di valore paesaggistico
04	inserimento del nuovo elemento perché non considerato dal PUTT

3.15 SIT_PUG54T_C_MOD_PUTT_A

Codice	Descrizione
01	recepito dallo strato informativo esistente senza modifiche
02	riperimetrazione dovuta esclusivamente alla scala di maggior dettaglio
03	modifica sostanziale della perimetrazione
04	inserimento del nuovo elemento perché non considerato dal PUTT

3.16 SIT_PUG55T_C_MOD_PUTT_L

Codice	Descrizione
01	recepito dallo strato informativo esistente senza modifiche
02	modifica dovuta esclusivamente alla scala di maggior dettaglio
03	modifica sostanziale
04	inserimento del nuovo elemento perché non considerato dal PUTT

3.17 SIT_PUG56T_C_MOD_PUTT_P

Codice	Descrizione
01	recepito dallo strato informativo esistente senza modifiche
02	spostamento dovuto esclusivamente alla scala di maggior dettaglio
03	spostamento sostanziale
04	inserimento del nuovo elemento perché non considerato dal PUTT

3.18 SIT_PUG11T_C_CLASSE_ATDGROTTE

Codice	Descrizione
01	grotta
02	dolina, pulo, vora, inghiottitoio
03	mista

3.19 SIT_PUG14T_C_CLASSE_ATDCOSTE

Codice	Descrizione
01	alta a versante
02	alta a terrazzi
03	a fascia litoranea stretta
04	bassa di pianura
05	mista

3.20 SIT_PUG18T_C_TIPO_ADTCOSTE

Codice	Descrizione
01	zona litoranea
02	area annessa
03	zona adlitoranea
04	mista

3.21 SIT_PUG73T_C_DESC_CI_ATDCOSTE

Codice	Descrizione
01	costa rocciosa
0101	costa rocciosa con spiaggia ciottolosa al piede
0102	costa rocciosa con spiaggia sabbiosa al piede
02	falesia
0201	falesia con spiaggia ciottolosa al piede
0202	falesia con spiaggia sabbiosa al piede
03	rias
04	spiaggia sabbiosa
05	spiaggia ciottolosa
06	spiaggia sabbiosa-ciottolosa
07	cordone dunare
08	opera di difesa

3.22 SIT_PUG81T_C_CLASSE_ATDIDRO_BACINO

Codice	Descrizione
01	con costa alta a versante
02	con costa alta a terrazzi
03	con costa a fascia litoranea stretta
04	con costa bassa di pianura
05	mista

3.23 SIT_PUG76T_C_DESC_CI_ATDIDROB

Codice	Descrizione
01	lago naturale
02	lago artificiale
03	laguna

3.24 SIT_PUG16T_C_CLASSE_ATDIDRO_CORSO

Codice	Descrizione
01	corso d'acqua, fiume, torrente, canale
02	gravina, lama
03	pantano, acquitrino
04	vasca, salina
05	sorgente
06	mista

3.25 SIT_PUG75T_C_DESC_CI_ATDIDROC

Codice	Descrizione
01	corso d'acqua
0101	corso d'acqua episodico
0102	corso d'acqua obliterato
0103	corso d'acqua tombato
02	canale lagunare
03	ripa di erosione
04	ciglio di sponda
05	salina
06	stagno, acquitrino, zona palustre

3.26 SIT_PUG59T_C_CLASSE_ATDIDRO_L

Codice	Descrizione
01	corso d'acqua, fiume, torrente, canale
02	gravina, lama

3.27 SIT_PUG78T_C_DESC_CI_ATDIDRO_L

Codice	Descrizione
01	corso d'acqua
0101	corso d'acqua episodico
0102	corso d'acqua obliterato
0103	corso d'acqua tombato
02	canale lagunare
03	ripa di erosione
04	ciglio di sponda

3.28 SIT_PUG17T_C_PROPR_ATDIDRO

Codice	Descrizione
01	acqua pubblica
02	acqua non pubblica

3.29 SIT_PUG20T_C_CLASSE_ATDVECRI

Codice	Descrizione
01	pendenza > 30 %
02	pendenza < 30%
03	mista

3.30 SIT_PUG21T_C_TIPO_ATDVECRI

Codice	Descrizione
01	area di versante
02	area annessa al ciglio/crinale

3.31 SIT_PUG23T_C_CLASSE_ATDBOMA

Codice	Descrizione
01	bosco
02	macchia
03	mista

3.32 SIT_PUG25T_C_CLASSE_ATDNATURA

Codice	Descrizione
01	oasi di protezione
02	zona di ripopolamento e cattura
03	zona a gestione sociale
04	azienda agricola centro produzione privata per la selvaggina
05	zona addestramento cani
06	azienda faunistico-venatoria

07	zona umida
08	riserva naturale orientata
09	riserva naturale integrale
10	parco naturale attrezzato
11	riserva naturale biogenetica
12	riserva naturale forestale di protezione
13	bandita di caccia
14	biotopi
15	mista

3.33 SIT_PUG27T_C_CLASSE_ATDBEDI

Codice	Descrizione
01	piante isolate o a gruppi, sparse, di rilevante importanza
02	alberatura stradale e poderale
03	parete a secco con relative siepi
04	mista

3.34 SIT_PUG29T_C_CATEG_ATDBECU

Codice	Descrizione
01	vincolo archeologico
02	segnalazione archeologica
03	vincolo architettonico
04	segnalazione architettonica
05	segnalazione archeologica e architettonica subordinata all'autorizzazione della soprintendenza archeologica
06	segnalazione archeologica e architettonica subordinata a comunicazione della soprintendenza archeologica
07	mista

3.35 SIT_PUG53T_C_PERIM_ATDBECU

Codice	Descrizione
01	perimetrazione effettiva
02	perimetrazione ipotetica, di massima

3.36 SIT_PUG30T_C_CLASSE_ATDBECU

Codice	Descrizione
01	agro
02	area archeologica
03	abitato
04	abbazia
05	casino, caselle, casole, casale, casalino, casa, posta, riparo, casone, stazionamento
06	castello
07	contrada
08	chiesa, cattedrale, cripta, basilica, chiostro

09	convento, badia, monastero
10	cappella
11	chiesa rupestre o rurale
12	pulo, gravina, gorgo, lama, cava, vallone, valle, caverna, antro, foce, collina, colle
13	seminario
14	centro urbano, cittadella
15	dolmen
16	grotta
17	insediamento
18	ipogeo, cava ipogea
19	lago, cisterna, canale
20	località, borgo
21	menhir
22	masseria, masseriola, trullo, fattoria, iazzo, taverna, fortino
23	necropoli
24	ponte
25	palazzo, edificio, tempio, anfiteatro, monumento
26	resti, residui, ruderi, rovine, cippo, colonna, pietre miliari, stele
27	specchia
28	strutture abitative
29	santuario
30	tombe, sepolture
31	torre, torretta, torrione
32	tracciato
33	trappeto, frantoio
34	tratturo, traturello
35	villaggio
36	villa, villino
37	molo, colombaia, cala, pozzi, epitaffio, titolo, cinta muraria, mura, buca, tettoie, braccio, piazza, parco, complesso, fontana, monte, bonifici, pedali, portale, giardino, rione, pozzo, arco, acquedotto, zona, serra, vigne, podere, terme, sciale, porto, bifora, lavatoio, miniera, punta, viadotto, scogli, fornace, stazioni, impianti produttivi, muraglie, murgia
99	non classificato
00	mista

3.37 SIT_PUG67T_C_CATEG_ATDBECU_L_P

Codice	Descrizione
01	segnalazione archeologica
02	segnalazione architettonica

3.38 SIT_PUG32T_C_CLASSE_ATDPAGRI

Codice	Descrizione
01	segni di stratificazione storico-insediativa
02	segni di tecniche di conduzione agricola
03	contesti di riferimento formale e visuale dei centri storici
04	mista

3.39 SIT_PUG34T_C_CLASSE_ATDCIVICI

Codice	Descrizione
01	terre private gravate
02	terre di demanio civico
03	mista

3.40 SIT_PUG68T_C_RIF_CL_INT

Codice	Descrizione
01	relativa a beni riportati allo stesso strato ma classificati in modo diverso
02	relativa a beni riportati in strati diversi e duplicata nei relativi strati
03	relativa ad un solo bene o a più beni classificati nel medesimo modo

3.41 SIT_PUG38T_C_CLASSE_PUTT_ATE

Codice	Descrizione
A	ambito di valore eccezionale
B	ambito di valore rilevante
C	ambito di valore distinguibile
D	ambito di valore relativo

3.42 SIT_PUG40T_C_CLASSE_PUTT_TC

Codice	Descrizione
01	aree tipizzate dagli strumenti urbanistici vigenti come zone omogenee "A" e "B"
02	aree tipizzate dagli strumenti urbanistici vigenti come zone omogenee "C" oppure come zone "turistiche" "direzionali" "artigianali" "industriali" "miste" se, alla data del 6 giugno 1990, incluse in strumento urbanistico esecutivo (piano particolareggiato o piano di lottizzazione) regolarmente presentato e, inoltre, le aree incluse, anche se in percentuale, in Programmi Pluriennali di Attuazione approvati alla stessa data
03	aree che, ancorché non tipizzate come zone omogenee "B" dagli strumenti urbanistici vigenti ne abbiamo di fatto le caratteristiche (ai sensi del DIM n.1444/1968), vengano riconosciute come regolarmente edificate (o con edificato già "sanato" ai sensi della legge n.47/1985), e vengano perimetrate su cartografia catastale con specifica deliberazione di Consiglio Comunale
04	aree che, ancorché non tipizzate come zone omogenee "B" dagli strumenti urbanistici vigenti siano intercluse nell'interno del perimetro definito dalla presenza di maglie regolarmente edificate, e vengano perimetrate su cartografia catastale con specifica deliberazione di Consiglio Comunale

3.43 SIT_PUG80T_TIPO_VINCOLO

Codice	Descrizione
01	ai sensi della L. 364/1909
02	ai sensi della L. 778/1922
03	ai sensi della L. 1089/1939

04	ai sensi della L. 1497/1939
05	ai sensi della L. 1497/1939 - Galassino
06	ai sensi della L. 42/2004
07	ope legis
08	ai sensi della L. 490/1999
09	ai sensi del RD 3267/1923
10	ai sensi della L. 898/1976

4 Analisi delle tabelle di decodifica

4.1 SIT_PUG46T_C_CLASSE_INF

Descrizione

La tabella funge da decodifica per i possibili valori che il campo CLASSE può assumere in ogni singola istanza della tabella SIT_PUG45G_INF. Il tracciato record è del tipo *Codice-Descrizione*.

Relazioni principali

Sussiste la sola relazione di decodifica con la tabella SIT_PUG45G_INF sul campo CLASSE di quest'ultima.

Campi

Chiavi primarie			
CODICE	Codifica univoca relativa ad un singolo valore possibile per l'attributo.	Stringa max 10 caratteri (valori codificati)	Obbligatorio
Campi ulteriori			
DESCRIZIONE	Descrizione testuale relativa al codice presente nel campo precedente.	Stringa max 255 caratteri (testo libero)	Obbligatorio

4.2 SIT_PUG47T_C_TIPO_INF

Descrizione

La tabella funge da decodifica per i possibili valori che il campo TIPO può assumere in ogni singola istanza della tabella SIT_PUG45G_INF. Il tracciato record è del tipo *Codice-Descrizione*.

Relazioni principali

Sussiste la sola relazione di decodifica con la tabella SIT_PUG45G_INF sul campo TIPO di quest'ultima.

Campi

Chiavi primarie			
CODICE	Codifica univoca relativa ad un singolo valore possibile per l'attributo.	Stringa max 10 caratteri (valori codificati)	Obbligatorio
Campi ulteriori			
DESCRIZIONE	Descrizione testuale relativa al codice presente nel campo precedente.	Stringa max 255 caratteri (testo libero)	Obbligatorio

4.3 SIT_PUG48T_C_STA_FATTO_INF

Descrizione

La tabella funge da decodifica per i possibili valori che il campo STA_FATTO può assumere in ogni singola istanza della tabella SIT_PUG45G_INF. Il tracciato record è del tipo *Codice-Descrizione*.

Relazioni principali

Sussiste la sola relazione di decodifica con la tabella SIT_PUG45G_INF sul campo STA_FATTO di quest'ultima.

Campi

Chiavi primarie			
CODICE	Codifica univoca relativa ad un singolo valore possibile per l'attributo.	Stringa max 10 caratteri (valori codificati)	Obbligatorio
Campi ulteriori			
DESCRIZIONE	Descrizione testuale relativa al codice presente nel campo precedente.	Stringa max 255 caratteri (testo libero)	Obbligatorio

4.4 SIT_PUG50T_C_AMBITO**Descrizione**

La tabella funge da decodifica per i possibili valori che il campo AMBITO può assumere in ogni singola istanza della tabella SIT_PUG49G_CT. Il tracciato record è del tipo *Codice-Descrizione*.

Relazioni principali

Sussiste la relazione di decodifica con la tabella SIT_PUG49G_CT sul campo AMBITO di quest'ultima e con la tabella SIT_PUG63G_PREV_PROGRAMMATICHE sul campo AMBITO_C.

Campi

Chiavi primarie			
CODICE	Codifica univoca relativa ad un singolo valore possibile per l'attributo.	Stringa max 10 caratteri (valori codificati)	Obbligatorio
Campi ulteriori			
DESCRIZIONE	Descrizione testuale relativa al codice presente nel campo precedente.	Stringa max 255 caratteri (testo libero)	Obbligatorio

4.5 SIT_PUG51T_C_TIPO_CT**Descrizione**

La tabella funge da decodifica per i possibili valori che il campo TIPO può assumere in ogni singola istanza della tabella SIT_PUG49G_CT. Il tracciato record è del tipo *Codice-Descrizione*.

Relazioni principali

Sussiste la relazione di decodifica con la tabella SIT_PUG49G_CT sul campo TIPO di quest'ultima e con la tabella SIT_PUG63G_PREV_PROGRAMMATICHE sul campo TIPO_C.

Campi

Chiavi primarie			
CODICE	Codifica univoca relativa ad un singolo valore possibile per l'attributo.	Stringa max 10 caratteri (valori codificati)	Obbligatorio
Campi ulteriori			
DESCRIZIONE	Descrizione testuale relativa al	Stringa max 255 caratteri	Obbligatorio

	codice presente nel campo precedente.	(testo libero)	
--	---------------------------------------	----------------	--

4.6 SIT_PUG64T_C_MOD_ATT_PP

Descrizione

La tabella funge da decodifica per i possibili valori che il campo MOD_ATT può assumere in ogni singola istanza della tabella SIT_PUG63G_PREV_PROGRAMMATICHE. Il tracciato record è del tipo *Codice-Descrizione*.

Relazioni principali

Sussiste la sola relazione di decodifica con la tabella SIT_PUG63G_PREV_PROGRAMMATICHE sul campo MOD_ATT di quest'ultima.

Campi

Chiavi primarie			
CODICE	Codifica univoca relativa ad un singolo valore possibile per l'attributo.	Stringa max 10 caratteri (valori codificati)	Obbligatorio
Campi ulteriori			
DESCRIZIONE	Descrizione testuale relativa al codice presente nel campo precedente.	Stringa max 255 caratteri (testo libero)	Obbligatorio

4.7 SIT_PUG65T_C_AMB_APPL_PP

Descrizione

La tabella funge da decodifica per i possibili valori che il campo AMB_APPL può assumere in ogni singola istanza della tabella SIT_PUG63G_PREV_PROGRAMMATICHE. Il tracciato record è del tipo *Codice-Descrizione*.

Relazioni principali

Sussiste la sola relazione di decodifica con la tabella SIT_PUG63G_PREV_PROGRAMMATICHE sul campo AMB_APPL di quest'ultima.

Campi

Chiavi primarie			
CODICE	Codifica univoca relativa ad un singolo valore possibile per l'attributo.	Stringa max 10 caratteri (valori codificati)	Obbligatorio
Campi ulteriori			
DESCRIZIONE	Descrizione testuale relativa al codice presente nel campo precedente.	Stringa max 255 caratteri (testo libero)	Obbligatorio

4.8 SIT_PUG66T_C_ARCO_VAL_PP

Descrizione

La tabella funge da decodifica per i possibili valori che il campo AMB_APPL può assumere in ogni singola istanza della tabella SIT_PUG63G_PREV_PROGRAMMATICHE. Il tracciato record

è del tipo *Codice-Descrizione*.

Relazioni principali

Sussiste la sola relazione di decodifica con la tabella SIT_PUG63G_PREV_PROGRAMMATICHE sul campo AMB_APPL di quest'ultima.

Campi

Chiavi primarie			
CODICE	Codifica univoca relativa ad un singolo valore possibile per l'attributo.	Stringa max 10 caratteri (valori codificati)	Obbligatorio
Campi ulteriori			
DESCRIZIONE	Descrizione testuale relativa al codice presente nel campo precedente.	Stringa max 255 caratteri (testo libero)	Obbligatorio

4.9 SIT_PUG02T_C_CLASSE_PAI_PG

Descrizione

La tabella funge da decodifica per i possibili valori che il campo CLASSE può assumere in ogni singola istanza della tabella SIT_PUG01_PAI_PG. Il tracciato record è del tipo *Codice-Descrizione*.

Relazioni principali

Sussiste la sola relazione di decodifica con la tabella SIT_PUG01_PAI_PG sul campo CLASSE di quest'ultima.

Campi

Chiavi primarie			
CODICE	Codifica univoca relativa ad un singolo valore possibile per l'attributo.	Stringa max 10 caratteri (valori codificati)	Obbligatorio
Campi ulteriori			
DESCRIZIONE	Descrizione testuale relativa al codice presente nel campo precedente.	Stringa max 255 caratteri (testo libero)	Obbligatorio

4.10 SIT_PUG04T_C_CLASSE_PAI_PI

Descrizione

La tabella funge da decodifica per i possibili valori che il campo CLASSE può assumere in ogni singola istanza della tabella SIT_PUG03_PAI_PI. Il tracciato record è del tipo *Codice-Descrizione*.

Relazioni principali

Sussiste la sola relazione di decodifica con la tabella SIT_PUG03_PAI_PI sul campo CLASSE di quest'ultima.

Campi

Chiavi primarie			
CODICE	Codifica univoca relativa ad un singolo valore possibile per	Stringa max 10 caratteri (valori codificati)	Obbligatorio

	l'attributo.		
Campi ulteriori			
DESCRIZIONE	Descrizione testuale relativa al codice presente nel campo precedente.	Stringa max 255 caratteri (testo libero)	Obbligatorio

4.11 SIT_PUG06T_C_CLASSE_PAI_R

Descrizione

La tabella funge da decodifica per i possibili valori che il campo CLASSE può assumere in ogni singola istanza della tabella SIT_PUG05_PAI_R. Il tracciato record è del tipo *Codice-Descrizione*.

Relazioni principali

Sussiste la sola relazione di decodifica con la tabella SIT_PUG05_PAI_R sul campo CLASSE di quest'ultima.

Campi

Chiavi primarie			
CODICE	Codifica univoca relativa ad un singolo valore possibile per l'attributo.	Stringa max 10 caratteri (valori codificati)	Obbligatorio
Campi ulteriori			
DESCRIZIONE	Descrizione testuale relativa al codice presente nel campo precedente.	Stringa max 255 caratteri (testo libero)	Obbligatorio

4.12 SIT_PUG08T_C_CLASSE_ATDGEOL

Descrizione

La tabella funge da decodifica per i possibili valori che il campo CLASSE può assumere in ogni singola istanza della tabella SIT_PUG07_PUTT_ATDGEOL. Il tracciato record è del tipo *Codice-Descrizione*.

Relazioni principali

Sussiste la sola relazione di decodifica con la tabella SIT_PUG07_PUTT_ATDGEOL sul campo CLASSE di quest'ultima.

Campi

Chiavi primarie			
CODICE	Codifica univoca relativa ad un singolo valore possibile per l'attributo.	Stringa max 10 caratteri (valori codificati)	Obbligatorio
Campi ulteriori			
DESCRIZIONE	Descrizione testuale relativa al codice presente nel campo precedente.	Stringa max 255 caratteri (testo libero)	Obbligatorio

4.13 SIT_PUG09T_C_TIPO_PUTT

Descrizione

La tabella funge da decodifica per i possibili valori che il campo TIPO può assumere in ogni singola istanza delle seguenti tabelle:

- SIT_PUG07_PUTT_ATDGEOL
- SIT_PUG10_PUTT_ATDGROTT
- SIT_PUG22_PUTT_ATDBOMA
- SIT_PUG24_PUTT_ATDNATUR
- SIT_PUG28_PUTT_ATDBECU

Il dominio dei valori per l'attributo di queste tabelle è condiviso.

Il tracciato record è del tipo *Codice-Descrizione*.

Relazioni principali

Sussiste la sola relazione di decodifica con le tabelle:

- SIT_PUG07_PUTT_ATDGEOL
- SIT_PUG10_PUTT_ATDGROTT
- SIT_PUG22_PUTT_ATDBOMA
- SIT_PUG24_PUTT_ATDNATUR
- SIT_PUG28_PUTT_ATDBECU

sul campo TIPO di queste..

Campi

Chiavi primarie			
CODICE	Codifica univoca relativa ad un singolo valore possibile per l'attributo.	Stringa max 10 caratteri (valori codificati)	Obbligatorio
Campi ulteriori			
DESCRIZIONE	Descrizione testuale relativa al codice presente nel campo precedente.	Stringa max 255 caratteri (testo libero)	Obbligatorio

4.14 SIT_PUG11T_C_CLASSE_ATDGROTTE

Descrizione

La tabella funge da decodifica per i possibili valori che il campo CLASSE può assumere in ogni singola istanza delle tabelle SIT_PUG10_PUTT_ATDGROTT e SIT_PUG57_PUTT_ATDGROTT_P.

Il tracciato record è del tipo *Codice-Descrizione*.

Relazioni principali

Sussiste la sola relazione di decodifica con le tabelle SIT_PUG10G_PUTT_ATDGROTT e SIT_PUG5G_PUTT_ATDGROTT_P sul campo CLASSE di entrambe.

Campi

Chiavi primarie			
CODICE	Codifica univoca relativa ad un singolo valore possibile per l'attributo.	Stringa max 10 caratteri (valori codificati)	Obbligatorio
Campi ulteriori			
DESCRIZIONE	Descrizione testuale relativa al	Stringa max 255 caratteri	Obbligatorio

	codice presente nel campo precedente.	(testo libero)	
--	---------------------------------------	----------------	--

4.15 SIT_PUG12T_C_MOD_PUTT

Descrizione

La tabella funge da decodifica per i possibili valori che il campo MOD_PUTT può assumere in ogni singola istanza della tabella geometrica SIT_PUG37G_PUTT_ATE.
Il tracciato record è del tipo *Codice-Descrizione*.

Relazioni principali

Sussiste la sola relazione di decodifica con la tabella SIT_PUG37G_PUTT_ATE sul campo MOD_PUTT di questa.

Campi

Chiavi primarie			
CODICE	Codifica univoca relativa ad un singolo valore possibile per l'attributo.	Stringa max 10 caratteri (valori codificati)	Obbligatorio
Campi ulteriori			
DESCRIZIONE	Descrizione testuale relativa al codice presente nel campo precedente.	Stringa max 255 caratteri (testo libero)	Obbligatorio

4.16 SIT_PUG54T_C_MOD_PUTT_A

Descrizione

La tabella funge da decodifica per i possibili valori che il campo MOD_PUTT può assumere in ogni singola istanza delle seguenti tabelle geometriche poligonali:

- SIT_PUG10G_PUTT_ATDGROTT
- SIT_PUG15G_PUTT_ATDIDRO
- SIT_PUG22G_PUTT_ATDBOMA
- SIT_PUG24G_PUTT_ATDNATUR
- SIT_PUG28G_PUTT_ATDBECU
- SIT_PUG33G_PUTT_ATDCIVIC

Il tracciato record è del tipo *Codice-Descrizione*.

Relazioni principali

Sussiste la sola relazione di decodifica con le tabelle sopra citate sul campo MOD_PUTT di questa.

Campi

Chiavi primarie			
CODICE	Codifica univoca relativa ad un singolo valore possibile per l'attributo.	Stringa max 10 caratteri (valori codificati)	Obbligatorio
Campi ulteriori			
DESCRIZIONE	Descrizione testuale relativa al codice presente nel campo precedente.	Stringa max 255 caratteri (testo libero)	Obbligatorio

4.17 SIT_PUG54T_C_MOD_PUTT_L

Descrizione

La tabella funge da decodifica per i possibili valori che il campo MOD_PUTT può assumere in ogni singola istanza della tabella geometrica lineare SIT_PUG58G_ATDIDRO_L. Il tracciato record è del tipo *Codice-Descrizione*.

Relazioni principali

Sussiste la sola relazione di decodifica con la tabella SIT_PUG58G_ATDIDRO_L sul campo MOD_PUTT di questa.

Campi

Chiavi primarie			
CODICE	Codifica univoca relativa ad un singolo valore possibile per l'attributo.	Stringa max 10 caratteri (valori codificati)	Obbligatorio
Campi ulteriori			
DESCRIZIONE	Descrizione testuale relativa al codice presente nel campo precedente.	Stringa max 255 caratteri (testo libero)	Obbligatorio

4.18 SIT_PUG54T_C_MOD_PUTT_P

Descrizione

La tabella funge da decodifica per i possibili valori che il campo MOD_PUTT può assumere in ogni singola istanza delle seguenti tabelle geometriche poligonali:

- SIT_PUG57G_PUTT_ATDGROTT_P
- SIT_PUG60G_ATDBECU_P

Il tracciato record è del tipo *Codice-Descrizione*.

Relazioni principali

Sussiste la sola relazione di decodifica con le tabelle sopra citate sul campo MOD_PUTT di questa.

Campi

Chiavi primarie			
CODICE	Codifica univoca relativa ad un singolo valore possibile per l'attributo.	Stringa max 10 caratteri (valori codificati)	Obbligatorio
Campi ulteriori			
DESCRIZIONE	Descrizione testuale relativa al codice presente nel campo precedente.	Stringa max 255 caratteri (testo libero)	Obbligatorio

4.19 SIT_PUG14T_C_CLASSE_ATDCOSTE

Descrizione

La tabella funge da decodifica per i possibili valori che il campo CLASSE può assumere in ogni singola istanza della tabella SIT_PUG13G_PUTT_ATDCOSTE. Il tracciato record è del tipo *Codice-Descrizione*.

Relazioni principali

Sussiste la sola relazione di decodifica con la tabella SIT_PUG13G_PUTT_ATDCOSTE sul campo CLASSE di quest'ultima.

Campi

Chiavi primarie			
CODICE	Codifica univoca relativa ad un singolo valore possibile per l'attributo.	Stringa max 10 caratteri (valori codificati)	Obbligatorio
Campi ulteriori			
DESCRIZIONE	Descrizione testuale relativa al codice presente nel campo precedente.	Stringa max 255 caratteri (testo libero)	Obbligatorio

4.20 SIT_PUG18T_C_TIPO_ADTDCOSTE**Descrizione**

La tabella funge da decodifica per i possibili valori che il campo TIPO può assumere in ogni singola istanza della tabella SIT_PUG13G_PUTT_ATDCOSTE. Il tracciato record è del tipo *Codice-Descrizione*.

Relazioni principali

Sussiste la sola relazione di decodifica con la tabella SIT_PUG13G_PUTT_ATDCOSTE sul campo TIPO di quest'ultima.

Campi

Chiavi primarie			
CODICE	Codifica univoca relativa ad un singolo valore possibile per l'attributo.	Stringa max 10 caratteri (valori codificati)	Obbligatorio
Campi ulteriori			
DESCRIZIONE	Descrizione testuale relativa al codice presente nel campo precedente.	Stringa max 255 caratteri (testo libero)	Obbligatorio

4.21 SIT_PUG16T_C_CLASSE_ATDIDRO_CORSO**Descrizione**

La tabella funge da decodifica per i possibili valori che il campo CLASSE può assumere in ogni singola istanza della tabella SIT_PUG15G_PUTT_ATDIDRO. Il tracciato record è del tipo *Codice-Descrizione*.

Relazioni principali

Sussiste la sola relazione di decodifica con la tabella SIT_PUG15G_PUTT_ATDIDRO sul campo CLASSE di quest'ultima.

Campi

Chiavi primarie			
CODICE	Codifica univoca relativa ad un singolo valore possibile per l'attributo.	Stringa max 10 caratteri (valori codificati)	Obbligatorio

Campi ulteriori			
DESCRIZIONE	Descrizione testuale relativa al codice presente nel campo precedente.	Stringa max 255 caratteri (testo libero)	Obbligatorio

4.22 SIT_PUG59T_C_CLASSE_ATDIDRO_L

Descrizione

La tabella funge da decodifica per i possibili valori che il campo CLASSE può assumere in ogni singola istanza della tabella SIT_PUG15_PUTT_ATDIDRO. Il tracciato record è del tipo *Codice-Descrizione*.

Relazioni principali

Sussiste la sola relazione di decodifica con la tabella SIT_PUG58G_PUTT_ATDIDRO_L sul campo CLASSE di quest'ultima.

Campi

Chiavi primarie			
CODICE	Codifica univoca relativa ad un singolo valore possibile per l'attributo.	Stringa max 10 caratteri (valori codificati)	Obbligatorio
Campi ulteriori			
DESCRIZIONE	Descrizione testuale relativa al codice presente nel campo precedente.	Stringa max 255 caratteri (testo libero)	Obbligatorio

4.23 SIT_PUG17T_C_PROPR_ATDIDRO

Descrizione

La tabella funge da decodifica per i possibili valori che il campo PROPRIETA può assumere in ogni singola istanza della tabella SIT_PUG15G_PUTT_ATDIDRO. Il tracciato record è del tipo *Codice-Descrizione*.

Relazioni principali

Sussiste la sola relazione di decodifica con la tabella SIT_PUG15G_PUTT_ATDIDRO sul campo TIPO di quest'ultima.

Campi

Chiavi primarie			
CODICE	Codifica univoca relativa ad un singolo valore possibile per l'attributo.	Stringa max 10 caratteri (valori codificati)	Obbligatorio
Campi ulteriori			
DESCRIZIONE	Descrizione testuale relativa al codice presente nel campo precedente.	Stringa max 255 caratteri (testo libero)	Obbligatorio

4.24 SIT_PUG20T_C_CLASSE_ATDVECRI

Descrizione

La tabella funge da decodifica per i possibili valori che il campo CLASSE può assumere in ogni

singola istanza della tabella SIT_PUG19G_PUTT_ATDVECRI. Il tracciato record è del tipo *Codice-Descrizione*.

Relazioni principali

Sussiste la sola relazione di decodifica con la tabella SIT_PUG19G_PUTT_ATDVECRI sul campo CLASSE di quest'ultima.

Campi

Chiavi primarie			
CODICE	Codifica univoca relativa ad un singolo valore possibile per l'attributo.	Stringa max 10 caratteri (valori codificati)	Obbligatorio
Campi ulteriori			
DESCRIZIONE	Descrizione testuale relativa al codice presente nel campo precedente.	Stringa max 255 caratteri (testo libero)	Obbligatorio

4.25 SIT_PUG21T_C_TIPO_ATDVECRI

Descrizione

La tabella funge da decodifica per i possibili valori che il campo TIPO può assumere in ogni singola istanza della tabella SIT_PUG19G_PUTT_ATDVECRI. Il tracciato record è del tipo *Codice-Descrizione*.

Relazioni principali

Sussiste la sola relazione di decodifica con la tabella SIT_PUG19G_PUTT_ATDVECRI sul campo TIPO di quest'ultima.

Campi

Chiavi primarie			
CODICE	Codifica univoca relativa ad un singolo valore possibile per l'attributo.	Stringa max 10 caratteri (valori codificati)	Obbligatorio
Campi ulteriori			
DESCRIZIONE	Descrizione testuale relativa al codice presente nel campo precedente.	Stringa max 255 caratteri (testo libero)	Obbligatorio

4.26 SIT_PUG23T_C_CLASSE_ATDBOMA

Descrizione

La tabella funge da decodifica per i possibili valori che il campo CLASSE può assumere in ogni singola istanza della tabella SIT_PUG22G_PUTT_ATDBOMA. Il tracciato record è del tipo *Codice-Descrizione*.

Relazioni principali

Sussiste la sola relazione di decodifica con la tabella SIT_PUG22G_PUTT_ATDBOMA sul campo CLASSE di quest'ultima.

Campi

Chiavi primarie			
CODICE	Codifica univoca relativa ad un	Stringa max 10 caratteri	Obbligatorio

	singolo valore possibile per l'attributo.	(valori codificati)	
Campi ulteriori			
DESCRIZIONE	Descrizione testuale relativa al codice presente nel campo precedente.	Stringa max 255 caratteri (testo libero)	Obbligatorio

4.27 SIT_PUG25T_C_CLASSE_ATDNATURA

Descrizione

La tabella funge da decodifica per i possibili valori che il campo CLASSE può assumere in ogni singola istanza della tabella SIT_PUG24G_PUTT_ATDNATUR. Il tracciato record è del tipo *Codice-Descrizione*.

Relazioni principali

Sussiste la sola relazione di decodifica con la tabella SIT_PUG24G_PUTT_ATDNATUR sul campo CLASSE di quest'ultima.

Campi

Chiavi primarie			
CODICE	Codifica univoca relativa ad un singolo valore possibile per l'attributo.	Stringa max 10 caratteri (valori codificati)	Obbligatorio
Campi ulteriori			
DESCRIZIONE	Descrizione testuale relativa al codice presente nel campo precedente.	Stringa max 255 caratteri (testo libero)	Obbligatorio

4.28 SIT_PUG27T_C_CLASSE_ATDBEDI

Descrizione

La tabella funge da decodifica per i possibili valori che il campo CLASSE può assumere in ogni singola istanza della tabella SIT_PUG26G_PUTT_ATDBEDI. Il tracciato record è del tipo *Codice-Descrizione*.

Relazioni principali

Sussiste la sola relazione di decodifica con la tabella SIT_PUG26G_PUTT_ATDBEDI sul campo CLASSE di quest'ultima.

Campi

Chiavi primarie			
CODICE	Codifica univoca relativa ad un singolo valore possibile per l'attributo.	Stringa max 10 caratteri (valori codificati)	Obbligatorio
Campi ulteriori			
DESCRIZIONE	Descrizione testuale relativa al codice presente nel campo precedente.	Stringa max 255 caratteri (testo libero)	Obbligatorio

4.29 SIT_PUG67T_C_CATEG_ATDBECU_L_P

Descrizione

La tabella funge da decodifica per i possibili valori che il campo CATEGORIA può assumere in ogni singola istanza della tabella SIT_PUG60G_PUTT_ATDBECU_P e della tabella SIT_PUG77G_PUTT_ATDBECU_L. Il tracciato record è del tipo *Codice-Descrizione*.

Relazioni principali

Sussiste la sola relazione di decodifica con le tabelle geometriche sopra citate sul campo CATEGORIA di quest'ultima.

Campi

Chiavi primarie			
CODICE	Codifica univoca relativa ad un singolo valore possibile per l'attributo.	Stringa max 10 caratteri (valori codificati)	Obbligatorio
Campi ulteriori			
DESCRIZIONE	Descrizione testuale relativa al codice presente nel campo precedente.	Stringa max 255 caratteri (testo libero)	Obbligatorio

4.30 SIT_PUG29T_C_CATEG_ATDBECU

Descrizione

La tabella funge da decodifica per i possibili valori che il campo CATEGORIA può assumere in ogni singola istanza della tabella SIT_PUG28G_PUTT_ATDBECU. Il tracciato record è del tipo *Codice-Descrizione*.

Relazioni principali

Sussiste la sola relazione di decodifica con le tabelle SIT_PUG28_PUTT_ATDBECU sul campo CATEGORIA di quest'ultima.

Campi

Chiavi primarie			
CODICE	Codifica univoca relativa ad un singolo valore possibile per l'attributo.	Stringa max 10 caratteri (valori codificati)	Obbligatorio
Campi ulteriori			
DESCRIZIONE	Descrizione testuale relativa al codice presente nel campo precedente.	Stringa max 255 caratteri (testo libero)	Obbligatorio

4.31 SIT_PUG53T_C_PERIM_ATDBECU

Descrizione

La tabella funge da decodifica per i possibili valori che il campo PERIM può assumere in ogni singola istanza della tabella SIT_PUG28G_PUTT_ATDBECU. Il tracciato record è del tipo *Codice-Descrizione*.

Relazioni principali

Sussiste la sola relazione di decodifica con la tabella SIT_PUG28G_PUTT_ATDBECU sul campo PERIM di quest'ultima.

Campi

Chiavi primarie			
CODICE	Codifica univoca relativa ad un singolo valore possibile per l'attributo.	Stringa max 10 caratteri (valori codificati)	Obbligatorio
Campi ulteriori			
DESCRIZIONE	Descrizione testuale relativa al codice presente nel campo precedente.	Stringa max 255 caratteri (testo libero)	Obbligatorio

4.32 SIT_PUG30T_C_CLASSE_ATDBECU**Descrizione**

La tabella funge da decodifica per i possibili valori che il campo CLASSE può assumere in ogni singola istanza delle tabelle SIT_PUG28G_PUTT_ATDBECU e SIT_PUG60G_PUTT_ATDBECU_P. Il tracciato record è del tipo *Codice-Descrizione*.

Relazioni principali

Sussiste la sola relazione di decodifica con le tabelle SIT_PUG28_PUTT_ATDBECU e SIT_PUG60G_PUTT_ATDBECU_P sul campo CLASSE di entrambe.

Campi

Chiavi primarie			
CODICE	Codifica univoca relativa ad un singolo valore possibile per l'attributo.	Stringa max 10 caratteri (valori codificati)	Obbligatorio
Campi ulteriori			
DESCRIZIONE	Descrizione testuale relativa al codice presente nel campo precedente.	Stringa max 255 caratteri (testo libero)	Obbligatorio

4.33 SIT_PUG32T_C_CLASSE_ATDPAGRI**Descrizione**

La tabella funge da decodifica per i possibili valori che il campo CLASSE può assumere in ogni singola istanza della tabella SIT_PUG31G_PUTT_ATDPAGRI. Il tracciato record è del tipo *Codice-Descrizione*.

Relazioni principali

Sussiste la sola relazione di decodifica con la tabella SIT_PUG31G_PUTT_ATDPAGRI sul campo CLASSE di quest'ultima.

Campi

Chiavi primarie			
CODICE	Codifica univoca relativa ad un singolo valore possibile per l'attributo.	Stringa max 10 caratteri (valori codificati)	Obbligatorio

Campi ulteriori			
DESCRIZIONE	Descrizione testuale relativa al codice presente nel campo precedente.	Stringa max 255 caratteri (testo libero)	Obbligatorio

4.34 SIT_PUG34T_C_CLASSE_ATDCIVICI

Descrizione

La tabella funge da decodifica per i possibili valori che il campo CLASSE può assumere in ogni singola istanza della tabella SIT_PUG33G_PUTT_ATDCIVIC. Il tracciato record è del tipo *Codice-Descrizione*.

Relazioni principali

Sussiste la sola relazione di decodifica con la tabella SIT_PUG33G_PUTT_ATDCIVIC sul campo CLASSE di quest'ultima.

Campi

Chiavi primarie			
CODICE	Codifica univoca relativa ad un singolo valore possibile per l'attributo.	Stringa max 10 caratteri (valori codificati)	Obbligatorio
Campi ulteriori			
DESCRIZIONE	Descrizione testuale relativa al codice presente nel campo precedente.	Stringa max 255 caratteri (testo libero)	Obbligatorio

4.35 SIT_PUG38T_C_CLASSE_PUTT_ATE

Descrizione

La tabella funge da decodifica per i possibili valori che il campo CLASSE può assumere in ogni singola istanza della tabella SIT_PUG37G_PUTT_ATE. Il tracciato record è del tipo *Codice-Descrizione*.

Relazioni principali

Sussiste la sola relazione di decodifica con la tabella SIT_PUG37G_PUTT_ATE sul campo CLASSE di quest'ultima.

Campi

Chiavi primarie			
CODICE	Codifica univoca relativa ad un singolo valore possibile per l'attributo.	Stringa max 10 caratteri (valori codificati)	Obbligatorio
Campi ulteriori			
DESCRIZIONE	Descrizione testuale relativa al codice presente nel campo precedente.	Stringa max 255 caratteri (testo libero)	Obbligatorio

4.36 SIT_PUG40T_C_CLASSE_PUTT_TC

Descrizione

La tabella funge da decodifica per i possibili valori che il campo CLASSE può assumere in ogni

singola istanza della tabella SIT_PUG39G_PUTT_TC. Il tracciato record è del tipo *Codice-Descrizione*.

Relazioni principali

Sussiste la sola relazione di decodifica con la tabella SIT_PUG39G_PUTT_TC sul campo CLASSE di quest'ultima.

Campi

Chiavi primarie			
CODICE	Codifica univoca relativa ad un singolo valore possibile per l'attributo.	Stringa max 10 caratteri (valori codificati)	Obbligatorio
Campi ulteriori			
DESCRIZIONE	Descrizione testuale relativa al codice presente nel campo precedente.	Stringa max 255 caratteri (testo libero)	Obbligatorio

4.37 SIT_PUG68T_C_RIF_CL_INT

Descrizione

La tabella funge da decodifica per i possibili valori che il campo RIF_CL_INT può assumere in ogni singola istanza delle seguenti tabelle:

- SIT_PUG07G_PUTT_ATD_GEOL
- SIT_PUG10G_PUTT_ATDGROTTE
- SIT_PUG13G_PUTT_ATDCOSTE
- SIT_PUG15G_PUTT_ATDIDRO_CORSO
- SIT_PUG74G_PUTT_ATDIDRO_BACINO
- SIT_PUG19G_PUTT_ATDVECRI
- SIT_PUG22G_PUTT_ATDBOMA
- SIT_PUG24G_PUTT_ATDNATUR
- SIT_PUG26G_PUTT_ATDBEDI
- SIT_PUG28G_PUTT_ATDBECU
- SIT_PUG31G_PUTT_ATDAGRI
- SIT_PUG33G_PUTT_ATDCIVIC

Il tracciato record è del tipo *Codice-Descrizione*.

Relazioni principali

Sussiste la sola relazione di decodifica con le tabelle sopra citate sul campo RIF_CL_INT di queste ultime.

Campi

Chiavi primarie			
CODICE	Codifica univoca relativa ad un singolo valore possibile per l'attributo.	Stringa max 10 caratteri (valori codificati)	Obbligatorio
Campi ulteriori			
DESCRIZIONE	Descrizione testuale relativa al codice presente nel campo precedente.	Stringa max 255 caratteri (testo libero)	Obbligatorio

4.38 SIT_PUG73T_C_DESC_CI_ATDCOSTE

Descrizione

La tabella funge da decodifica per i possibili valori che il campo DESC_CI può assumere in ogni singola istanza delle seguenti tabelle:

- SIT_PUG13G_PUTT_ATDCOSTE
- SIT_PUG15G_PUTT_ATDIDRO_CORSO
- SIT_PUG74G_PUTT_ATDIDRO_BACINO
- SIT_PUG58G_PUTT_ATDIDRO_L

Il tracciato record è del tipo *Codice-Descrizione*.

Relazioni principali

Sussiste la sola relazione di decodifica con le tabelle sopra elencate sul campo DESC_CI di queste.

Campi

Chiavi primarie			
CODICE	Codifica univoca relativa ad un singolo valore possibile per l'attributo.	Stringa max 12 caratteri (valori codificati)	Obbligatorio
Campi ulteriori			
DESCRIZIONE	Descrizione testuale relativa al codice presente nel campo precedente.	Stringa max 255 caratteri (testo libero)	Obbligatorio

4.39 SIT_PUG75T_C_DESC_CI_ATDIDROC

Descrizione

La tabella funge da decodifica per i possibili valori che il campo DESC_CI può assumere in ogni singola istanza della tabella SIT_PUG15G_PUTT_ATDIDRO_CORSO. Il tracciato record è del tipo *Codice-Descrizione*.

Relazioni principali

Sussiste la sola relazione di decodifica con la tabella SIT_PUG15G_PUTT_ATDIDRO_CORSO sul campo DESC_CI di quest'ultima.

Campi

Chiavi primarie			
CODICE	Codifica univoca relativa ad un singolo valore possibile per l'attributo.	Stringa max 12 caratteri (valori codificati)	Obbligatorio
Campi ulteriori			
DESCRIZIONE	Descrizione testuale relativa al codice presente nel campo precedente.	Stringa max 255 caratteri (testo libero)	Obbligatorio

4.40 SIT_PUG76T_C_DESC_CI_ATDIDROB

Descrizione

La tabella funge da decodifica per i possibili valori che il campo DESC_CI può assumere in ogni

singola istanza della tabella SIT_PUG74G_PUTT_ATDIDRO_BACINO.
Il tracciato record è del tipo *Codice-Descrizione*.

Relazioni principali

Sussiste la sola relazione di decodifica con la tabella SIT_PUG74G_PUTT_ATDIDRO_BACINO sul campo DESC_CI di quest'ultima.

Campi

Chiavi primarie			
CODICE	Codifica univoca relativa ad un singolo valore possibile per l'attributo.	Stringa max 12 caratteri (valori codificati)	Obbligatorio
Campi ulteriori			
DESCRIZIONE	Descrizione testuale relativa al codice presente nel campo precedente.	Stringa max 255 caratteri (testo libero)	Obbligatorio

4.41 SIT_PUG78T_C_DESC_CI_ATDIDRO_L

Descrizione

La tabella funge da decodifica per i possibili valori che il campo DESC_CI può assumere in ogni singola istanza della tabella SIT_PUG58G_PUTT_ATDIDRO_L.
Il tracciato record è del tipo *Codice-Descrizione*.

Relazioni principali

Sussiste la sola relazione di decodifica con la tabella SIT_PUG58G_PUTT_ATDIDRO_L sul campo DESC_CI di quest'ultima.

Campi

Chiavi primarie			
CODICE	Codifica univoca relativa ad un singolo valore possibile per l'attributo.	Stringa max 12 caratteri (valori codificati)	Obbligatorio
Campi ulteriori			
DESCRIZIONE	Descrizione testuale relativa al codice presente nel campo precedente.	Stringa max 255 caratteri (testo libero)	Obbligatorio

4.42 SIT_PUG80T_TIPO_VINCOLO

Descrizione

La tabella funge da decodifica per i possibili valori che il campo TIPO può assumere in ogni singola istanza della tabella SIT_PUG79G_VINCOLI.

Il tracciato record è del tipo *Codice-Descrizione*.

Relazioni principali

Sussiste la sola relazione di decodifica con la tabella SIT_PUG79G_VINCOLI sul campo TIPO di quest'ultima.

Campi

Chiavi primarie			
CODICE	Codifica univoca relativa ad un singolo valore possibile per l'attributo.	Stringa max 12 caratteri (valori codificati)	Obbligatorio
Campi ulteriori			
DESCRIZIONE	Descrizione testuale relativa al codice presente nel campo precedente.	Stringa max 255 caratteri (testo libero)	Obbligatorio

5 Ulteriori osservazioni e vincoli

5.1 Osservazioni sui vincoli topologici

Si ritiene opportuno, riportare alcuni vincoli importanti per garantire la consistenza topologica delle geometrie prodotte in fase di redazione degli strati informativi.

I vincoli descritti vanno intesi applicati alle tabelle fisiche disponibili per ciascun Comune.

1. Le geometrie della tabella SIT_PUG49_CT non possono presentare sovrapposizioni; inoltre, individuano una copertura dell'intero territorio comunale (non sono ammessi buchi tra le geometrie).
2. Le geometrie delle seguenti tabelle devono soddisfare il vincoli di non sovrapposibilità (è ammessa al più la situazione di condivisione di tratti di frontiera):
 - SIT_PUG01_PAI_PG
 - SIT_PUG03_PAI_PI
 - SIT_PUG05_PAI_R
 - SIT_PUG13_PUTT_ATDCOSTE
 - SIT_PUG19_PUTT_ATDVECRI
 - SIT_PUG31_PUTT_ATDPAGRI
 - SIT_PUG33_PUTT_ATDCIVIC
 - SIT_PUG37_PUTT_ATE
 - SIT_PUG39_PUTT_TC

5.2 Osservazioni sul valore Booleano

Nel modello del PUG, il tipo definito come Booleano si basa su una logica a tre valori per cui, oltre ai valori di vero e falso che vengono simulati con gli interi 1 e 0 rispettivamente, è necessario introdurre il valore negativo -1 corrispondente alla definizione "da definire".

Per tutti i campi obbligatori dichiarati di tipo Booleano nelle tabelle introdotte, il valore -1 "da definire" va assunto come valore di default.

5.3 Campi richiesti nell' introduzione di nuovi strati

Qualora si ritenga opportuno introdurre nuovi strati informativi geometrici, si richiede come requisito base imprescindibile la presenza dei seguenti tre campi:

- FILE_ID di tipo intero lungo, obbligatorio (not null): rappresenta un identificativo numerico univoco per ciascun elemento geometrico introdotto nello strato;
- COD_ISTAT di tipo testo, lunghezza max 6 caratteri, obbligatorio (not null): rappresenta il codice ISTAT del Comune al quale lo strato si riferisce, deve essere esattamente di 6 caratteri dati da cifre (esempio: per Valenzano il codice ISTAT è 072048, non 72048, valore confondibile con un numerico);
- DESCRIZION di tipo testo, lunghezza max 255 caratteri, non obbligatorio: consente di associare in maniera facoltativa una descrizione ad ogni singola geometria; i criteri logici alla base dei contenuti espressi dovrebbero essere gli stessi per le varie geometrie dello strato, eventualmente codificando le diciture in forme quanto più standardizzate possibile.

Il tracciato record può essere arricchito da vari altri campi secondo le necessità, con la viva raccomandazione di utilizzare laddove possibile domini codificati con valori prefissati, in armonia con la logica seguita nella costruzione del modello; tale scelta progettuale rende più agevoli ed efficienti le interrogazioni sulla base dati associata allo strato. In ogni caso, per una maggiore fruibilità delle informazioni, è utile che anche i testi liberi siano compilati secondo delle precise regole sintattiche di riferimento.

ALLEGATO 5

Identificazione in rete del cittadino



LINEE GUIDA PER L'EMISSIONE E L'UTILIZZO DELLA CARTA NAZIONALE DEI SERVIZI

Versione 3.0
15 maggio 2006

Ufficio Standard e tecnologie d'identificazione
Centro Nazionale per l'informatica nella Pubblica Amministrazione

Sommario

CAPITOLO 1 INTRODUZIONE	813
1.1 OBIETTIVI E CONTENUTO DEL DOCUMENTO	813
1.2 LA VISIONE CONDIVISA.....	813
1.3 LA VISIONE TECNOLOGICA DELLA CNS	814
CAPITOLO 2 IL QUADRO NORMATIVO DI RIFERIMENTO.....	816
2.1 IL REGOLAMENTO DI ATTUAZIONE	817
2.2 LE REGOLE TECNICHE	1 819
2.2.1 <i>Caratteristiche della carta e standard di riferimento</i>	<i>1 819</i>
2.2.2 <i>La certificazione della smart card.....</i>	<i>1 820</i>
2.2.3 <i>Le informazioni registrate nella memoria della carta.....</i>	<i>1 820</i>
2.2.4 <i>L'emissione della CNS</i>	<i>1 821</i>
2.2.5 <i>Il circuito della CNS</i>	<i>1 833</i>
2.2.6 <i>La gestione della CNS</i>	<i>1 833</i>
2.2.7 <i>Requisiti per la partecipazione al circuito della CNS</i>	<i>1 823</i>
2.2.8 <i>La sicurezza</i>	<i>1 824</i>
CAPITOLO 3 INTEROPERABILITÀ TRA LE CARTE	1 825
3.1 STANDARD DI RIFERIMENTO	1 825
3.1.1 <i>Carte e norme ISO, lo stato dell'arte.....</i>	<i>1 827</i>
3.1.2 <i>Interoperabilità a livello applicativo.....</i>	<i>1 827</i>
3.1.3 <i>Interoperabilità a livello di sistema operativo della carta.....</i>	<i>2 831</i>
3.2 CARTE "DUAL INTERFACE"	2 831
3.3 LA PIATTAFORMA JAVACARD	2 832
3.4 IL PROTOCOLLO D'INTESA 13 MAGGIO 2003	2 833
CAPITOLO 4 L'IDENTIFICAZIONE E L'AUTENTICAZIONE IN RETE.....	2 835
4.1 I PROCESSI DI IDENTIFICAZIONE E AUTENTICAZIONE	2 835
4.1.1 <i>Mutua autenticazione tramite il protocollo SSL/TLS</i>	<i>2 835</i>
4.2 L'AUTENTICAZIONE DEL SERVER	2 836
4.2.1 <i>Configurazione del client Internet Explorer.....</i>	<i>2 837</i>
4.2.2 <i>Configurazione di browser open source (Netscape, Mozilla, ecc.).....</i>	<i>2 837</i>
4.2.3 <i>Configurazione del server</i>	<i>2 837</i>
4.2.4 <i>Installazione del certificato del server</i>	<i>3 838</i>
4.3 PERSONALIZZAZIONE DELLE FUNZIONI DI SICUREZZA	3 838
4.4 AUTENTICAZIONE IN MODALITÀ CHALLENGE/RESPONSE(CH/R).....	3 839
CAPITOLO 5 I CERTIFICATI DIGITALI.....	3 840
5.1 CERTIFICATI E FORMATI PER LA FIRMA DIGITALE	3 840
5.2 CERTIFICATI DI AUTENTICAZIONE E CRITTOGRAFIA	3 842
5.3 PROCESSO DI ATTESTAZIONE	3 842
CAPITOLO 6 LE APPLICAZIONI SANITARIE DELLA CARTA.....	3 843
6.1 IL MODELLO DI SANITÀ BASATO SULLA CARTA SANITARIA.....	3 844
6.2 LE SPECIFICHE NETLINK	3 844
CAPITOLO 7 LA FIRMA DIGITALE.....	3 845
7.1 LA FIRMA DIGITALE NELLA CNS	3 845

CAPITOLO 8 ALTRE APPLICAZIONI NELLA CNS	847
8.1 I SERVIZI AGGIUNTIVI	847
8.2 I SISTEMI DI PAGAMENTO IN LINEA.....	848
8.3 LA CNS E LA TELEVISIONE DIGITALE TERRESTRE.....	849
8.4 MODALITÀ DI COLLOQUIO CON LA SMARTCARD.....	849
8.5 POSSIBILI UTILIZZI DELLA CNS IN AMBIENTE MHP	850
8.5.1 <i>Identificazione ed autenticazione in rete</i>	850
8.6 DATI PERSONALI E SERVIZI AGGIUNTIVI.....	850
8.7 UNA NOTA SULLA SICUREZZA DELLE APPLICAZIONI MHP.....	851
8.8 LO STATO DELL'ARTE.....	851
CAPITOLO 9 L'AMBIENTE SOFTWARE SUL CLIENT	852
9.1 MODALITÀ DI UTILIZZO DELLA CNS IN AMBIENTE OPEN SOURCE (NETSCAPE, MOZILLA, ECC.)...	852
9.2 MODALITÀ DI UTILIZZO DELLA CNS IN AMBIENTE MICROSOFT	852
9.3 MODALITÀ DI UTILIZZO DELLA CNS IN MODO SEMPLIFICATO	853
9.4 MODALITÀ DI UTILIZZO DELLA CNS IN AMBIENTE LINUX O MACOS X.....	853
CAPITOLO 10 L'AMBIENTE DI ACCESSO SUL SERVER	854
10.1 L'AMBIENTE DI ACCESSO IN MODALITÀ WEB	854
10.1.1 <i>Il processo di autorizzazione</i>	855
10.1.2 <i>Tecnologie per un'identità federata</i>	856
CAPITOLO 11 LA SICUREZZA DEL CIRCUITO DELLA CNS	857
11.1 LA SICUREZZA DELLA FASE DI PRODUZIONE	857
11.1.1 <i>Fasi di lavorazione della carta</i>	857
11.1.2 <i>Conservazione e trasporto delle carte</i>	858
11.1.3 <i>Gestione degli scarti</i>	858
11.1.4 <i>Generazione delle chiavi</i>	858
11.1.5 <i>Tracciatura delle operazioni</i>	858
11.1.6 <i>Protezione delle informazioni di tracciatura</i>	858
11.1.7 <i>Misure organizzative</i>	859
11.1.8 <i>Misure di sicurezza fisiche</i>	859
11.2 LA SICUREZZA DELLA FASE DI EMISSIONE.....	860
11.2.1 <i>Protezione delle carte inizializzate</i>	860
11.2.2 <i>Protezione dei flussi di dati</i>	860
CAPITOLO 12 CONCLUSIONI	861
12.1 LO STATO DELL'ARTE	861
APPENDICE 1.....	862
PROFILO DI CERTIFICATO DIGITALE PER L'AUTENTICAZIONE MEDIANTE CARTA NAZIONALE DEI SERVIZI (CNS)	862
APPENDICE 2	867
PROTOCOLLO D'INTESA DEL 13 MAGGIO 2003.....	867
APPENDICE 3	873
DATI PRESENTI SULLA CNS.....	873

Capitolo 1

Introduzione

La progressiva disponibilità di servizi on-line erogati dalla pubblica amministrazione rende necessarie modalità di accesso sicure, facili da utilizzare per i servizi di tutte le amministrazioni.

L'accesso a tali servizi deve essere garantito indipendentemente dallo strumento di identificazione digitale utilizzato dall'utente. Parallelamente è indispensabile evitare la proliferazione di strumenti di identificazione digitale per l'accesso ai servizi delle amministrazioni, garantendo, invece, la convergenza verso uno standard unitario, le cui caratteristiche di realizzazione, distribuzione e gestione siano largamente condivise, rapidamente realizzabili su tutto il territorio nazionale in modo economicamente sostenibile.

Il nome di questo standard è "Carta Nazionale di accesso ai Servizi" o "Carta Nazionale dei Servizi".

Il presente documento contiene le Linee guida per l'emissione, la gestione e l'utilizzo della Carta Nazionale dei Servizi (nel seguito CNS).

1.1 Obiettivi e contenuto del documento

Obiettivo di questo documento è quello di fornire indicazioni ai comuni, alle province, alle comunità montane, alle regioni e alle amministrazioni centrali sull'emissione e utilizzo della CNS. Nei vari capitoli vengono presentati l'ambito politico nel quale ci si muove ovvero quello della visione condivisa; il contesto normativo al quale la CNS deve conformarsi; le tecnologie ICT di riferimento necessarie per un corretto e omogeneo funzionamento nell'ambito del controllo d'accesso ai servizi in rete erogati dalla pubblica amministrazione. Vengono anche descritti sinteticamente gli obiettivi sanitari che la CNS si pone in conformità con quelli della CIE; le possibilità di integrazione con i sistemi di pagamento in linea.

Infine vengono date le specifiche generali per consentire alla CNS di essere utilizzata dalle applicazioni sulle postazioni client e alle applicazioni server di gestire l'ambiente di autenticazione e autorizzazione in conformità alle regole di cooperazione applicativa.

Si è ritenuto opportuno ricordare anche le regole di sicurezza del circuito di produzione e emissione della CNS, secondo quanto stabilito nelle regole tecniche di riferimento.

1.2 La visione condivisa

Il documento "L'E-GOVERNMENT PER UN FEDERALISMO EFFICIENTE - UNA VISIONE CONDIVISA, UNA REALIZZAZIONE COOPERATIVA"⁽¹⁾, come recita il suo sottotitolo, contiene le "Note di riferimento per lo sviluppo dell'e-government nelle Amministrazioni Centrali, nelle Regioni e negli Enti Locali." Questo documento ha l'obiettivo di formulare una visione comune

¹ Disponibile sul sito del Ministro per l'innovazione e le tecnologie (www.innovazione.gov.it), nella sezione "Enti locali".

nell'ambito delle pubbliche amministrazioni coinvolte nel percorso di innovazione del paese che ha come impegnativo processo la riorganizzazione della Stato in senso federale.

Come già evidenziato in precedenza l'efficacia, l'efficienza e l'economicità dei processi di e-government richiedono scelte omogenee nella visione tecnologica per evitare inutili sprechi di risorse economiche.

A tal proposito è stata sviluppata una visione comune tra i diversi livelli di governo e di responsabilità amministrativa sui seguenti temi:

1. l'interconnessione tra tutte le Pubbliche amministrazioni e tra le Pubbliche amministrazioni i cittadini e le imprese;
2. gli strumenti di accesso ai servizi erogati sul canale telematico;
3. le modalità di erogazione dei servizi sul canale telematico;
4. i requisiti per garantire la sicurezza;
5. le architetture che garantiscono l'interoperabilità dei servizi sul territorio nazionale;
6. sistemi federati e riuso delle soluzioni;
7. le strutture organizzative per l'attuazione dell'e-government;
8. verso architetture condivise di sistema.

La CNS, ovviamente, è contemplata nell'ambito degli strumenti di accesso ai servizi on-line. Le carte per l'accesso ai servizi in rete sono diverse tipologie di smart card che hanno in comune le seguenti caratteristiche:

- sono emesse da un ente pubblico che convalida le informazioni di rilevanza sociale in esse contenute;
- hanno requisiti di sicurezza che permettono di utilizzare in rete queste informazioni con la massima garanzia di sicurezza e tutela dei diritti personali.

Con questi strumenti si supera il modello di interazione tradizionale che costringe gli utenti a fornire una serie di dati in rete e soprattutto a gestire un numero elevato (circa 40) di pin o password per accedere ai servizi erogati on-line dalle diverse pubbliche amministrazioni.

Le carte per l'accesso ai servizi sono riconducibili a due tipologie:

- la Carta d'Identità Elettronica (CIE), emessa dai comuni in sostituzione della carta d'identità tradizionale;
- le altre carte per accedere ai servizi in rete (carta sanitaria, tributaria, carte regionali e cittadine dei servizi, etc.), che devono essere conformi a un unico standard denominato "Carta Nazionale dei Servizi".

La CNS rappresenta uno standard per le carte di accesso ai servizi in rete rilasciate dalla Pubblica amministrazione.

La descrizione della CIE non è tra gli obiettivi del presente documento.

1.3 La visione tecnologica della CNS

La CNS è una carta a microprocessore che, per quanto concerne la parte elettronica, presenta le stesse caratteristiche funzionali della CIE, ma mentre quest'ultima contiene gli elementi di sicurezza necessari per il riconoscimento a vista del titolare (in particolare gli ologrammi prodotti dall'Istituto Poligrafico dello Stato e la banda ottica inserita sul retro della carta), la CNS non contiene gli elementi "esterni" tipici di una carta d'identità.

Questa semplificazione permette di adottare un circuito di emissione più snello e flessibile di quello della CIE, infatti gli enti emittitori potranno rivolgersi a strutture esterne accreditate per quanto attiene le attività di produzione/inizializzazione delle smart card e di emissione dei certificati digitali. Infine, l'apertura al libero mercato delle smart card avrà come immediata conseguenza le economie indotte dalla concorrenza e dalla molteplicità delle offerte.

La CNS è, quindi, principalmente uno strumento di identificazione in rete. Sfruttando le capacità di memorizzazione della carta stessa è possibile ospitare informazioni necessarie per altre funzionalità.

Il modello tecnologico della CNS consente anche l'inserimento delle informazioni crittografiche necessarie per la firma digitale. In tal modo il titolare della CNS ha la possibilità di sottoscrivere documenti elettronici.

Naturalmente, per assicurare la fruizione dei servizi garantendone la sicurezza e l'interoperabilità è necessario non solo che l'utente disponga di strumenti per l'identificazione in rete, ma anche che i servizi siano progettati e realizzati secondo precise regole che permettono di garantire il rispetto dei principi di sicurezza enunciati

In ogni caso, il quadro normativo di riferimento è la base di partenza alla quale attenersi. Questo è l'argomento del prossimo capitolo.

Capitolo 2

Il quadro normativo di riferimento

I documenti di riconoscimento in formato elettronico compaiono nel nostro ordinamento giuridico con la legge 15 maggio 1997 n. 127 che all'articolo 2, comma 10, successivamente sostituito dall'articolo 2 comma 4 della legge 16 giugno 1998 n. 191, stabilisce: *“con decreto del Presidente del Consiglio dei ministri, su proposta del Ministro dell'interno, di concerto con il Ministro per la funzione pubblica, sono individuate le caratteristiche e le modalità per il rilascio della carta di identità e di altri documenti di riconoscimento muniti di supporto magnetico o informatico. La carta di identità e i documenti di riconoscimento devono contenere i dati personali e il codice fiscale e possono contenere anche l'indicazione del gruppo sanguigno, nonché delle opzioni di carattere sanitario previste dalla legge. Il documento, ovvero il supporto magnetico o informatico, può contenere anche altri dati, al fine di razionalizzare e semplificare l'azione amministrativa e la erogazione dei servizi al cittadino, nel rispetto della legge 31 dicembre 1996, n. 675, e successive modificazioni, nonché le procedure informatiche e le informazioni, che possono o debbono essere conosciute dalla pubblica amministrazione o da altri soggetti, ivi compresa la chiave biometrica, occorrenti per la firma digitale ai sensi dell'articolo 15, comma 2, della legge 15 marzo 1997, n. 59, e dei relativi regolamenti di attuazione; analogo documento contenente i medesimi dati e' rilasciato a seguito della dichiarazione di nascita. La carta di identità potrà essere utilizzata anche per il trasferimento elettronico dei pagamenti tra soggetti privati e pubbliche amministrazioni. Con decreto del Ministro dell'interno, sentite l'Autorità per l'informatica nella pubblica amministrazione e la Conferenza Stato-città ed autonomie locali, sono dettate le regole tecniche e di sicurezza relative alle tecnologie e ai materiali utilizzati per la produzione delle carte di identità e dei documenti di riconoscimento di cui al presente comma. Le predette regole sono adeguate con cadenza almeno biennale in relazione alle esigenze dettate dall'evoluzione delle conoscenze scientifiche e tecnologiche. La carta di identità può essere rinnovata a decorrere dal centottantesimo giorno precedente la scadenza, ovvero, previo pagamento delle spese e dei diritti di segreteria, a decorrere dal terzo mese successivo alla produzione di documenti con caratteristiche tecnologiche e funzionali innovative. Nel rispetto della disciplina generale fissata dai decreti di cui al presente comma e nell'ambito dei rispettivi ordinamenti, le pubbliche amministrazioni possono sperimentare modalità di utilizzazione dei documenti di cui al presente comma per l'erogazione di ulteriori servizi o utilità”*.

Il decreto del Presidente del Consiglio dei Ministri del 22 ottobre 1999, n. 437 ha quindi definito il regolamento per il rilascio della carta di identità elettronica e del documento di identità elettronico, mentre il decreto del Ministro dell'interno del 19 luglio 2000 ha fissato le relative regole tecniche e di sicurezza.

La Carta Nazionale dei Servizi è introdotta nel quadro normativo italiano dal Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa (decreto del Presidente della Repubblica 28 dicembre 2000, n. 445), modificato dal decreto legislativo 23 gennaio 2002 n.10 e dal decreto del Presidente della Repubblica 7 aprile 2003 n. 137, in attuazione della direttiva europea 1999/93/CE relativa ad un quadro comunitario per le firme elettroniche.

Nel Testo unico la Carta Nazionale dei Servizi è definita come *“il documento rilasciato su supporto informatico per consentire l'accesso per via telematica ai servizi erogati dalla pubblica amministrazione”* (articolo 1 lettera bb). Tale definizione è rimasta inalterata (articolo 1, comma 1, lettera d)) nel decreto legislativo 4 aprile 2006, n. 159 recante *“Disposizioni integrative e correttive al decreto legislativo 7 marzo 2005, n. 82, recante codice dell'amministrazione digitale”*.

Il medesimo decreto legislativo aggiorna anche le regole per l'accesso ai servizi erogati in rete dalle pubbliche amministrazioni. L'articolo 64 contiene queste regole e di seguito lo si riporta per comodità in modo integrale:

“64. Modalità di accesso ai servizi erogati in rete dalle pubbliche amministrazioni.

1. La carta d'identità elettronica e la carta nazionale dei servizi costituiscono strumenti per l'accesso ai servizi erogati in rete dalle pubbliche amministrazioni per i quali sia necessaria l'autenticazione informatica.

2. Le pubbliche amministrazioni possono consentire l'accesso ai servizi in rete da esse erogati che richiedono l'autenticazione informatica anche con strumenti diversi dalla carta d'identità elettronica e dalla carta nazionale dei servizi, purché tali strumenti consentano di accertare l'identità del soggetto che richiede l'accesso. L'accesso con carta d'identità elettronica e carta nazionale dei servizi è comunque consentito indipendentemente dalle modalità di accesso predisposte dalle singole amministrazioni.

3. Ferma restando la disciplina riguardante le trasmissioni telematiche gestite dal Ministero dell'economia e delle finanze e dalle agenzie fiscali, con decreto del Presidente del Consiglio dei Ministri o del Ministro delegato per l'innovazione e le tecnologie, di concerto con il Ministro per la funzione pubblica e d'intesa con la Conferenza unificata di cui all'articolo 8 del decreto legislativo 28 agosto 1997, n. 281, è fissata la data, comunque non successiva al 31 dicembre 2007, a decorrere dalla quale non è più consentito l'accesso ai servizi erogati in rete dalle pubbliche amministrazioni, con strumenti diversi dalla carta d'identità elettronica e dalla carta nazionale dei servizi. E' prorogato alla medesima data il termine relativo alla procedura di accertamento preventivo del possesso della Carta di identità elettronica (CIE), di cui all'articolo 8, comma 5, del decreto del Presidente della Repubblica 2 marzo 2004, n. 117, limitatamente alle richieste di emissione di Carte nazionali dei servizi (CNS) da parte dei cittadini non residenti nei comuni in cui è diffusa la CIE.”

2.1 Il regolamento di attuazione

L'attuazione di quanto previsto nel Testo unico è disciplinata dal decreto del Presidente della Repubblica 2 marzo 2004, n. 117 “Regolamento recante disposizioni la diffusione della carta nazionale dei servizi, a norma dell'articolo 27, comma 8, lettera b), della legge 16 gennaio 2003, n.3”.

In tale decreto si precisa che la Carta Nazionale dei Servizi è emessa dalle pubbliche amministrazioni interessate *“al fine di anticiparne le funzioni di accesso ai servizi in rete delle pubbliche amministrazioni”* (art. 2 comma 1). Quindi la CNS è intesa quale strumento “ponte” verso la carta d'identità elettronica, che resta il mezzo nazionale per l'identificazione in rete.

La CNS viene emessa se l'utente non è in possesso della Carta d'Identità Elettronica². Al momento dell'emissione l'amministrazione, oltre a verificare tale condizione, controlla i dati identificativi utilizzando i servizi telematici resi disponibili dall'Indice nazionale delle anagrafi³. Se i controlli hanno esito positivo, l'amministrazione emette la CNS ed aggiorna l'indice inviando il codice numerico identificativo della carta e le date di rilascio e di scadenza (art. 2 comma 3). In questo contesto è importante tenere in conto quanto disposto nell'articolo 64, comma 3 del decreto legislativo 4 aprile 2006, n. 159 cioè le “Disposizioni integrative e correttive al decreto legislativo 7 marzo 2005, n. 82, recante codice dell'amministrazione digitale”.

Esso tra l'altro stabilisce che *“...è fissata la data, comunque non successiva al 31 dicembre 2007, a decorrere dalla quale non è più consentito l'accesso ai servizi erogati in rete dalle pubbliche amministrazioni, con strumenti diversi dalla carta d'identità elettronica e dalla carta nazionale dei servizi. E' prorogato alla medesima data il termine relativo alla procedura di accertamento preventivo del possesso della Carta d'identità elettronica (CIE), di cui all'articolo 8, comma 5, del decreto del Presidente della Repubblica 2 marzo 2004, n. 117, limitatamente alle richieste di emissione di Carte nazionali dei servizi (CNS) da parte dei cittadini non residenti nei comuni in cui è diffusa la CIE.*

² Le funzioni telematiche della CNS sono le stesse della Carta d'Identità Elettronica, dunque è superfluo fornire la prima a chi è già in possesso della seconda.

³ I servizi di validazione dei dati sono erogati dal Centro Nazionale per i Servizi Demografici, ai sensi dell'art. 2-*quater* del decreto legge 27 dicembre 2000, n.392, convertito dalla legge 28 febbraio 2001. Il regolamento di attuazione prevede la stipula di convenzioni tra il Ministero dell'interno ed i Comuni per l'accesso all'Indice Nazionale delle Anagrafi (INA), con la finalità di garantire a livello nazionale la congruenza e la correttezza delle informazioni anagrafiche.

Strutturalmente, la CNS è una smart card che contiene un certificato elettronico per l'autenticazione in rete del titolare. Tale certificato deve essere emesso da un certificatore abilitato al rilascio dei certificati per la firma digitale⁴ (art. 3 comma 1).

Il decreto rinvia alle regole tecniche la definizione delle proprietà informatiche della carta, mentre, per quanto concerne l'aspetto esteriore, impone unicamente che sul dorso sia presente la dicitura "CARTA NAZIONALE DEI SERVIZI" ed il nome della pubblica amministrazione che l'ha emessa (art. 3 comma 4).

Oltre ai dati comuni a tutte le CNS (descritti nelle regole tecniche), la carta può contenere informazioni aggiuntive, ossia *indicazioni di carattere individuale generate, gestite e distribuite dalle pubbliche amministrazioni per attività amministrative e per l'erogazione dei servizi al cittadino*, con l'eccezione dei dati personali sensibili (art. 4 comma 1).

Il comma 2 dell'articolo 4 stabilisce il principio secondo cui i dati personali presenti nella carta (compreso il codice fiscale) devono essere utilizzati esclusivamente per la finalità di *identificare in rete il titolare della carta nazionale dei servizi e per verificare la sua legittimazione al servizio*. Questo comma inserisce nel giusto contesto il principio di necessità introdotto dal Codice in materia di protezione dei dati personali⁵ (DL 30 giugno 2003, n. 196, art. 3) chiarendo che le informazioni personali presenti sulla carta devono essere utilizzate esclusivamente per la finalità di abilitare l'accesso ai servizi. E' opportuno osservare che, in conseguenza del principio di necessità espresso dal Codice della privacy, non sono consentite applicazioni che leggono i dati personali sulla carta e quindi li trasmettono via rete allorché sono disponibili tecniche che permettono l'identificazione e l'autorizzazione attraverso il codice di identificazione (codice fiscale) presente nel certificato digitale.

Particolarmente importante è il comma 2 dell'articolo 5 che recita: *tutte le pubbliche amministrazioni che erogano servizi in rete devono consentirne l'accesso ai titolari delle carta nazionale dei servizi indipendentemente dall'ente di emissione, che è responsabile del suo rilascio*. Questa norma, confermata nel Codice dell'amministrazione digitale, conferma e ribadisce che i servizi in rete erogati dalle pubbliche amministrazioni siano progettati in modo da accettare l'identificazione e l'autenticazione tramite la Carta nazionale dei Servizi, qualunque sia l'ente che l'ha emessa.

In pratica tutti i servizi della pubblica amministrazione dovranno prevedere una doppia modalità di autenticazione:

- tramite le carte per l'accesso ai servizi in rete (Carta d'identità elettronica e Carta nazionale dei servizi);
- con modalità alternative (PIN, password, ecc.) per gli utenti che ancora non dispongono di tali strumenti.

Il regolamento prevede inoltre la presenza di un sistema per interdire l'operatività della carta nazionale dei servizi in caso di smarrimento o furto della stessa. In sostanza viene prevista la presenza di un sistema di liste di revoca accessibili per via telematica, rimandando alle regole tecniche la definizione della modalità di accesso alle stesse (art. 6 ed art. 7 comma 1).

La competenza in merito ai controlli di qualità sulle procedure e sui dati utilizzati per l'emissione delle carte nazionali è assegnata al *Centro nazionale per l'informatica nella pubblica amministrazione (CNIPA)*. Quest'ultimo ha anche il compito di definire le iniziative atte a migliorare il sistema dei servizi accessibili in rete (art. 7 comma 2).

Le disposizioni transitorie sono rivolte principalmente a regolamentare l'allineamento dell'Indice Nazionale delle Anagrafi fino a quando tale sistema non sarà nella fase di regime, ossia in attesa della sottoscrizione delle convenzioni previste dal regolamento. Durante tale fase l'allineamento dell'indice delle anagrafi avverrà in modalità differita attraverso la procedura di seguito descritta.

Le amministrazioni, all'atto dell'emissione, effettuata la verifica dei dati identificativi del titolare della carta, rilasceranno la CNS ed invieranno all'Indice nazionale delle anagrafi i dati identificativi della

⁴ Il certificatore deve essere iscritto nell'elenco pubblico secondo quanto disposto dall'articolo 29, comma 6 del decreto legislativo 4 aprile 2006, n. 159.

⁵ I sistemi informativi e i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità

persona, il codice numerico identificativo della carta, la data del rilascio e la data di scadenza. Successivamente l'Indice nazionale delle anagrafi verificherà la correttezza di tali dati e, se la verifica avrà esito positivo, inserirà nella propria banca dati le informazioni relative all'emissione della CNS. Nel caso la verifica manifesti l'assenza delle informazioni anagrafiche presso dell'Indice nazionale delle anagrafi, quest'ultimo trasmetterà i dati anagrafici al comune competente affinché li convalidi⁶ e, ricevuta la convalida, aggiornerà l'Indice. Nel caso in cui la verifica evidenzi l'inesattezza dei dati anagrafici, l'Indice nazionale delle anagrafi segnalerà all'amministrazione emittente la necessità di attivarsi nei confronti del titolare per interdire la carta emessa (art. 8 commi 2 e 3).

Al fine di assicurare l'aggiornamento delle informazioni presenti nella carta, l'Indice nazionale delle anagrafi segnalerà all'amministrazione che ha emesso la CNS eventuali variazioni dei dati identificativi del titolare comunicate dal Comune di residenza del titolare all'Indice nazionale delle anagrafi; a seguito di ciò l'amministrazione di emissione dovrà interdire la carta emessa (art. 8 comma 4).

Un'ulteriore norma transitoria riguardava la verifica preventiva del possesso della carta d'identità elettronica: fintantoché il sistema di allineamento dell'Indice nazionale delle anagrafi non sarà nella fase di regime (e comunque non oltre il 31 dicembre 2005) tale verifica potrà essere effettuata *limitatamente ai residenti nei comuni che diffondono la carta d'identità elettronica, previo accordo con i comuni interessati* (art. 8 comma 5). Tale norma è stata modificata nel Codice dell'amministrazione digitale aggiornato nel 2006 (cfr. art. 64, comma 3).

2.2 Le regole tecniche

Le regole tecniche individuano le caratteristiche informatiche della Carta Nazionale dei Servizi e la modalità di gestione del ciclo di vita della stessa.

Esse sono definite nel decreto del Presidente del Consiglio dei ministri 9 dicembre 2004 "Regole tecniche e di sicurezza relative alle tecnologie e ai materiali utilizzati per la produzione della Carta nazionale dei servizi".

Nel seguito vengono sintetizzati alcuni aspetti essenziali per la caratterizzazione della CNS.

In particolare la CNS è caratterizzata da tre funzionalità principali:

- la CNS è uno strumento di identificazione in rete;
- la CNS può essere predisposta per operare come carta sanitaria (Netlink);
- la CNS deve essere predisposta per ospitare il servizio di firma digitale, fornendo al titolare la possibilità di sottoscrivere documenti informatici.

Queste tre funzionalità devono essere comuni a tutte le CNS, anche se le ultime due possono non essere attive al momento dell'emissione della carta.

2.2.1 Caratteristiche della carta e standard di riferimento

La CNS non presenta particolari restrizioni per quanto riguarda la struttura del supporto fisico, dovranno essere comunque rispettati i vincoli imposti dagli standard internazionali sulle smart card, con particolare attenzione alle norme che regolamentano i documenti di identità (ISO/IEC 7816-1-2).

Le dimensioni, lo spessore e le tolleranze devono essere conformi a quanto specificato dalla norma ISO/IEC 7810: 1995 per la carta di tipo ID-1.

Sulla carta deve essere presente la scritta Carta Nazionale dei Servizi ed è consigliato l'inserimento del logo dell'Ente emittitore. I dati da stampare sulla CNS e l'eventuale loro memorizzazione sul microchip sono decisi e disposti dall'Ente emittitore che la rilascerà.

⁶ Si noti che non è detto che l'amministrazione emittente coincida con il comune di residenza del titolare della carta, per cui è necessaria questa fase di convalida da parte di quest'ultimo.

Le regole tecniche precisano comunque che l'aspetto della CNS deve essere tale da evitare che la carta possa essere scambiata per un documento di riconoscimento a vista, per cui *sulla CNS non devono essere presenti dei dati utilizzabili in alcun modo per il riconoscimento a vista del titolare, come per esempio la fotografia.*

Per quanto concerne le caratteristiche interne della carta, le regole tecniche stabiliscono che deve essere presente una memoria EEPROM della capacità non inferiore a 32 KB.

Inoltre, il microprocessore deve essere conforme agli standard ISO/IEC 7816 parte 3, 4 e 8.

Inoltre, in aggiunta a quanto prescritto dallo standard ISO/IEC 7816 parte 4 circa i comandi del sistema operativo, dovranno essere rispettate le specifiche del sistema operativo (APDU) oggetto del protocollo d'intesa per la realizzazione dei progetti Carta d'identità elettronica e Carta nazionale dei servizi (cfr. il sito Internet del CNIPA www.cnipa.gov.it).

2.2.2 La certificazione della smart card

Dall'obbligo relativo alla predisposizione per la funzionalità di firma digitale derivano alcune caratteristiche fondamentali delle smart card. Infatti, per poter ospitare la firma digitale, la smart card deve essere conforme a quanto stabilito dal più volte citato Codice dell'amministrazione digitale.

In particolare, la smart card dovrà avere le caratteristiche di un "dispositivo sicuro per la generazione della firma" basata su quanto stabilito nell'articolo 35 del Codice dell'amministrazione digitale⁷. Le regole tecniche per la firma digitale precisano che *i dispositivi sicuri di firma di cui all'articolo 29-sexies del testo unico, devono essere conformi alle norme generalmente riconosciute a livello internazionale o individuate dalla Commissione europea secondo la procedura di cui all'articolo 9 della direttiva n. 1999/93/CE.*

La decisione della Commissione europea del 14 luglio 2003 circa i riferimenti a standard generalmente riconosciuti per i prodotti di firma elettronica ha riportato, relativamente ai dispositivi sicuri per la creazione della firma, lo standard CWA 14169 (marzo 2002) che dunque costituisce il riferimento (peraltro non esclusivo) per la certificazione delle smart card che possono ospitare la firma elettronica⁸. Potranno essere anche accettati dispositivi dichiarati conformi alle caratteristiche di sicurezza di un dispositivo sicuro di firma, mediante apposita dichiarazione e certificazione da parte di un "certification body" accreditato operante anche all'interno dell'Unione Europea.

2.2.3 Le informazioni registrate nella memoria della carta

La struttura della memoria interna della carta è conforme al file di sistema (file system) pubblicato sul sito del Centro nazionale per l'informatica nella pubblica amministrazione.

La struttura del file di sistema è stata concepita per consentire un uso flessibile della CNS e può essere suddivisa in:

- un'area necessaria per la gestione della carta (DF0, DF1, PIN, PUK, Id_carta, PIN_SO);
- un'area contenente le informazioni necessarie per l'autenticazione in rete (Kpri, c_carta, Dati_personali);
- un'area predisposta per le funzioni di carta sanitaria (Carta_sanitaria);
- un'area predisposta per le funzioni di firma digitale (Firma_digitale);

⁷ Si riportano i primi due commi dell'articolo 35 :1. *I dispositivi sicuri e le procedure utilizzate per la generazione delle firme devono presentare requisiti di sicurezza tali da garantire che la chiave privata: a) sia riservata; b) non possa essere derivata e che la relativa firma sia protetta da contraffazioni; c) possa essere sufficientemente protetta dal titolare dall'uso da parte di terzi.*

2. *I dispositivi sicuri di cui al comma 1 devono garantire l'integrità dei dati elettronici a cui la firma si riferisce. I dati devono essere presentati al titolare, prima dell'apposizione della firma, chiaramente e senza ambiguità, e si deve richiedere conferma della volontà di generare la firma.*

3. *Il secondo periodo del comma 2 non si applica alle firme apposte con procedura automatica, purché l'attivazione della procedura sia chiaramente riconducibile alla volontà del titolare.*

4. *I dispositivi sicuri di firma sono sottoposti alla valutazione e certificazione di sicurezza ai sensi dello schema nazionale per la valutazione e certificazione di sicurezza nel settore della tecnologia dell'informazione di cui all'articolo 10, comma 1, del decreto legislativo 23 gennaio 2002, n. 10.*

⁸ In sostanza per la CNS si deve utilizzare una smart card certificata in base alla norma ISO/IEC 15408 (Common Criteria) secondo il Protection Profile riportato nell'allegato A dello standard CWA 14169.

- un'area disponibile per eventuali servizi aggiuntivi (Memoria_residua).

La tabella 1 delle regole tecniche riporta la descrizione dei campi elencati e, per ogni campo, le responsabilità in merito alla generazione, la predisposizione e la registrazione dell'informazione.

Il file elementare dei dati personali è codificato secondo le modalità previste per la Carta d'Identità Elettronica, riportate nella tabella 2 delle regole tecniche.

Viene inoltre precisato che, nel contesto della Carta Nazionale dei Servizi, in aggiunta a quanto definito per la CIE, la locuzione "dati identificativi della persona" si riferisce ai dati anagrafici ed al codice fiscale, dove, per dati anagrafici si intende il nome, il cognome, il sesso, la data, il luogo di nascita e il comune di residenza al momento dell'emissione.

2.2.4 L'emissione della CNS

Le regole tecniche chiariscono che la CNS può essere emessa da tutte le pubbliche amministrazioni. La Pubblica Amministrazione che emette la CNS è definita **ente emittitore** ed è responsabile:

- della correttezza dei dati identificativi memorizzati nella carta e nel certificato di autenticazione;
- della correttezza del codice fiscale memorizzato nella carta e riportato nel certificato di autenticazione;
- della sicurezza delle fasi di produzione, inizializzazione, distribuzione ed aggiornamento/ritiro della carta;
- dell'invio dei dati identificativi al Ministero dell'interno, Centro Nazionale Servizi Demografici, per l'aggiornamento dell'INA, secondo le modalità previste dal regolamento di attuazione, con procedure operative e formati che saranno definiti da apposita circolare del Ministero dell'interno.

Si osserva che non è richiesto che l'Ente emittitore effettui in proprio le attività necessarie alla personalizzazione, al rilascio ed alla successiva gestione della carta, esso comunque, anche nel caso queste attività vengano delegate ad altre strutture, ne mantiene le responsabilità ed è il referente diretto nei confronti del Ministero dell'interno - Centro Nazionale Servizi Demografici.

Durante la fase preparatoria, l'ente emittitore analizza ed individua i servizi da rendere disponibili in rete mediante CNS, valuta l'offerta di mercato relativa alla fornitura delle smart card e decide se far fronte in maniera autonoma all'emissione della CNS, ovvero utilizzare servizi di strutture delegate. Eventualmente stipula accordi con le Regioni per la predisposizione delle carte con le funzionalità di tessera sanitaria.

L'ente emittitore avvia la produzione di un lotto di CNS, si dota eventualmente di tutte le risorse hardware e software necessarie all'emissione della CNS, tenendo conto delle direttive e delle norme vigenti⁹, commissiona quindi al produttore individuato la fornitura dei lotti di CNS inizializzate.

L'Ente emittitore non è l'unico soggetto che concorre al processo di emissione della CNS. Gli altri soggetti sono:

il **produttore**, ossia l'azienda che provvede alla fornitura delle carte a microprocessore con un chip compatibile con quello previsto dalla CNS, che predispose opportunamente gli spazi dedicati alla carta sanitaria (Netlink) ed alla firma digitale, che applica al supporto fisico l'artwork e gli elementi costanti;

il **certificatore**, cioè il soggetto che presta servizi di certificazione delle informazioni necessarie per l'autenticazione o per la verifica delle firme elettroniche (sono abilitati a prestare servizi di certificazione per la CNS i soggetti di cui all'articolo 5 del Decreto Legislativo n.10 del 23 gennaio 2002 per le informazioni relative all'autenticazione o alla firma elettronica).

⁹ In generale si dovrà ricorrere ad una procedura di appalto concorso di tipo aperto. Nel disciplinare di gara dovranno quindi essere indicati gli elementi di conformità alle caratteristiche ed agli standard della CNS (norme di riferimento, APDU, file system, criteri di sicurezza, certificazione, ecc.)

2.2.5 Il circuito della CNS

Le regole tecniche stabiliscono le modalità con cui deve essere prodotta, rilasciata emessa e gestita la Carta Nazionale dei Servizi.

Attività a carico del produttore

Il produttore della CNS è responsabile della produzione della carta plastica, della sua inizializzazione tramite la generazione del file system, e della creazione delle condizioni necessarie per controllare l'accesso ai file.

L'operazione di inizializzazione è finalizzata a produrre in maniera sicura delle carte che siano pronte ad essere personalizzate, ossia risultino in uno stato definito "Attivate".

Attività a carico dell'ente emettitore

L'ente emettitore è responsabile della registrazione degli utenti, dell'aggiornamento dell'Indice Nazionale delle Anagrafi, della personalizzazione e consegna della CNS e della successiva gestione della carta.

La registrazione consiste nell'identificazione del cittadino attraverso un documento di riconoscimento valido. Al momento della registrazione, il cittadino deve dichiarare di non possedere la Carta d'Identità Elettronica.

Prima di personalizzare la CNS, l'ente emettitore verifica i dati identificativi ed aggiorna l'Indice Nazionale delle Anagrafi, direttamente o tramite struttura delegata, mediante i servizi del sistema informativo del Ministero dell'Interno – Centro Nazionale dei Servizi Demografici (in via transitoria potrà essere utilizzata la procedura differita prevista dall'articolo 9 del regolamento attuativo).

La personalizzazione delle carte ed il loro rilascio è condotta dagli enti emettitori per mezzo di strutture proprie o esterne. Nel corso dell'attività di personalizzazione, vengono inserite le informazioni utente necessarie per l'identificazione in rete e per gli altri servizi previsti, viene inoltre generato il PIN_utente ed il PUK, utilizzabile per lo sbocco della carta nel caso di iterata digitazione errata del PIN. Il PIN ed il codice PUK sono stampati in buste retinate atte a garantire la riservatezza di tali informazioni.

Dopo la personalizzazione, la CNS viene consegnata al titolare, previa verifica dell'identità, unitamente alla busta contenente il PIN ed il codice PUK. L'ente emettitore deve illustrare al titolare le modalità di uso della carta e le procedure che dovranno essere utilizzate in caso di anomalie o disservizi. Deve fornire al titolare un numero telefonico per l'assistenza in caso di problemi ed il numero telefonico utile per richiedere la sospensione o la revoca.

L'ente emettitore provvede inoltre alla gestione delle CNS emesse predisponendo le strutture per l'assistenza agli utenti, la gestione dei malfunzionamenti e l'eventuale sostituzione o rinnovo delle carte in scadenza (anche per le funzioni di gestione delle carte l'ente può avvalersi di strutture delegate), provvede inoltre al ritiro della CNS a seguito di problemi di funzionamento della smart card o allorché questa abbia raggiunto il naturale termine di scadenza. L'ente emettitore è tenuto al ritiro della CNS prima dell'emissione di una nuova carta o del suo rinnovo.

Attività a carico del certificatore

Il certificatore è responsabile della generazione del certificato di autenticazione. Le informazioni anagrafiche ottenute in fase di registrazione, congiuntamente con la chiave pubblica generata in fase di personalizzazione, sono utilizzate dal certificatore per generare il certificato secondo le specifiche riportate in appendice e disponibili presso il sito del Centro Nazionale per l'Informatica nella Pubblica Amministrazione (www.cnipa.gov.it).

2.2.6 La gestione della CNS

L'ente emettitore è responsabile della gestione del circuito di emissione che a lui fa capo. L'ente dovrà definire le procedure di gestione, personalizzazione e rilascio delle carte CNS e descriverle in un apposito manuale operativo accessibile al pubblico, dovrà inoltre predisporre, eventualmente avvalendosi di terzi, le strutture per l'assistenza agli utenti, per la gestione dei malfunzionamenti e l'eventuale sostituzione o rinnovo delle carte in scadenza, infine, è responsabile di definire un servizio di "contact center" per l'assistenza, nonché la revoca o sospensione della CNS.

L'ente emittitore può distribuire software di complemento alla CNS, tenendo in conto che il software per la CIE è distribuito dal Ministero dell'Interno.

L'ente emittitore ha la facoltà di procedere di propria iniziativa alla revoca della CNS; in tal caso ha l'obbligo di avvertire il titolare esplicitando le motivazioni della revoca.

2.2.7 Requisiti per la partecipazione al circuito della CNS

Produttori

Ai fini della sicurezza dell'intero circuito di emissione, i fornitori di smart card che intendono offrire i propri servizi agli enti emittitori per le fasi di inizializzazione delle smart card, devono rispettare le specifiche previste nel presente documento.

In particolare, i fornitori sono vincolati al rispetto delle specifiche del sistema operativo (APDU) e della struttura interna della carta (file system) pubblicate sul sito del Centro Nazionale per l'informatica nella pubblica amministrazione.

Ogni consegna di lotti di CNS dovrà essere accompagnata da distinta cartacea o elettronica, da consegnare all'ente emittitore richiedente, dalla quale si evinca il numero di CNS inizializzate ed i relativi numeri seriali.

Enti emittitori

Per quanto riguarda gli enti emittitori, essi devono rispettare caratteristiche di qualità e di affidabilità tali da garantire la sicurezza dell'intero circuito.

In particolare devono:

- definire le procedure del sistema di emissione e gestione della CNS in modo conforme alle specifiche di qualità previste dalla norma ISO 9000;
- soddisfare i requisiti di sicurezza del circuito della CNS;
- definire modalità di interazione con i produttori ed i certificatori che forniscano adeguate garanzie di affidabilità e sicurezza;
- predisporre un manuale operativo che evidenzi le procedure seguite per la gestione di tutte le fasi del processo di emissione e di gestione della CNS;
- predisporre un manuale utente che illustri le modalità d'uso della CNS, i modi per usufruire dei servizi in rete e le procedure da seguire in caso di smarrimento, furto o timore di compromissione della carta;
- organizzarsi in modo da costituire il riferimento per ogni problema di funzionalità, disponibilità o sicurezza del circuito di emissione, rendendo disponibile un recapito telefonico costantemente attivo;
- predisporre il piano della sicurezza relativo all'intero circuito di emissione.

L'ente emittitore può avvalersi di servizi di terzi per lo svolgimento delle funzioni di emissione della CNS o di parte di esse, purché questi assicurino il rispetto dei requisiti di cui ai precedenti punti.

L'ente emittitore mantiene la responsabilità della sicurezza del circuito di emissione e del rispetto delle normative vigenti in merito alla tutela dei dati personali. L'ente emittitore ha comunque la facoltà di trasferire, nei termini di legge, tale responsabilità a terzi.

Certificatori

Possono operare come emittitori dei certificati di autenticazione della CNS esclusivamente i certificatori accreditati di cui all'articolo 5 del Decreto Legislativo 23 gennaio 2002, n.10.

Tali soggetti devono operare in aderenza alle vigenti norme che regolano l'emissione e la gestione dei certificati qualificati.

I certificatori che rilasciano certificati di autenticazione CNS sono iscritti in un elenco consultabile in via telematica, tenuto dal CNIPA in perfetta analogia con la normativa sulla firma digitale.

2.2.8 La sicurezza

La sicurezza della CNS dipende:

- dalle caratteristiche intrinseche della carta;
- dalla modalità con cui questa viene utilizzata e gestita;
- dalla sicurezza del ciclo di produzione e del circuito della CNS.

Per quanto concerne il primo punto, le regole tecniche fanno riferimento a standard che assicurano un elevato livello di protezione delle carte nei confronti di possibili attacchi.

Il secondo aspetto viene demandato alla responsabilità dell'ente emittitore che ha il compito di fornire una adeguata informativa all'utente sulle regole per il corretto uso della carta e sulle procedure da seguire in caso di problemi.

Per quanto concerne l'ultimo aspetto, va osservato che il modello adottato permette diverse soluzioni organizzative. Infatti, in funzione delle strategie e delle scelte di mercato dell'ente emittitore, le strutture che concorrono alla produzione e gestione della CNS possono far capo ad un diverso numero di organizzazioni, non escludendosi il caso che una stessa organizzazione gestisca l'intero ciclo di vita della CNS.

Le regole tecniche forniscono dunque delle indicazioni di carattere generale che devono trovare corretta applicazione nell'effettivo contesto operativo. Tali indicazioni saranno esposte in un successivo capitolo del presente documento.

L'ente emittitore potrà definire varianti alle linee guida che consentano una maggiore flessibilità, mantenendo livelli di sicurezza equivalenti. L'Ente emittitore, peraltro, può adempiere a tali requisiti utilizzando fornitori già in possesso di idonea certificazione o accreditamento nazionale o internazionale.

Capitolo 3

Interoperabilità tra le carte

La proliferazione non controllata di carte di differenti produttori, anche se omogenea con gli standard di riferimento, comporta un elevato rischio di interoperabilità anche tra applicazioni coerenti. Ne consegue che l'interoperabilità deve essere garantita, al fine di evitare sprechi di risorse, tramite ulteriori regole.

Tali regole possono essere il risultato di due scelte architetturali:

- uniformità del sistema operativo della smart card, della sua organizzazione e struttura interna dei dati;
- appropriato riconoscimento della carta da parte dell'applicazione che gestisce quest'ultima.

Nei paragrafi successivi viene trattata in dettaglio la tematica dell'interoperabilità, approfondendo gli aspetti tecnici e funzionali e fornendo delle motivazioni relative alla scelta effettuata.

Prima di entrare nel dettaglio delle possibili soluzioni, saranno esaminati gli standard riconosciuti a livello internazionale che disciplinano la materia delle smart card (carte a microcircuito).

E' bene, inoltre, ricordare che i progetti che utilizzano pienamente la specifica Netlink (descritta nel capitolo successivo), devono prevedere due distinte tipologie di carte: la carta del cittadino (CNS) e la carta dell'operatore sanitario.

La carta del cittadino, che ha la funzione di carta sanitaria, contiene le informazioni di carattere sanitario e le chiavi simmetriche segrete, derivate dalle chiavi di gruppo custodite dalle strutture del Ministero della salute, al fine di custodire le informazioni sensibili. Essa contiene inoltre la chiave asimmetrica privata e il certificato digitale del cittadino utilizzate per i processi di autenticazione e attestazione che saranno descritti nel seguito. La carta dell'operatore sanitario contiene le chiavi di gruppo del Ministero della salute per accedere ai dati protetti della carta del cittadino, certificato e chiave asimmetrica privata per la firma digitale. Infine contiene il certificato e la chiave asimmetrica privata per i processi di autenticazione e cifratura dei dati.

E' bene anche ricordare che la descrizione successiva è svolta per completezza descrittiva, ma la soluzione di riferimento è quella presentata nel successivo capitolo relativo al Protocollo d'intesa 13 maggio 2003.

3.1 Standard di riferimento

Lo standard internazionale che definisce, nell'ambito delle carte a microcircuito, le caratteristiche fisiche ed elettriche, il protocollo di comunicazione, il protocollo applicativo, l'organizzazione dei dati e gli aspetti di sicurezza è la norma ISO/IEC 7816. Essa è suddivisa nelle seguenti parti:

- Parti 1 e 2 per la definizione delle dimensioni, delle caratteristiche meccaniche ed elettriche, le condizioni ambientali di funzionamento e la disposizione dei contatti elettrici;
- Parte 3 che disciplina in merito ai seguenti temi :
 - le caratteristiche elettriche dell'interfaccia;
 - il protocollo di comunicazione per il trasferimento dei comandi tra lettore e carta;
 - la risposta al comando di "reset" (ATR) in cui sono contenute le informazioni atte ad individuare il tipo di carta ed il costruttore della stessa.
- Parte 4 che disciplina in merito ai seguenti temi :
 - il formato dei comandi applicativi (APDU) per accedere ai dati ed alle funzioni di sicurezza interne della carta;
 - le modalità per costruire ed organizzare le strutture dati (file system);
 - le modalità di accesso;
 - la tipologia delle strutture dati ovvero la tipologia dei file che conterranno i dati.
- Parte 5 che disciplina in merito alle procedure per l'ottenimento degli "application identifiers";
- Parte 6 che disciplina in merito allo "Inter-industry data element" cioè la modalità con cui descrivere e codificare i dati all'interno della smart card;
- Parte 7 (non pubblicata);
- Parte 8 che disciplina in merito ai seguenti temi :
 - protocolli di sicurezza ed estensioni del secure messaging definito nella parte 4 della norma;
 - la definizione degli ambienti di sicurezza e la loro gestione;
 - l'estensione dei comandi applicativi (APDU), definiti nella parte 4, per la gestione degli ambienti di sicurezza e l'espletamento delle funzioni di sicurezza (es.: gestione della chiave privata di firma, comando di firma digitale,etc.).
- Parte 9 che disciplina in merito ai seguenti temi :
 - la gestione del ciclo di vita della carta e degli oggetti ad essa correlati;
 - definizione degli attributi di sicurezza degli oggetti crittografici;
 - formalizzazione, rispetto a quanto definito nella parte 4, delle condizioni di accesso;
 - estensione dei comandi applicativi (APDU), rispetto a quanto definito nella parte 4 e 8, soprattutto per ciò che concerne la gestione del ciclo di vita della carta e degli oggetti ad essa correlati.

Le parti 3,4,8 e 9 definiscono il sistema operativo della smart card e come questa si interfaccia ai dispositivi di lettura e scrittura, mentre le parti 5 e 6 specificano come definire gli identificativi delle applicazioni e come strutturare i dati contenuti nei file.

Altre parti come la 10, la 11 e la 15 sono in sviluppo o già pubblicate ma il loro contenuto è al di fuori degli scopi del presente documento.

Nei paragrafi successivi sarà fornita una panoramica sull'applicazione di tale norma da parte dei produttori di carte a microcircuito.

3.1.1 Carte e norme ISO, lo stato dell'arte

La norma ISO 7816 può essere considerata la specifica di riferimento per la progettazione delle smart card soprattutto per le carte che in gergo sono chiamate *ID-Card*, ovvero le carte di identificazione come, la Carta Nazionale dei Servizi e la Carta di Identità Elettronica. E' doveroso osservare che le varie parti della norma sono state emesse in tempi differenti e, a volte, tali da poter essere recepite solo dai fornitori che si accingevano a progettarne una nuova e tali da scoraggiare le aziende che avevano da poco immesso una carta sul mercato (ad esempio la parte 9 è stata emessa solo un anno dopo la parte 8). Un altro aspetto consiste nella libertà di interpretazione che viene lasciata in alcuni punti della norma e che spinge i produttori ad adottare soluzioni quanto più possibile vicine a quelle adottate nelle precedenti realizzazioni.

L'effetto di tutto ciò è riassumibile nel seguente modo:

- sino alla parte terza la norma è rispettata praticamente da tutti i fornitori e questo implica che a livello di protocollo fisico esiste interoperabilità e, grazie alla standardizzazione della risposta all'inizializzazione (ATR), le applicazioni sono in grado di capire con quale carta stanno interagendo e chi ne è il produttore;
- la parte quarta è ampiamente rispettata almeno per ciò che concerne l'organizzazione delle strutture dati (file system) e l'implementazione dei comandi applicativi per la creazione, cancellazione, lettura e scrittura dei file; non si può dire altrettanto per i comandi relativi alla gestione ed utilizzo delle chiavi asimmetriche utilizzati nei processi di autenticazione e di firma digitale; tali comandi sono implementati in modo proprietario;
- la parte 8 è recepita da un numero ristretto di fornitori e nella maggior parte dei casi limitatamente all'estensione dei comandi applicativi e con differenti livelli di conformità;
- la parte 9 è rispettata solo da pochissimi fornitori e da questi solo parzialmente.

Da quanto esposto si evince che l'esigenza di interoperabilità tra le carte non può essere soddisfatta solamente con la richiesta di dispositivi conformi alla norma ISO 7816 in quanto questa è soggetta ad implementazioni parziali, ma deve essere affrontata secondo le modalità anticipate nel presente capitolo.

3.1.2 Interoperabilità a livello applicativo

Questo livello di interoperabilità, come anticipato precedentemente, non pone vincoli restrittivi sul sistema operativo delle smart card, salvo la presenza di comandi consoni alle applicazioni che si vogliono sviluppare (es.: presenza di motori crittografici se devono essere attivati processi di autenticazione o di firma digitale). L'interoperabilità è garantita dagli strati Software di interfaccia, mostrati nella figura 1. Questi, che chiameremo Software di Gestione Unificata (**SGU**), consentono di utilizzare smart card di differenti fornitori senza vincoli restrittivi sul sistema operativo. L'architettura descritta si presta a processi di Autenticazione e Firma Digitale ma è carente per quanto concerne la gestione dei dati sanitari o dei servizi erogati dalle Pubbliche Amministrazioni Locali (es.: applicazioni qualificate dei Comuni). Dopo aver esaminato nel dettaglio l'architettura SW saranno mostrati gli ampliamenti per la gestione di dati non strettamente crittografici.

Inoltre, in appendice 3, vengono descritti i dati presenti sulla CNS, descrivendone contenuto e codifica.

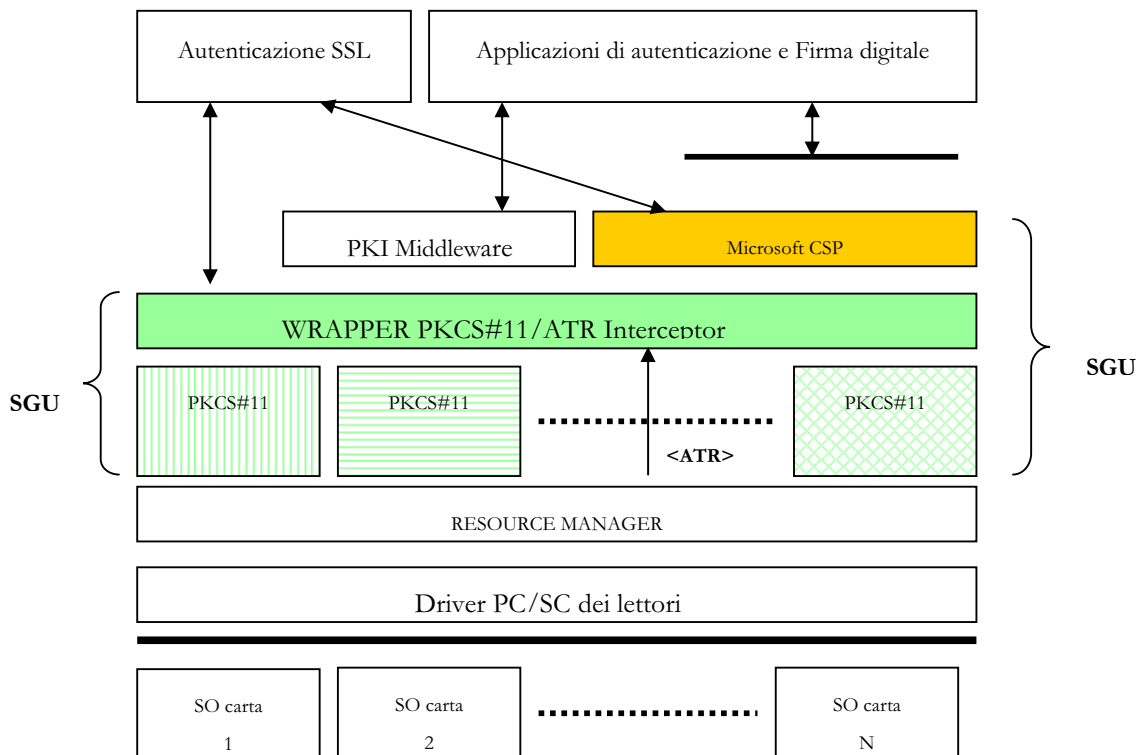


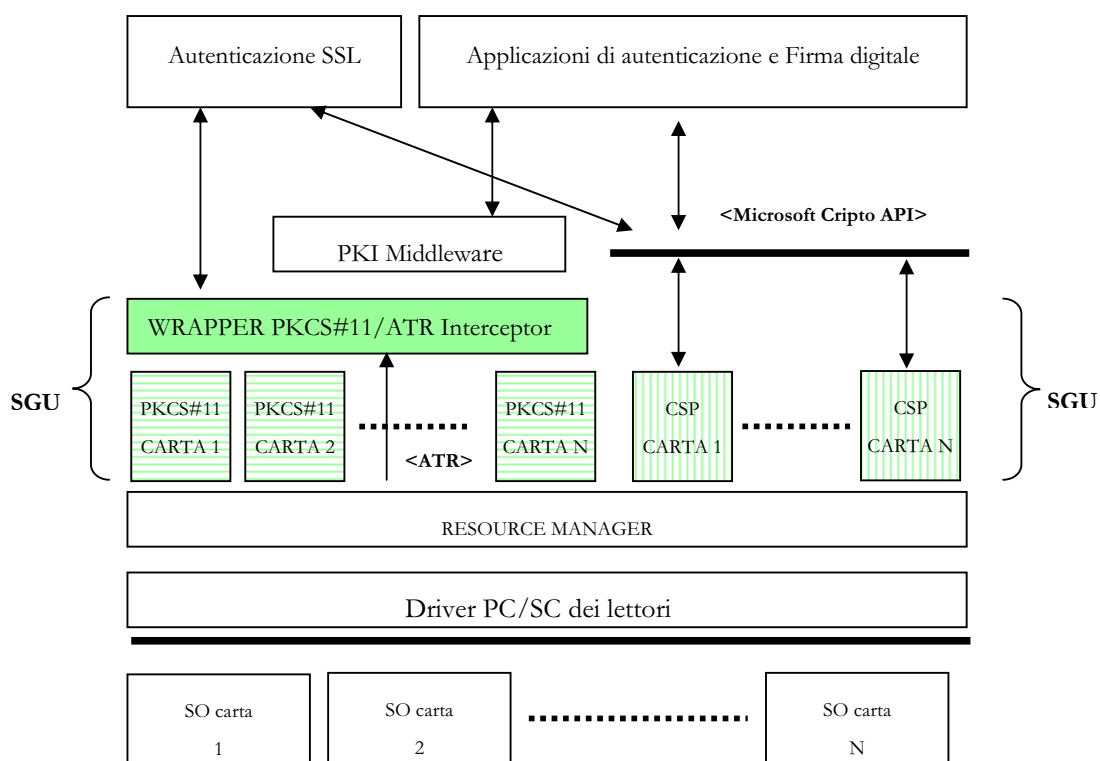
Fig. 1

In questo scenario ogni fornitore, oltre alla smart card, deve rendere disponibile anche la libreria crittografica PKCS#11, realizzata in funzione dei comandi applicativi (APDU) della propria smart card; tale libreria deve essere integrata nel Software di Gestione Unificata (SGU). All'atto dell'inserzione di una smart card il Resource Manager dell'ambiente Windows rende disponibili le informazioni della risposta al reset (ATR), fornendo quindi uno strumento per attivare la libreria PKCS#11 specifica della carta (se questa è stata prevista nel modulo SGU). L'attivazione della libreria può essere fatta dal PKCS#11 WRAPPER al quale è anche affidato il compito di rendere omogenee le funzioni esposte da ciascuna libreria.

A valle di questa operazione sarà possibile attivare i processi di autenticazione SSLv3 con i BROWSER che utilizzano le librerie PKCS#11 e processi di Firma digitale tramite applicazioni che si appoggiano a middleware crittografici di mercato (PKI Middleware).

Per consentire l'utilizzo di Browser di grande diffusione presso l'utenza, come Internet Explorer, è necessario disporre di un ulteriore strato SW esclusivo dell'ambiente Microsoft, il Crypto Service Provider (CSP). Attraverso questo strato sono possibili processi di autenticazione in modalità SSLv3 oppure applicazioni di Firma Digitale che utilizzano le Cryptographic API di Microsoft (C-API).

In genere i fornitori di carte, insieme alle librerie PKCS#11 forniscono anche le librerie CSP, necessarie per interfacciarsi con l'ambiente Microsoft (Browser IE, Outlook, OutlookExpress ...).



Le applicazioni risiedenti su PC (Application) sono messe in comunicazione con applicazioni sulla carta per mezzo del gestore delle risorse ICC (ICC Resource Manager) ed un fornitore di servizi.

Resource Manager

È il modulo più utilizzato anche in contesti e piattaforme non Microsoft e si occupa di tre aspetti legati alla gestione di lettori e carte multipli. Il componente fa parte del Sistema Operativo del PC.

Identificazione ed indirizzamento delle risorse disponibili

Contiene una lista dei lettori installati e delle carte per cui esiste un fornitore dei servizi. Identifica le interfacce supportate, sia comuni (accesso ai file e autenticazioni) che appartenenti a standard di dominio ristretto (EMV, GSM). Mantiene informazioni sulle carte inserite nei lettori e segnala inserimenti o rimozioni. Si occupa della connessione logica tra funzioni offerte dalle carte e fornitore dei servizi (Service provider).

Allocazione delle risorse tra applicazioni multiple

Permette alle applicazioni l'accesso esclusivo o condiviso a dati e funzioni della carta e fornisce lo stato delle risorse. Si occupa di accessi concorrenti a risorse in mutua esclusione.

Controllo delle transazioni per specifiche carte

Assicura che particolari sequenze di comandi siano portate a termine senza interruzioni, come avviene in contesto transazionale.

Crypto Service Provider

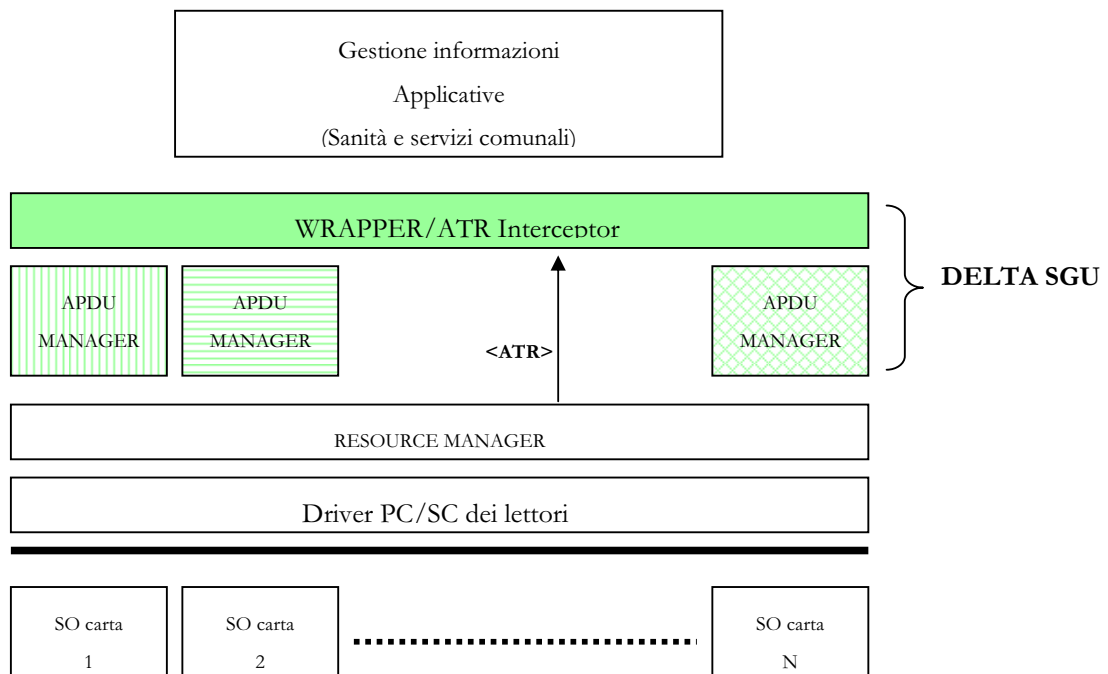
Questo componente, fornito dagli sviluppatori della carta, fornisce un'interfaccia di alto livello che definisce le funzioni supportate da una specifica carta, ed in particolare fornisce servizi crittografici, che presentano particolari condizioni di Input/Output. Contiene le specifiche di componenti opzionali dipendenti dalla specifica carta (per esempio coprocessori crittografici). Le interfacce supportate sono definite per:

- Generazione e gestione di chiavi crittografiche
- Generazione di numeri casuali
- Firme digitali
- Scambio di chiavi e gestione dati crittografati

Per poter gestire le informazioni sanitarie contenute nella smart card del cittadino, ad esempio i dati di emergenza, ed effettuare processi di autenticazione locale tra la carta dell'operatore sanitario e la carta del cittadino è necessaria una visibilità "fine" dei comandi APDU rispetto a quella offerta dalle librerie crittografiche. In questo caso i fornitori di smart card dovranno rendere disponibili ulteriori moduli SW, che chiameremo APDU Manager, allo scopo di poter intervenire sulle strutture dati delle smart card. Il Modulo Wrapper, che oltre alla libreria crittografica attiverà anche il modulo APDU Manager, dovrà essere tale da fornire alle applicazioni una visione unificata dei comandi APDU (questo modulo è più di un semplice Wrapper ed è relativamente sofisticato). La figura seguente mostra come deve essere arricchito il modulo **SGU**.

Il discorso vale anche nel caso delle librerie CSP, che inglobano il modulo ICC Service Provider. Questo componente, fornito dagli sviluppatori della carta, fornisce un'interfaccia di alto livello che definisce le funzioni supportate da una specifica carta. In generale contiene i comandi specificati dalla 7816-4, ma può includere anche particolari funzionalità personalizzate. Prima di poter fornire il servizio alle applicazioni deve essere inizializzato presso il Resource Manager.

Per quanto riguarda il WRAPPER /ATR Interceptor, in ambiente Microsoft è il resource manager che, inserita una carta del lettore, riceve la stringa ATR e la passa al servizio di winlogon. Il servizio, ricerca nel registry del S.O. la corrispondenza con gli ATR registrati e, se presente, attiva il CSP relativo.



I punti a favore di questa soluzione sono rilevanti, in quanto questa consente, entro ragionevoli limiti, di non essere condizionati dai fornitori di carte e può essere considerata uno strumento di standardizzazione. Tuttavia presenta alcuni punti a sfavore:

- se non ci si limita alla Firma Digitale o a processi di autenticazione basati sull'utilizzo di Infrastrutture a Chiave Pubblica non è sufficiente disporre delle librerie PKCS#11 /CSP e del

modulo APDU Manager, ma è necessario definire il File System delle carte, le sue modalità di navigazione e le condizioni di accesso; da questo punto di vista non è a priori certo che una carta valga l'altra anche se entrambe sono dotate di motori crittografici indispensabili nei processi di Firma ed Autenticazione;

- l'architettura SW descritta è efficiente nella fase di utilizzo delle smart card ma non considera in modo esaustivo le fasi di inizializzazione ed emissione che restano vincolate al sistema operativo della Carta; questo aspetto deve essere valutato con attenzione quando si intenda distribuire sul territorio milioni di carte come nel caso del progetto CRS-SISS.

Il modulo **SGU** precedentemente descritto ha un discreto livello di sofisticazione e deve essere mantenuto aggiornato in termini di librerie PKCS#11, CSP e moduli APDU manager. Questa soluzione potrebbe rivelarsi uno strumento poco efficiente nell'ottica di una distribuzione capillare ai cittadini che intendano utilizzare la smart card sul proprio Personal Computer per accedere ai servizi resi disponibili dalle Pubbliche Amministrazioni.

3.1.3 Interoperabilità a livello di sistema operativo della carta

Questo livello di interoperabilità, come anticipato precedentemente, prevede l'omogeneità dei sistemi operativi delle carte a microcircuito e della struttura del file system. Lo standard internazionale a cui riferirsi è la norma ISO 7816 e nell'ambito di tale norma devono essere fatte le scelte che condizionano il sistema operativo. I principi che devono guidare nella scelta delle funzionalità del sistema operativo, compatibilmente con le esigenze applicative, sono:

- completa conformità con la parte 3 in quanto adottata praticamente da tutti i produttori e indispensabile sia per l'interoperabilità a livello di sistema operativo che a livello di applicazione;
- conformità con la parte 4 almeno per quanto concerne i comandi APDU inerenti la gestione del file system della carta;
- conformità con la parte 8 almeno per quanto concerne i comandi APDU che trattano gli oggetti di sicurezza;
- conformità con la parte 9 almeno per quanto concerne le condizioni di accesso e i comandi APDU per la gestione del ciclo di vita.

Per gestire una situazione di mercato non perfettamente conforme alle esigenze appena esposte è stato insediato un gruppo di lavoro, coordinato dalla allora attiva Autorità per l'informatica nella pubblica amministrazione, composto da tutti i maggiori produttori di sistemi operativi per carte.

Tale tavolo di lavoro ha sviluppato una soluzione tecnica che soddisfa i requisiti imposti e che è stata formalizzata in un protocollo d'intesa tra i fornitori stessi e il Ministero dell'interno e il Ministro per l'innovazione e le tecnologie. Il paragrafo successivo fornisce una serie di dettagli su questo protocollo d'intesa disponibile in appendice.

3.2 Carte "dual interface"

Alcune tipologie di applicazione rendono non consigliabile l'utilizzo di una carta a contatti. Si pensi ad esempio ai servizi di bigliettazione elettronica (e-ticketing) basati sull'uso di carte a microchip. Queste carte richiedono la capacità di eseguire un numero elevato di interazioni nel tempo più breve possibile e secondo modalità che garantiscano una sufficiente durata del supporto costituito dalla carta.

Come si può intuire, l'interfacciamento tra i terminali di accettazione e le carte attraverso i normali contatti elettrici presenta il duplice inconveniente di un alto tempo di transazione, dovuto sostanzialmente anche al tempo necessario per il corretto inserimento della carta nel lettore, e all'usura dei contatti elettrici che porta a conseguenti malfunzionamenti.

Le smartcard, tuttavia, possono anche essere dotate di un'interfaccia a radiofrequenza (si parla in tal caso di tecnologia RFID e di carte "contactless"), che permette il colloquio tra carta e lettore senza alcun contatto fisico, entro una distanza di alcuni centimetri. Il principale standard di riferimento è quello noto come ISO 14443 che prevede l'uso di una segnale radio con frequenza di 13.56 MHz. Il criterio di modulazione del segnale radio può variare secondo due schemi noti rispettivamente come "Tipo A" e "Tipo B".

L'utilizzo di una carta contactless riduce il tempo complessivo di transazione in quanto la carta deve essere semplicemente avvicinata al terminale; la transazione può inoltre essere effettuata anche senza estrarre la carta da un portafoglio o da un'apposita custodia. Anche l'usura si riduce ai minimi termini, per evidenti ragioni.

Dal punto di vista della fabbricazione, la plastica di una carta contactless contiene un'antenna necessaria per catturare l'energia del campo elettromagnetico emesso dal terminale (energia che serve anzitutto per alimentare il microprocessore) nonché per scambiare dati col terminale.

Le specifiche tecniche della Carta Nazionale dei Servizi prevedono come obbligatoria l'interfaccia a contatti, nel rispetto dello standard ISO 7816-3, ma non escludono che la CNS sia anche dotata di un'interfaccia contactless. Le carte dotate di entrambe le interfacce (a contatti e contactless) sono chiamate "dual interface".

Si noti che una carta dual interface è sostanzialmente diversa da una carta "ibrida", dove con questo termine si intende una normale carta a contatti il cui supporto plastico contiene anche un "transponder" separato. Solo nel caso di una carta dual interface è possibile interagire coi medesimi dati previsti dalle specifiche CNS (chiavi crittografiche, certificati, dati anagrafici, servizi aggiuntivi, ecc) anche in modalità RFID.

Una CNS di tipo dual interface è evidentemente più versatile di una CNS dotata dei soli contatti elettrici, perché ne consente l'uso anche in applicazioni di bigliettazione elettronica e in ogni altro contesto caratterizzato da esigenze analoghe (per es. rilevazione presenze in azienda, accesso a parcheggi, mense, etc).

3.3 La piattaforma JAVACARD

Una carta CNS deve ovviamente rispettare le specifiche tecniche definite a livello normativo e pubblicate sul sito internet del CNIPA. Queste specifiche non pongono restrizioni sulle caratteristiche del sistema operativo (purché siano garantite le funzionalità delle APDU), quindi la carta può essere dotata di un sistema operativo "nativo" oppure di un sistema JavaCard (Java Card Technology, <http://java.sun.com/products/javacard/>, Sun Microsystems).

A parità di altre condizioni, l'utilizzo di una carta con tecnologia Javacard offre alcuni vantaggi:

- un supporto multi-applicazione nel senso più pieno del termine: la carta può contenere molteplici applicazioni che rispondono ciascuna ai propri comandi (che possono anche essere proprietari, secondo le esigenze dell'applicazione); applicazioni aggiuntive possono essere installate in modo sicuro sulla carta anche dopo l'emissione;
- la portabilità delle applicazioni sulle carte Javacard di molti differenti produttori (vedere il sito <http://www.javacardforum.org/>) e dunque anche la possibilità di installare sulla carta applicazioni già pronte (es. applicazioni di pagamento in standard EMV, borsellini elettronici, schemi di loyalty, ecc);
- una maggiore economicità e semplicità nello sviluppo delle applicazioni (applet); poiché un'applet è scritta in linguaggio Java, lo sviluppo può essere realizzato in modo autonomo

dall'Amministrazione emittente, senza necessità di coinvolgimento del produttore della carta, utilizzando strumenti standard di sviluppo software.

Una CNS realizzata con tecnologia Javacard offre dunque più “gradi di libertà” alle Amministrazioni. Per contro, dato che un'applicazione Java tende ad occupare più memoria sul microchip rispetto a quanto richiesto da una carta “nativa”, una Javacard deve avere una maggiore capacità di memoria e quindi un prezzo tendenzialmente maggiore di quello di una carta nativa.

Non bisogna dimenticare che bisogna applicare i requisiti di sicurezza che si applicano a tutte le CNS. Pertanto, anche una carta CNS basata su tecnologia Javacard dev'essere sottoposta alla certificazione di sicurezza secondo i criteri indicati dalla normativa sulla firma digitale.

3.4 Il protocollo d'intesa 13 maggio 2003

Essendo passati 36 mesi dalla sottoscrizione del protocollo d'intesa, questo è scaduto alla data di pubblicazione del presente documento. Ma nonostante ciò la sua importanza è stata cruciale per garantire un modello di riferimento nell'ambito dell'interoperabilità delle smart card. Per tali motivi viene lasciato pressoché inalterato, rispetto alle versioni precedenti, il presente paragrafo e di conseguenza il testo del protocollo d'intesa in allegato.

L'appena citata scadenza del Protocollo d'intesa rende necessario una nuova tipologia di aggregazione tra gli enti governativi di riferimento e i produttori di smart card. Sono in fase di studio alcune ipotesi tra le quali quella della costituzione di un tavolo permanente di concertazione tecnica sotto la probabile presidenza del Ministero dell'Interno e il coordinamento tecnico del CNIPA.

Nell'ambito della diffusione degli strumenti d'accesso ai servizi in rete sia di tipo CIE che di tipo CNS si deve garantire la totale e completa interoperabilità delle carte utilizzate su tutto il territorio nazionale. L'interoperabilità è condizione primaria per la diffusione del modello CIE/CNS e dei servizi erogabili ai cittadini, garantendo nello stesso tempo il contenimento dei costi per le pubbliche amministrazioni nel progettare l'infrastruttura di accesso ai servizi. Alla base dell'interoperabilità è il processo di standardizzazione del microprocessore presente sulla smart card, che è previsto essere dello stesso tipo e con analoghe funzionalità sia per la CIE, che per la CNS. A tal fine si è definito uno standard “aperto” che consenta a tutti i produttori di carte di poter fornire microchip conformi ai requisiti previsti.

Come già detto, un apposito gruppo di lavoro ha elaborato, con i produttori di microchip e le pubbliche amministrazioni direttamente interessate al progetto, specifiche comuni e standard che il microprocessore deve possedere. E' necessario ricordare che, allo stato attuale, gli standard internazionali non garantiscono funzionalità di interoperabilità dei microprocessori per quanto riguarda proprio le funzioni di sicurezza nell'accesso ai servizi in rete.

Il gruppo di lavoro ha concluso le sue attività alla fine di gennaio 2003 e il documento finale, accluso in allegato al protocollo di intesa, è stato accettato da tutte le aziende.

Tale documento aggiornato recentemente alla versione 1.1.3 per renderne più chiare alcune parti e eliminare dei refusi è stato considerato anche la base tecnologica per le specifiche tecniche del microchip della CIE.

Ovviamente questo accordo ha costituito un passo fondamentale per l'attuazione dell'e-government, paragonabile alla definizione degli standard GSM per la telefonia mobile o EMV per la carte bancarie di debito e credito. Va ulteriormente ricordato che tale accordo costituisce un'assoluta novità a livello internazionale che può essere proposta in sede comunitaria quale possibile standard da adottare nei progetti e-Europe.

Tra gli elementi fondamentali del protocollo d'intesa è bene mettere in evidenza che i produttori di microchip si impegnano reciprocamente a garantire lo standard tecnologico definito nel progetto

CIE/CNS (art. 2 e art. 4) e a consultarsi periodicamente per la definizione e approvazione di eventuali variazioni indotte dallo sviluppo tecnologico (art. 3).

Una copia del protocollo d'intesa è allegata al presente documento. Le specifiche tecniche contenute nel protocollo sono disponibili sul sito del Centro nazionale per l'informatica nella pubblica amministrazione.

Hanno aderito successivamente al protocollo d'intesa le società:

GEP S.p.A. via Ferrante Imparato, 190 80146 Napoli (in data 20/09/2004);

EPS Engineering And Professional Services Incorporated, Via C. Fracassini, 25 00196 (in data 08/11/2004).

La società Schlumberger ha comunicato in data 09/12/2004 di aver cambiato la denominazione sociale in AXALTO SA.

La società CardNet Group S.p.A. ha comunicato in data 21/02/2005 di aver cambiato denominazione sociale in Kaitech S.p.A.

La società Ghirlanda S.p.A. ha comunicato in data 05/08/2005 di essersi trasformata in Ghirlanda Smart Card Solutions S.p.A. (dopo una scissione parziale delle attività in Ghirlanda Smart card Solutions S.r.l.).

Capitolo 4

L'identificazione e l'autenticazione in rete

L'identificazione è il processo con cui l'utente si dichiara a un sistema o a un'applicazione, l'autenticazione è il processo che consente al sistema o all'applicazione di accertare l'identità dell'utente. I metodi convenzionali sono basati sull'utilizzo della coppia "Username" e "Password", dove il primo elemento è fornito dall'utente per farsi riconoscere ed il secondo elemento viene fornito, sempre dall'utente, come prova di identità. Facendo un paragone con le tecniche moderne che fanno uso di infrastrutture a chiave pubblica e di dispositivi sicuri come le smart card si può sostenere che:

- lo "Username" è sostituito da un certificato digitale;
- la "Password" è sostituita da un crittogramma prodotto per mezzo della chiave privata di autenticazione contenuta nella smart card.

Nei paragrafi successivi vengono descritti in dettaglio i processi di autenticazione basati sull'utilizzo di smart card e di infrastrutture a chiave pubblica (PKI).

4.1 I processi di identificazione e autenticazione

Prima di affrontare il dettaglio dei processi di Identificazione/Autenticazione, che sfruttano la tecnologia PKI, è opportuno considerare le modalità con cui l'utente interagisce con le applicazioni, ovvero se opera in modalità WEB/Browsing oppure Client/Server.

Nel primo caso esiste la possibilità di utilizzare il protocollo TLS/SSL che è uno standard in ambito Internet, mentre nel secondo caso ci si deve riferire a procedure, chiamate Challenge/Response (CH/R), che definiscono il processo di autenticazione dal punto di vista funzionale, per le quali non esistono prodotti standard ma solo realizzazioni di tipo proprietario strettamente integrate con l'applicazione per cui sono state scritte e quindi difficilmente riusabili.

I successivi paragrafi tratteranno dettagliatamente questi aspetti. In particolare un capitolo sarà dedicato all'ambiente software sul client e un altro all'ambiente di accesso sul server.

4.1.1 Mutua autenticazione tramite il protocollo SSL/TLS

Il protocollo SSL/TLS è garantito da una libreria di programmi che consentono di stabilire un canale di comunicazione tra Browser e WEB Server che può garantire:

- riservatezza del contenuto dei messaggi;
- integrità dei messaggi;
- mutua autenticazione delle parti coinvolte.

Tali caratteristiche vengono ottenute con i seguenti procedimenti:

- per la riservatezza ed integrità dei messaggi:

- il protocollo che prevede l'autenticazione tra server e client, può basarsi su diversi meccanismi (RSA, Fortezza, alcune versioni dell'algoritmo di Diffie-Hellman);
- dopo l'iniziale fase di negoziazione della chiave di sessione, tutti i dati trasmessi sono crittografati, la crittografia è di tipo simmetrico;
- la connessione garantisce l'integrità dei messaggi utilizzando funzioni di hash .

- Per l'autenticazione delle parti:

SSL/TLS prevede l'uso di certificati digitali del tipo X509v3 e di coppie di chiavi asimmetriche utilizzate sia dal web server che dal browser e quindi si presta ad essere utilizzato con smart card crittografiche quali la Carta Nazionale dei Servizi (CNS) e la Carta di Identità Elettronica (CIE).

Il grosso vantaggio offerto da SSL/TLS risiede nel fatto che web browser e web server sono già predisposti per utilizzare tale protocollo e quindi qualunque applicazione WEB può sfruttare le caratteristiche di sicurezza sopra esposte. Occorre solo configurare opportunamente le opzioni di sicurezza del browser e del web server. Nei successivi paragrafi saranno fornite le caratteristiche dei certificati X509v3 adatti al protocollo SSL/TLS.

L'applicazione web, dopo la fase di autenticazione, può procedere a successive fasi di autorizzazione all'accesso ai servizi in funzione degli specifici diritti e privilegi dell'utente. Per fare ciò ha la necessità di riconoscere l'utente estraendo lo "Username" e eventualmente altre informazioni dal certificato.

4.2 L'autenticazione del server

Nello scenario dell'erogazione dei servizi in rete il cittadino deve essere tutelato che chi sta erogando il servizio richiesto sia proprio la pubblica amministrazione competente e responsabile del servizio da erogare. Ciò significa che ogni server della pubblica amministrazione abilitato ad erogare un servizio deve possedere un certificato identificativo.

A tale esigenza organizzativa bisogna aggiungere che sono proprio i meccanismi SSL ad avere bisogno che sul web server sia necessariamente installato un certificato identificativo.

Esistono tre possibilità:

- i siti vengono autenticati da una struttura governativa (Es. SSCE);
- i siti vengono autenticati dai certificatori di firma digitale;
- i siti vengono autenticati da soggetti autorizzati generici.

Nel primo caso va definita e costruita una struttura ad hoc presso un qualche settore governativo; inoltre c'è il rischio che la centralità di questo servizio possa creare problemi di competenza con gli enti locali.

Nel secondo caso si deve garantire un livello di fiducia adeguato dei certificati che queste strutture utilizzano per la loro attività. Il modello che appare adeguato, perché poco invasivo e già sperimentato per la firma digitale, è quello dell'elenco pubblico dei certificatori di autenticazione".

La catena di fiducia rimane sotto il controllo centrale (è indispensabile per garantire integrità ed autenticità dell'elenco stesso) mediante la firma digitale di tale elenco, che può essere effettuata dal Ministero dell'Interno.

Lo stesso vale per la terza ipotesi, anche se in questo caso bisognerebbe discriminare sui servizi offerti. L'autenticazione dei siti non dovrebbe essere effettuata da un soggetto generico se sono offerti servizi di pagamento o comunque servizi ad elevato rischio informatico dal punto di vista dell'analisi del rischio effettuata.

Esistono soluzioni alternative ma come variazione di dettaglio di quelle presentate.

Deve essere risolto il problema delle liste di revoca. Se operano i certificatori, non è efficiente far gestire ai web server le oltre dieci CRL/CSL necessarie. E' invece sicuramente opportuno utilizzare un server, ad esempio di tipo OCSP, che garantisce informazioni applicative sullo stato della revoca e si alimenta per proprio conto con i dati dei certificatori.

Anche in questo esistono soluzioni analoghe ma comunque basate su un server (logicamente) centrale.

4.2.1 Configurazione del client Internet Explorer

Se si dispone della CNS (o della CIE), il client potrà utilizzare la coppia di chiavi contenute nella carta a microprocessore con le modalità che saranno illustrate di seguito⁽¹⁰⁾.

Nel sistema operativo Windows, le funzioni di crittografia sono gestite dal modulo CSP (Cryptographic Service Provider). Quando le chiavi di cifratura sono memorizzate su smart card, il CSP deve essere in grado di interagire con quest'ultima.

Sul sito del CNIPA sono descritte le modalità mediante le quali, quest'ultimo rende disponibile il software di supporto all'uso della CNS da parte dei cittadini e delle amministrazioni.

Con questa soluzione il browser Explorer può utilizzare le funzioni di sicurezza della CNS in modalità nativa.

Sullo stesso sito è anche riportato il manuale utente per l'attivazione della protezione SSL (CIE_CSP Guida Utente)⁽¹¹⁾.

4.2.2 Configurazione di browser open source (Netscape, Mozilla, ecc.)

I browser Netscape e Mozilla non utilizzano le funzioni del CSP ma interagiscono con le librerie della smart card in modalità PKCS #11.

Anche in questo caso sul sito del CNIPA sono descritte le modalità mediante le quali, quest'ultimo rende disponibile il software di supporto all'uso della CNS da parte dei cittadini e delle amministrazioni.

4.2.3 Configurazione del server

Il responsabile dell'erogazione del servizio dovrà invece provvedere alla generazione di una coppia di chiavi sul web server, nonché alla pubblicazione della chiave pubblica utilizzando un certificato for-

¹⁰ Per queste funzioni viene utilizzata la coppia di chiavi, presente sulla smart card, che identifica univocamente la CNS o CIE. Le operazioni crittografiche avvengono all'interno della smart card, in modo che la chiave segreta non possa essere in alcun modo estratta.

¹¹ Le modalità operative per l'installazione e l'utilizzo delle funzioni SSL/TLS dipendono anche dalle caratteristiche del browser e quindi possono variare in funzione della versione utilizzata. Sulla documentazione pubblicata nel sito è riportata la modalità operativa relativa alla versione più recente.

mato X.509 v.3⁽¹²⁾. Dovrà inoltre provvedere ad inserire il certificato utente, reperibile dalla CNS, nell'elenco dei certificati abilitati ad usufruire del servizio.

Il web server dovrà infine essere configurato in modo da gestire la lista dei certificati revocati (CRL)⁽¹³⁾.

4.2.4 Installazione del certificato del server

Indipendentemente dal browser utilizzato è necessario che sullo stesso sia presente il certificato che contiene la chiave pubblica del server. Ciò può ottenersi nei seguenti modi:

- il certificato viene preinstallato sul browser (ad esempio con un opportuno kit di installazione);
- il certificato viene scaricato ed installato sul browser al momento del primo utilizzo della funzione protetta (in tal caso uno specifico messaggio chiederà all'utente se intende installare ed utilizzare il certificato);
- il certificato del server è firmato da una certification authority il cui certificato è presente per default sul browser, in tal caso non è necessaria alcuna installazione.

Ovviamente l'ultima soluzione è quella più semplice sotto l'aspetto operativo, ma richiede che si utilizzino i servizi di una certification authority appartenente ad una ristretta rosa di società i cui certificati sono inseriti «all'origine» nei browser.

4.3 Personalizzazione delle funzioni di sicurezza

La soluzione esposta ha il vantaggio di non richiedere la scrittura di software aggiuntivo, ma presenta le seguenti limitazioni:

- è adatta solo ad applicazioni di tipo web (ad esempio non è utilizzabile per applicazioni client server tradizionali);
- non permette di realizzare funzioni di sicurezza diverse da quelle standard SSL/TLS;
- le modalità operative sono rigidamente condizionate dai prodotti browser e web server utilizzati.

In tutti quei casi in cui tali limitazioni non sono accettabili, è possibile utilizzare funzioni di sicurezza «ad hoc».

In generale sono possibili due strade:

- l'impiego di funzioni di sicurezza proprie dell'ambiente client Windows (ad esempio le funzioni del CIE_CSP utilizzabili con le CryptoApi o l'interfaccia standard PKCS#11);
- l'interazione con il middleware che gestisce la smart card attraverso i Metacomandi.

¹² Ciò può essere fatto sfruttando le caratteristiche del web server oppure ricorrendo ai servizi di un certificatore. Nel caso di ricorso a certificati acquisiti da terzi, è necessario che gli stessi consentano la crittografia simmetrica con chiavi lunghe 128 bit.

¹³ La verifica della validità del certificato mediante accesso alla CRL è gestita in modo differente dai web server.

Tra le due possibilità deve essere preferita la seconda, in quanto consente l'interazione con l'ambiente di sicurezza attraverso una modalità standard indipendente dallo specifico ambiente software.

Utilizzando i Metacomandi è infatti possibile combinare le funzioni di sicurezza in modo semplice ed integrato con le altre funzioni applicative. In ogni caso tali funzioni applicative devono essere sviluppate secondo il modello di autenticazione Challenge/Response (CH/R).

4.4 Autenticazione in modalità Challenge/Response(CH/R)

Questa modalità di autenticazione consente di accertare l'identità dell'utente tramite un processo relativamente semplice, che non ha impatti di tipo computazionale sia sul client che sul server erogatore del servizio, ma deve essere appositamente sviluppata in conformità con l'ambiente operativo sia del client che del server.

Il processo di autenticazione in modalità CH/R segue i seguenti passi funzionali:

- dopo una fase iniziale di identificazione, eseguita verificando il certificato dell'utente, il server produce un messaggio di autenticazione (Challenge), in generale diversificato da un numero pseudocasuale per evitarne possibili riutilizzi, e lo invia al client;
- il client, tramite la chiave privata dell'utente, effettua un'operazione di "signature" del Challenge producendo il Response che rinvia al server;
- il server, per mezzo della chiave pubblica contenuta nel certificato dell'utente ne accerta l'identità verificando l'autenticità del Response.

Dopo la fase di autenticazione il server può procedere a successive fasi di autorizzazione all'accesso ai servizi in funzione degli specifici diritti e privilegi dell'utente.

La coppia di chiavi ed il certificato di autenticazione specifici per il protocollo SSL/TLS possono essere utilizzati anche per i processi di autenticazione in modalità CH/R.

Il processo di autenticazione in modalità CH/R, da un punto di vista strettamente tecnico, può essere effettuato tramite la coppia di chiavi e il certificato destinati alla Firma Digitale, ma è doveroso osservare che ciò è espressamente vietato dalle norme che disciplinano la Firma Digitale in ambito Nazionale ed Europeo per pericolosi rischi che questa pratica comporta.

Bisogna considerare che la firma digitale è un processo che un utente attiva su un documento elettronico a lui noto, che intende firmare digitalmente e che è conscio di non poter ripudiare. A discrezione dell'utente, questo processo può essere effettuato anche in modalità stand alone.

Il processo di autenticazione CH/R è strettamente on line e induce l'utente a firmare un messaggio che è, in generale, non visibile e prodotto nell'ambito stesso del processo di autenticazione.

È possibile utilizzare l'autenticazione CH/R anche utilizzando un browser. In questo caso su di esso, in base al tipo di browser, deve essere caricato un "Plugin", un'Applet oppure un ActiveX al fine di attivare la componente client del processo.

Capitolo 5

I Certificati digitali

I processi di autenticazione descritti nei precedenti paragrafi fanno uso di tecniche PKI e quindi impiegano chiavi asimmetriche e certificati digitali. Queste quantità di sicurezza non sono utilizzate solamente per l'autenticazione in rete, ma anche per l'apposizione di firme digitali e per la produzione di buste crittografiche. Per questa ragione, nel seguito, saranno esaminate le caratteristiche dei certificati digitali e il formato dei dati da sottoporre sia ai processi di autenticazione che alle operazioni di firma digitale e crittografia.

5.1 Certificati e formati per la Firma Digitale

In accordo con quanto previsto dalla normativa vigente, il certificato di firma digitale per l'utilizzo di una smart card (come strumento di *sottoscrizione* di documenti elettronici) deve essere conforme allo standard RFC 2459 "Internet X.509 Public Key Infrastructure Certificate and CRL Profile" (alla data sostituito da RFC 3280) e contenere almeno le seguenti informazioni:

- numero di serie del certificato di sottoscrizione;
- ragione o denominazione sociale del certificatore;
- codice identificativo del titolare presso il certificatore (campo **subject** del certificato = **common name + description**);
- nome cognome e data di nascita del titolare;
- valore della chiave pubblica;
- tipo di algoritmi di generazione e verifica della sottoscrizione del titolare;
- inizio e fine del periodo di validità della coppia di chiavi;
- tipo di algoritmo di sottoscrizione utilizzato dal certificatore;
- eventuali limitazioni nell'uso della coppia di chiavi.

In particolare il **common name**, (object ID = 2.5.4.3), ha la seguente struttura:

<cognome>/<nome>/<codice fiscale>/<identificativo titolare presso il certificatore>.

Il campo **description** (object ID = 2.5.4.13), ha la seguente struttura:

"C="<cognome esteso>"/N="<nome esteso>"/D="<data di nascita>["/R="<ruolo titolare>]

Le estensioni necessariamente presenti nei certificati e quindi, secondo la specifica pubblica RFC 3280, sono:

- Authority Key Identifier: identifica la chiave pubblica corrispondente alla chiave privata utilizzata dal Certificatore per sottoscrivere il certificato;
- Subject Key Identifier: identifica certificati che contengono una particolare chiave pubblica;
- Key usage (estensione critica): indica l'uso delle chiavi (**non repudiation**);
- Certificate Policies: specifica la policy di riferimento del certificato ed il sito di distribuzione del manuale operativo;
- CrlDistributionPoint: contiene l'indirizzo che indica dove reperire la Certificate Revocation List che eventualmente conterrà le informazioni di revoca relative al certificato.

Questi certificati devono essere utilizzati per verificare la firma di documenti prodotti con la chiave privata a cui fanno riferimento. Il tentativo di usarli in un browser con il protocollo di mutua autenticazione SSL/TLS produrrebbe il rifiuto del certificato da parte del browser, causato dal **Key Usage** che, essendo una estensione critica, è obbligatoriamente verificata.

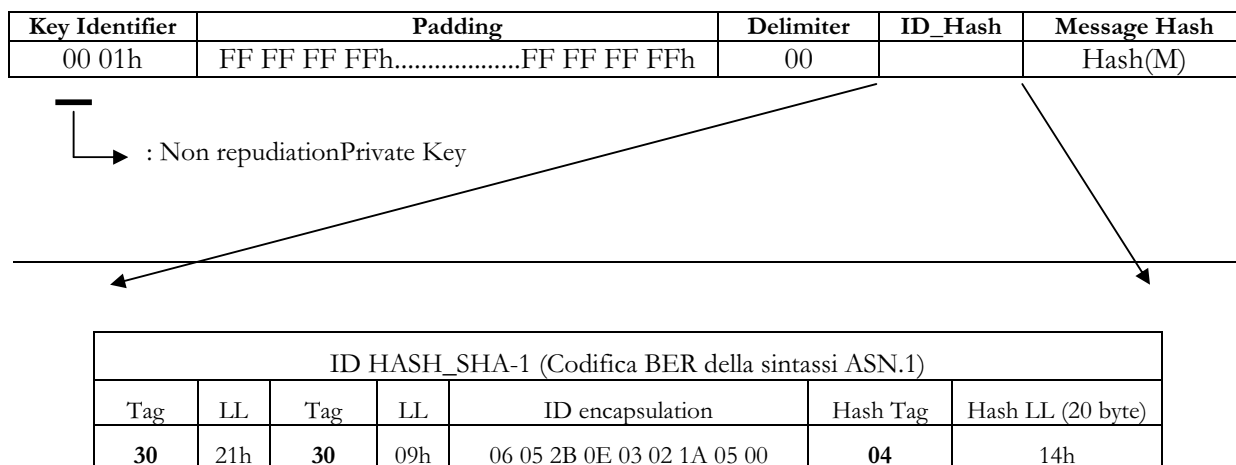
Il formato dei dati e le buste crittografiche utilizzate per la firma digitale fanno riferimento ai seguenti standard:

- PKCS#1 (RSA Laboratories - RSA Cryptography Standard);
- PKCS#7 (RFC 2315).

PKCS#1 è lo standard di riferimento per la crittografia a chiave pubblica applicata, fra gli altri, alla Firma Digitale di documenti elettronici e per i processi di autenticazione e crittografia in rete Internet.

PKCS#7 è lo standard di riferimento per le buste crittografiche create per contenere la firma e il documento al quale si riferisce.

Dato un messaggio "M", la componente che deve essere firmata digitalmente è l'impronta di "M" ed il formato dei dati da sottoporre al processo di firma secondo lo standard PKCS#1 è rappresentato nella figura seguente:



Le smart card conformi allo standard ISO 7816-8/9 (vedere paragrafo relativo agli standard di interoperabilità tra le carte) ammettono il formato PKCS#1 e, nei confronti delle operazioni di Digital Signature, si comportano nel seguente modo:

- controllano che l'oggetto chiave privata sia identificabile come chiave di firma digitale e non come chiave di autenticazione o di crittografia;
- se la precedente condizione è verificata forzano automaticamente il formato dei dati di firma secondo lo standard PKCS#1 descritto nella figura precedente.

Se si tentasse di utilizzare una chiave di autenticazione o di "encryption" con un comando di Signatura la smart card restituirebbe un codice di errore.

5.2 Certificati di autenticazione e crittografia

Sono di seguito rappresentate le caratteristiche salienti dei certificati di autenticazione e crittografia secondo lo standard X509v3, soprattutto per ciò che concerne le differenze con i certificati per la firma digitale. Le differenze salienti, cioè quelle che ne vincolano l'utilizzo, sono contenute nelle estensioni ed in particolare nel **Key Usage** e nello **Extended Key Usage**.

Sono previste dallo standard X509v3 le seguenti estensioni:

- **Key Usage** (critica) ::= Authentication, Encryption, Signature;
- **Extended Key Usage** ::= Client Authentication, Secure e-mail (non previste nel certificato di firma digitale);

Le precedenti estensioni consentono di utilizzare il certificato e la coppia di chiavi a cui esso si riferisce, nei seguenti ambienti:

- Browser WEB per l'autenticazione tramite il protocollo SSLv3;
- User Agent di posta elettronica per la produzione di e-mail cifrate e firmate elettronicamente secondo il formato standard S/MIME.

La componente Signature del **Key Usage** non è riferita alla Firma Digitale ma alla firma elettronica del formato S/MIME 2.

Ricordiamo infatti che il **Key Usage** per la firma digitale è : **non repudiation**.

La Carta di Identità Elettronica e Carta Nazionale dei Servizi usano, per i processi di autenticazione in rete, un certificato con le caratteristiche sopra descritte. Il profilo dettagliato, facente parte delle regole tecniche descritte nel capitolo 2 viene riportato in appendice.

5.3 Processo di attestazione

Nell'ambito del progetto CRS LOMBARDIA- SISS della Regione Lombardia la carta specifica del progetto è anche utilizzata per attestare la presenza del cittadino durante l'erogazione di un servizio sanitario. Per Attestazione si intende la firma elettronica di un documento effettuata con la chiave privata e certificato di autenticazione a bordo della carta del cittadino.

L'attestazione non ha di per sé valore legale ma è considerata valida solo nell'ambito del progetto CRS LOMBARDIA-SISS e per i fini sopra detti.

Capitolo 6

Le applicazioni sanitarie della carta

L'installazione facoltativa della componente sanitaria (Netlink) sulla CNS avviene in due fasi distinte:

- inizializzazione della CNS a cura dei produttori;
- formazione della CNS e caricamento dei dati sanitari.

Nella prima fase i produttori, delegati dall'Ente emittitore, predispongono le strutture dati sanitarie (secondo le specifiche Netlink), compilano i file elementari che non contengono dati specifici del cittadino e caricano le quantità di sicurezza derivate dalle chiavi di gruppo fornite dal Ministero della Salute.

I produttori devono garantire la segretezza delle chiavi di gruppo, conservandole in dispositivi che ne consentano l'utilizzo al solo fine di inizializzare le carte, ma ne impediscano la lettura o l'esportazione dei dati contenuti. L'Ente emittitore renderà disponibili, in modo sicuro, le chiavi di gruppo previa autorizzazione del Ministero della Salute.

Per la gestione della seconda fase (personalizzazione e caricamento dei dati sanitari), le Regioni possono costituire Centri Servizi Regionali omologati per il territorio di competenza.

La realizzazione della seconda fase può avvenire secondo le modalità che sono di seguito brevemente descritte e che possono essere liberamente scelte dagli enti emittitori:

- si utilizza un Centro Servizi Regionale il quale, per gli Enti emittitori che effettuano questa scelta, effettua la fase di formazione della CNS, l'installazione dei dati sanitari ed eventualmente il rilascio;
- gli Enti emittitori gestiscono autonomamente la formazione della CNS oppure si avvalgono di un Centro Servizi diverso da quello Regionale; in questo caso durante la fase di formazione sono installati i dati sanitari tramite collegamento con le ASL con cui gli Enti Emittitori avranno stabilito una opportuna convenzione;
- gli Enti emittitori gestiscono autonomamente la formazione della CNS oppure si avvalgono di un Centro Servizi diverso da quello Regionale e, dopo la fase di formazione e prima del rilascio della carta ai cittadini, inviano i lotti di CNS al Centro Servizi Regionale affinché possano essere caricati i dati sanitari;
- gli Enti emittitori gestiscono autonomamente la formazione della CNS predisponendo le strutture dati secondo quanto specificato in questo paragrafo e la rilasciano senza dati sanitari; i cittadini si recano presso gli sportelli delle amministrazioni competenti con cui l'ente emittitore avrà preventivamente stabilito accordi.

6.1 Il modello di sanità basato sulla Carta Sanitaria.

Nell'ambito dei vari progetti di e-government, che vengono sperimentati a livello nazionale, regionale e locale, è particolarmente interessante, per numero di attori coinvolti e per ampiezza del progetto, quello del Sistema Informativo Socio-Sanitario (CRS-SISS) in Lombardia.

Nel corso del 2001 è stata progettata e sperimentata con successo in provincia di Lecco, una carta dal formato e aspetto simile a un bancomat, con cui è possibile accedere, per via telematica, ai servizi integrati in Rete a livello regionale, con paradigmi e modelli mutuati dalla tecnologia web. La sperimentazione della Carta in provincia di Lecco ha coinvolto 306.000 cittadini, 1.500 operatori sanitari, 275 medici di base e pediatri e 88 farmacie. Nel corso della sperimentazione oltre il 35% delle prescrizioni di farmaci, visite ambulatoriali e richieste di ricoveri –con punte del 52% per le prescrizioni di farmaci- avviene con l'uso della Carta.

Inizialmente il Progetto supporta servizi in ambito socio-sanitario, ma prevede già da ora l'analisi delle modalità di coinvolgimenti di altri settori della pubblica amministrazione.

Il 15 marzo del 2002 la Regione Lombardia ha deliberato l'estensione del progetto CRS-SISS su tutto il territorio regionale. In questo ambito è prevista entro la metà del 2006 la diffusione della carta in tutta la Lombardia (9.000.000 cittadini, 100.000 operatori sanitari, 8500 medici di base e pediatri, 2500 farmacie e 15 Aziende Sanitarie Locali).

La sottoscrizione di un protocollo d'intesa tra il Ministro per l'innovazione e le tecnologie e il Governatore della Regione Lombardia in data 12 novembre 2002 ha, tra l'altro, determinato la convergenza del progetto CRS-SISS con gli obiettivi della CNS.

Alla fine di marzo 2005 è stata completata la distribuzione delle 9.255.000 smart card previste.

Altre regioni stanno utilizzando questo modello di Carta Sanitaria basato sulle specifiche Netlink.

6.2 Le specifiche Netlink

Il progetto Netlink ha rappresentato il pilota europeo di un modo innovativo di fare sanità nella gestione del rapporto paziente, operatore sanitario e, specificamente, il medico di base. I suoi meccanismi applicativi garantiscono un efficace controllo e gestione dell'offerta e della fruizione dei servizi socio-sanitari.

Le specifiche di Netlink sono pubbliche e si basano su principi di sicurezza che utilizzano mutua autenticazione tra due soggetti mediante meccanismi di crittografia simmetrica. Vista la struttura applicativa prevista la mutua autenticazione è tra il paziente e l'operatore sanitario rispetto al sistema informativo socio-sanitario con una elevata quantità di sicurezza anche nei confronti di quanto previsto dalla normativa vigente sulla privacy.

Sempre in quest'ottica e nell'ambito delle specifiche Netlink (tracciato record definito) la carta contiene una serie di informazioni sanitarie che consentono di gestire in modo più mirato le prestazioni sanitarie mediante la maggiore integrazione tra i diversi attori del processo di diagnosi, cura, riabilitazione e assistenza.

Ovviamente la tipologia dello strumento garantisce anche un più efficace controllo della spesa e costituisce la base per l'uso marginale di documenti cartacei.

Non è obiettivo del presente documento dare il dettaglio delle specifiche operative Netlink, ma è opportuno ricordare che i processi di gestione socio-sanitari basati su queste specifiche sono complessi e basati su un sistema informativo già pronto e rodato a prescindere dall'utilizzo dalla carta.

Il progetto CNS, peraltro, consente di predisporre gli spazi all'interno della smart card e di attivarli al momento opportuno, cioè quando le strutture informatiche di supporto sono popolate con un numero di dati sufficiente e funzionale agli obiettivi di efficacia e efficienza di questo tipo di progetti.

In ogni caso la struttura interna della carta conforme alle specifiche Netlink viene resa disponibile nell'ambito della pubblicazione delle specifiche del file system "multiservizi" previsto per la CNS.

Capitolo 7

La firma digitale

La firma digitale è stato il primo strumento introdotto per la semplificazione dei processi amministrativi.

Il compito di questo strumento è di consentire la stipula di atti basati su processi informatici, fornendo evidenza e prova della sottoscrizione, da parte del firmatario, degli atti, fatti o dati che il documento firmato rappresenta.

La firma digitale è dunque soprattutto uno strumento amministrativo, ma è anche in grado di assicurare l'integrità del documento firmato, infatti protegge il documento da contraffazioni anche se quest'ultimo viene conservato in un ambiente non sicuro.

La firma digitale è dunque uno strumento chiave dei processi di e-government e trova proficua applicazione in tutti i casi in cui il servizio comporta un atto amministrativo.¹⁴

E' evidente come l'integrazione di questo strumento nella CNS consenta al titolare di disporre di uno strumento utile non solo per identificarsi ed autenticarsi in rete, accedendo quindi ai servizi in rete, ma per sottoscrivere, con pieno valore legale, una propria volontà, una dichiarazione, un'istanza.

7.1 La firma digitale nella CNS

La CNS deve essere predisposta per accogliere le funzionalità di firma digitale. E' quindi indispensabile che la smart card utilizzata rispetti le norme relative al cosiddetto "dispositivo sicuro per la generazione delle firme" ed in particolare le caratteristiche previste dall'allegato III della Direttiva europea 1999/93/CE. Tali caratteristiche possono essere dimostrate come previsto dalla "Decisione della Commissione europea del 14 luglio 2003" (Gazzetta ufficiale dell'Unione europea n. L175/45 del 154 luglio 2003): valutazione EAL 4+ della norma ISO/IEC 15408 secondo le modalità previste nel CWA 14169 (marzo 2002). Sono ammessi livelli di valutazione internazionalmente riconosciuti come equivalenti.

La predisposizione della firma digitale può avvenire con due diverse modalità:

- a) il soggetto responsabile della certificazione delle chiavi di firma è stabilito dall'ente emittitore, nell'ambito dei soggetti accreditati ai sensi dell'articolo 29 del decreto legislativo 4 aprile 2006, n. 159;
- b) il titolare della CNS può scegliere il Certificatore responsabile dell'erogazione dei servizi suddetti tra quelli accreditati o notificati secondo la normativa vigente.

¹⁴ Tratto dal documento "L'e-government per un federalismo efficiente". Documento elaborato dal Comitato Tecnico della Commissione permanente per l'Innovazione e le Tecnologie

Nel primo caso l'ente emittitore predispone una procedura atta a far sì che il titolare della CNS possa disporre della firma digitale al momento del rilascio della carta o in una fase successiva. A tale scopo l'ente emittitore sceglie almeno un soggetto responsabile della certificazione fra quelli iscritti nell'elenco pubblico dei certificatori previsto dall'art. 29, comma 6 del decreto legislativo 4 aprile 2006, n.159.

Nel secondo caso, attuabile solo se l'ente emittitore non predispone la CNS nella modalità di cui al punto a), l'ente emittitore deve consegnare al cittadino, al momento del rilascio della CNS, le modalità operative da utilizzare per la predisposizione della carta quale dispositivo per generare firme digitali. Il titolare della CNS, tramite queste modalità, può successivamente richiedere l'installazione delle componenti inerenti l'utilizzo della firma digitale rivolgendosi ad uno dei certificatori accreditati secondo la normativa vigente. Sono ammessi metodi alternativi a quello appena indicato, con l'unico vincolo che questo metodo sia tale da non modificare la certificazione di sicurezza della smart card ai fini del dispositivo sicuro per la creazione della firma.

Più in dettaglio, il titolare della CNS, provvisto di un documento di identità e utilizzando le modalità stabilite dall'ente emittitore per l'attivazione del servizio di firma digitale, si mette in contatto con un certificatore che procede ad impostare la smart card in modo che possa essere utilizzata per i processi di firma. Si sottolinea che queste informazioni dedicate all'installazione della firma digitale sono necessarie per attivare i diritti di scrittura sulla directory dedicata a tale servizio.

Nel caso in cui l'ente emittitore attivi delle convenzioni con i certificatori di firma, non si esclude la possibilità che lo stesso ente emittitore svolga le funzioni di "registration authority" per le fasi di identificazione del cittadino.

In entrambi i casi, le procedure di predisposizione della carta, di gestione del certificato di firma digitale e delle relative chiavi, dovranno essere conformi alla normativa vigente in materia di firma digitale.

Capitolo 8

Altre applicazioni nella CNS

Un servizio essenziale nell'ambito dell'offerta di servizi in rete è quello dei sistemi di pagamento in linea. Un elevato numero di transazioni, infatti, si completa con una operazione di pagamento. E' ovvio che una operazione direttamente fruibile all'interno del servizio in rete è più efficace e efficiente nei confronti del fruitore. Nel seguito vengono descritte le modalità prescelte per sperimentare un servizio di pagamenti in linea con l'utilizzo della CNS.

Altri servizi possono essere erogati tramite la CNS su base locale, utilizzando lo spazio libero memoria permanente della CNS (EEPROM). In generale è il fornitore di carte che definisce le modalità del servizio, coordinandosi con la pubblica amministrazione cliente. Il CNIPA, comunque, offre supporto tecnico e organizzativo al fine di garantire la coerenza con il progetto globale e la sicurezza delle scelte effettuate rispetto all'emissione della carta.

8.1 I servizi aggiuntivi

La Carta Nazionale dei servizi può contenere anche i cosiddetti "servizi aggiuntivi". Con tale termine ci si riferisce ai dati memorizzati sulla smart card al fine di consentire l'erogazione di ulteriori servizi applicativi, oltre a quelli già previsti come standard per le carte CNS cioè l'autenticazione, più le opzionali firma digitale e carta sanitaria basata sulle specifiche Netlink.

I servizi aggiuntivi possono essere installati sulla carta al momento dell'emissione oppure essere installati successivamente. In ogni caso, essi vengono installati in un'apposita area della CNS nota come "DF2".

Per installare i servizi aggiuntivi è necessario inviare alla carta opportuni comandi in modalità protetta ("secure messaging"); ciò richiede l'impiego di apposite chiavi crittografiche detenute dall'Amministrazione emittente la CNS. L'Amministrazione può eventualmente delegare la creazione di servizi aggiuntivi ad altri soggetti coi quali abbia rapporti di collaborazione a diverso titolo, purché nel rigoroso rispetto delle specifiche e delle necessarie misure di sicurezza.

Ogni servizio aggiuntivo dev'essere contenuto in una specifica DF ("Dedicated File") all'interno di DF2. Una DF è in pratica una directory nella quale è contenuto l'insieme dei file necessari per un particolare servizio aggiuntivo: può trattarsi di una combinazione di file elementari (EF), oggetti di sicurezza (BSO) e ulteriori DF.

L'insieme degli identificatori (FID) dei servizi aggiuntivi presenti in una carta CNS è mantenuto in un apposito file anch'esso presente in DF2.

L'unica limitazione alla creazione di un servizio aggiuntivo è data dalla disponibilità di memoria residua sulla carta CNS. La memoria residua dipende a sua volta dalla capacità della carta, dallo spazio occupato dalle (eventuali) aree di firma digitale e Netlink e dallo spazio occupato dai servizi aggiuntivi già presenti.

L'allocazione di un identificatore (FID) univoco necessario per poter creare un servizio aggiuntivo in una carta CNS può essere ottenuta inviando una richiesta al CNIPA contenente una descrizione del

servizio che si intende registrare. L'elenco dei servizi registrati è reperibile sul sito del CNIPA alla pagina http://www.cnipa.gov.it/site/it-IT/Attivit%C3%A0/Certificatori_accreditati/Carta_Nazionale_dei_Servizi/Servizi_aggiuntivi/

I servizi aggiuntivi installabili sulla carta CNS possono rispondere alle più diverse esigenze applicative; ecco alcuni esempi significativi:

- rilevazione presenze in azienda,
- pagamenti (secondo vari schemi),
- memorizzazione di informazioni personali,
- bigliettazione elettronica (e-ticketing),
- raccolta e consumo di “punti fedeltà” (loyalty),
- ricarica ed utilizzo di “buoni” (pasto, carburante, ecc).

Ogni servizio può avere differenti requisiti per quanto riguarda le caratteristiche del lettore o terminale di “accettazione”; alcuni servizi potranno essere fruiti da differenti piattaforme (es. il normale PC, il decoder della TV digitale terrestre, terminali POS, ecc).

8.2 I sistemi di pagamento in linea

L'obiettivo principale di questo tipo di progetto è di consentire a cittadini e imprese di usufruire di servizi in rete offerti dalle pubbliche amministrazioni effettuando, anche in modo contestuale, i pagamenti eventualmente necessari.

Un secondo obiettivo è quello di utilizzare la carta CNS per l'identificazione dell'utente nella transazione relativa ai pagamenti in oggetto.

Un terzo obiettivo, non meno importante, è quello di rendere possibile al cittadino fruitore del servizio di utilizzare una gamma di strumenti di pagamento diversificati, largamente diffusi e soprattutto non legati a un singolo emittitore.

Un sistema di pagamento in linea deve obbligatoriamente fare riferimento a un circuito virtuale di pagamento. E' opportuno che tale circuito virtuale sia tale da rendere il cliente indipendente dal possesso di uno specifico strumento di pagamento e dal rapporto con una particolare banca o emittitore di carte di debito o credito.

L'indagine effettuata ha evidenziato che l'unico circuito rispondente ai requisiti indicati sia attualmente il sistema BANKPASS Web.

Tale circuito nasce all'interno dell'e-Committee, costituita da un'associazione di banche, promossa dall'ABI, nata per assumere il ruolo di motore per l'innovazione bancaria nell'ambito dell'ICT.

All'e-Committee oggi aderiscono 240 banche in rappresentanza di oltre il 90% del sistema.

BANKPASS Web è stato lanciato sul mercato il 28 gennaio 2002, nasce con l'obiettivo di rendere sicuri e flessibili gli acquisti in rete e dare impulso al commercio elettronico.

Il sistema si avvale di operatori tecnologici di tipo interbancari come SSB, SECETI e Consorzio Triveneto. Gli utenti aderenti a BANKPASS Web possono utilizzare una varietà di strumenti di pagamento (carte di credito, carte di debito e a breve bonifici).

Per operare gli utenti utilizzano un “portafoglio virtuale” in cui il consumatore può inserire tutti i propri strumenti di pagamento che può utilizzare per effettuare i propri acquisti in linea in totale sicurezza. L'esercente in rete può acquisire pagamenti con tutte le carte di credito (Visa, MasterCard, Amex, Diners, JCB, ecc.) e anche con il PagoBANCOMAT.

Associando alla categoria “esercente” la pubblica amministrazione che eroga il servizio in rete è possibile associare alle operazioni di acquisizione pagamenti il servizio in rete offerto dall'amministrazione stessa.

E' possibile a questo punto, realizzando un'opportuna interfaccia software, far colloquiare il portale di servizi con il circuito virtuale di pagamento.

8.3 La CNS e la televisione digitale terrestre.

Il decoder della Televisione Digitale Terrestre (DTT) rappresenta una piattaforma molto interessante per l'utilizzo della CNS. In tal senso è importante sottolineare che, a differenza dei PC, tutti i decoder interattivi ovvero la maggioranza di quelli presenti presso le famiglie, sono equipaggiati con un lettore di carte.

Il decoder della Televisione Digitale Terrestre (DTT) rappresenta una piattaforma molto interessante per l'utilizzo della CNS. Si noti infatti che, a differenza dei PC, tutti i decoder interattivi (la maggioranza) sono equipaggiati con un lettore di carte.

Il lettore di carte del decoder è stato inizialmente previsto per la fruizione delle trasmissioni TV a pagamento (Pay-TV), mediante l'inserimento di una carta di “accesso condizionato”. Tuttavia, nulla vieta di usare quel lettore anche per utilizzare una carta di altro tipo, come per es. una CNS.

I decoder interattivi sono dotati di un ambiente di elaborazione basato sullo standard MHP (Multimedia Home Platform). Si tratta in pratica di un ambiente Java, per il quale è possibile scrivere applicazioni dotate di interfaccia grafica, in grado anche di collegarsi ad Internet (attraverso il cosiddetto “canale di ritorno” rappresentato dal modem interno) e di interagire con una carta. Queste possibilità permettono quindi alle Amministrazioni di realizzare servizi on-line fruibili anche attraverso il decoder DTT. Laddove sia necessaria l'interattività, questa è supportabile dal “canale di ritorno” attraverso il quale è possibile effettuare comunicazioni anche col protocollo HTTP.

Le applicazioni sono inviate in modalità “broadcast” a tutti gli utenti, utilizzando il medesimo segnale radio che veicola la trasmissione TV. Su ogni canale DTT possono essere trasmesse diverse applicazioni, in orari diversi del giorno. Le Amministrazioni interessate a diffondere le proprie applicazioni MHP alla cittadinanza devono prendere accordi con un operatore di rete DTT al fine di accedere ad una “banda” di trasmissione.

Di seguito descriviamo le particolarità del colloquio con la carta in ambiente MHP.

8.4 Modalità di colloquio con la smartcard

Il parco di decoder installati in Italia al termine dell'anno 2005 risulta essere equipaggiato con un'implementazione di MHP v1.0.2 o v1.0.3. Buona parte di questi decoder consentono l'accesso alla smartcard tramite l'interfaccia “OCF” sviluppata dal consorzio Open Card (<http://www.opencard.org>); il colloquio avviene in modo conforme a quanto previsto dallo standard ISO 7816-4.

Anche la v1.1.1 delle specifiche MHP (l'ultima versione ufficiale pubblicata) prevede l'uso di OCF per il colloquio con la smartcard, ma tale versione di MHP non è ancora presente nei decoder sul mercato. La v1.1.2 delle specifiche MHP, ancora allo stato di bozza, prevede invece l'utilizzo del pacchetto “SATSA” della Sun Microsystems.

Al momento non è chiaro se la prossima generazione di decoder DTT che sarà immessa sul mercato sarà conforme alla specifica MHP v1.1.1 oppure alla specifica MHP v1.1.2. In ogni caso, le particolari API utilizzate per colloquiare con la smartcard (OCF, SATSA) possono essere mascherate alle applicazioni MHP tramite l'adozione di un opportuno layer di astrazione.

8.5 Possibili utilizzi della CNS in ambiente MHP

8.5.1 Identificazione ed autenticazione in rete

Anche in ambiente MHP è possibile effettuare l'identificazione ed autenticazione in rete, in quanto su ogni decoder è presente un "canale di ritorno" (modem interno) che permette la comunicazione TCP/IP con elaboratori raggiungibili su Internet. Sul canale di ritorno si possono utilizzare i classici protocolli Internet, tipicamente HTTP ed HTTPS (ovvero HTTP protetto con SSL).

Si possono adottare almeno due diverse tecniche per l'identificazione in rete:

8.5.1.1 Autenticazione in modalità Challenge/Response (CH/R)

Analogamente a quanto descritto nel paragrafo 4.4 del presente documento, il processo si articola nei seguenti passi:

- il client invia al server il proprio certificato di autenticazione (estratto dalla CNS);
- il server verifica il certificato utente, produce un messaggio randomico di autenticazione (Challenge) e lo invia al client;
- il client "firma" il Challenge con la chiave privata di autenticazione dell'utente (tramite la CNS) ottenendo un messaggio (Response) che viene inviato al server;
- il server verifica l'autenticità della Response tramite la chiave pubblica contenuta nel certificato utente;
- se la verifica ha successo, il server ha ottenuto l'identità certa dell'utente.

In questo caso, i dati scambiati tra client e server nei vari passaggi sono *veicolati a livello applicativo*, ossia sopra il livello dei sockets TCP (per esempio a livello HTTP, ma non necessariamente).

8.5.1.2 Autenticazione in modalità SSL Client Authentication

Il supporto per la *client authentication* SSL è solo opzionale nelle specifiche MHP v1.0.x e v1.1.1. Di fatto, negli attuali decoder, la SSL client authentication non è disponibile come funzionalità nativa. Chi desidera usare tale meccanismo, alla stregua di quanto si fa in ambiente PC, deve quindi utilizzare del software aggiuntivo.

Ricordando che l'ambiente MHP si basa sulle specifiche Java, per gestire la SSL client authentication è necessario disporre di un opportuno "provider crittografico" nei termini previsti dalla Java Cryptography Architecture (JCA) della Sun. Tale provider crittografico deve evidentemente interagire con la CNS se si desidera che la SSL client authentication utilizzi la chiave privata di autenticazione dell'utente.

8.6 Dati personali e servizi aggiuntivi

La digitazione di numeri e lettere tramite i tasti del telecomando di un decoder DTT è un'operazione piuttosto scomoda rispetto all'uso di una normale tastiera di PC: ci vuole più tempo ed è più facile commettere errori. L'uso delle cosiddette "tastiere virtuali", visualizzate sullo schermo TV, risolve il problema solo in parte.

Ogni qual volta un'applicazione MHP debba ottenere i dati anagrafici dell'utente, risulta molto più efficiente leggerli dalla CNS piuttosto che chiederne la digitazione. Alcuni dati potranno sempre essere

letti dal file *EF_DatiPersonali* presente su tutte le CNS: nome, cognome, codice fiscale, data di nascita, località di residenza, ecc.

Altri dati personali (es. numeri di telefono, numeri di conto corrente, userid/password, ecc) potranno invece essere letti da appositi “servizi aggiuntivi” sulla CNS, secondo le esigenze di ogni particolare applicazione. In un tale contesto, la disponibilità sulla CNS di un servizio che consenta la scrittura e lettura di dati generici può risultare molto utile ed efficiente, considerando che i decoder non consentono l’uso di memorie di massa rimovibili come floppy disk, chiavi USB, ecc.

Più in generale, i “servizi aggiuntivi” possono rappresentare la base per un’ampia gamma di possibili applicazioni interattive fruibili in ambiente MHP.

8.7 Una nota sulla sicurezza delle applicazioni MHP

Lo standard MHP prevede che l’accesso alle “risorse critiche” del decoder, quali il canale di ritorno e la smartcard, venga concesso solo ad applicazioni *firmate digitalmente dall’autore* e provviste dei necessari privilegi di accesso alla risorsa richiesta. Tuttavia, negli attuali decoder, tale meccanismo di sicurezza è disabilitato.

Il consorzio dei broadcaster italiani (DGTVi) intende abilitare la sicurezza nei decoder quanto prima, ma per il momento occorre ricordare che tutte le applicazioni MHP (firmate o non) possono accedere alla smartcard e al canale di ritorno.

D’altra parte, va detto che la particolare modalità di distribuzione delle applicazioni MHP rende molto più difficile e quindi più improbabile la circolazione di applicazioni “maligne” rispetto al caso di Internet. Lo stesso ambiente MHP impone molti più vincoli alle applicazioni di quanto non accada sui PC. Queste considerazioni, insieme al fatto che la CNS è per definizione una smartcard molto sicura, portano a ritenere che l’uso della CNS sul decoder DTT sia più sicuro che non sui normali PC, anche con la sicurezza MHP disabilitata.

8.8 Lo stato dell’arte

Sono state condotte numerose sperimentazioni sull’utilizzo della CNS nell’ambito dei sistemi di pagamento, del digitale terrestre e del contactless tramite l’interfaccia esterna dell’antenna.

Nei sistemi di pagamento sono significative le esperienze del Progetto TESEO (collegato a un gruppo di comuni guidati dal Comune di Verona che ha sperimentato il Sistema BankPass Web per i pagamenti online di una serie di servizi locali erogati in rete) e della Regione Lombardia (che ha installato un sistema di pagamento elettronico nella CNS emessa su l’intero territorio regionale nell’ambito del Progetto CRS-SISS).

Significativi i numerosi esperimenti condotti sull’utilizzo della CNS nei decoder interattivi nell’ambito dei progetti cofinanziati dal CNIPA e dal Ministero delle Comunicazioni.

Infine è importante citare anche le sperimentazioni della CNS come controllo accesso ai varchi, biglietto elettronico, strumento per il controllo presenze e supporto per la gestione di informazioni biometriche.

Capitolo 9

L'ambiente software sul client

L'utilizzo della carta sul client differisce in base al sistema operativo installato sulla macchina ove opera l'utente (client). Inoltre, se la carta viene utilizzata come token crittografico per l'autenticazione o la firma digitale, la configurazione differisce se si opera in ambiente open source piuttosto che in ambiente win32 con Explorer.

L'utilizzo dell'applicazione sanitaria basata su Netlink è basata su software specifico che utilizza i comandi di sistema operativo della carta (APDU) e quindi le librerie di corredo della carta (PKCS#11 e CSP - Cryptographic Service Provider) non sono di alcuna utilità per tale specifica applicazione.

Le librerie PKCS#11 vengono interfacciate direttamente da questa tipologia di codice. La stessa libreria in ambiente Microsoft deve essere mediata rispetto all'utilizzo crittografico (autenticazione e firma digitale) da uno specifico modulo denominato, come già detto, CSP.

9.1 Modalità di utilizzo della CNS in ambiente open source (Netscape, Mozilla, ecc.)

Per tranquillità dell'utente e del gestore locale del progetto è bene precisare che pur trattandosi di tecnologie complesse, l'onere sull'utente finale è minimo. Ogni carta viene fornita di una libreria PKCS#11 in grado di utilizzarne le caratteristiche di token crittografico. In particolare se si utilizza la CNS come token di accesso ai siti sicuri, la libreria deve essere installata sul sistema client e il browser configurato per poter "vedere" il nuovo modulo crittografico.

Ovviamente l'utilizzo della carta per la firma digitale può avvenire con la stessa libreria ma con un software specifico per l'operazione diverso da quello del browser. Per tale circostanza, in alcune configurazioni, è accettabile la disponibilità di due librerie. La prima solo per l'autenticazione in rete in modalità "autenticazione forte" e l'altra, da installare eventualmente in seguito, per le operazioni di firma digitale.

In ogni caso il client deve disporre di software (driver) conforme allo standard PC/SC. Tale software è indispensabile per utilizzare il lettore/scrittore di smart card.

Le modalità di configurazione ed utilizzo di tali librerie non è tra gli scopi del documento, ma sarà oggetto di specifica documentazione.

9.2 Modalità di utilizzo della CNS in ambiente Microsoft

L'unica differenza con quanto descritto nel paragrafo precedente è che per utilizzare la libreria PKCS#11 fornita a corredo della carta bisogna disporre di un ulteriore software denominato CSP.

In realtà il CSP non utilizza le PKCS#11 ma, per eseguire operazioni crittografiche, si poggia sull'uso delle Microsoft Crypto API. Come detto nei capitoli precedenti, anche la libreria CSP viene fornita a corredo della carta e risulta essere l'alternativa alla libreria PKCS#11 in ambiente Microsoft.

Anche in questo caso le operazioni di autenticazione e firma utilizzano software di supporto specifico (il browser e il software di firma).

Le modalità di configurazione e utilizzo del CSP non è tra gli scopi del presente documento, ma sarà oggetto di specifica documentazione.

9.3 Modalità di utilizzo della CNS in modo semplificato

Anche se ben documentate le librerie PKCS#11 e CSP non sono di facile utilizzo per uno sviluppatore medio. Per limitare i disagi si può prevedere di sviluppare un'ulteriore libreria per rendere direttamente fruibili allo sviluppatore funzionalità complesse. Una tale libreria, che possiamo definire di metacomandi, una volta referenziata, può direttamente attivare le funzioni di lettura della carta, di firma digitale o altre specifiche funzioni come l'estrazione del codice fiscale dalla carta stessa.

Sul sito web del CNIPA è disponibile una libreria di riferimento definita nell'ambito di una fornitura aggiudicata tramite una gara d'appalto comunitaria.

9.4 Modalità di utilizzo della CNS in ambiente Linux o MACOS X

La possibilità di utilizzo della CNS da parte di titolari che non utilizzano la piattaforma Windows non deve essere trascurata in considerazione del fatto che il numero di utenti che utilizzano piattaforme Linux piuttosto che MAC è tutt'altro che trascurabile.

Si deve tenere in conto anche degli aspetti relativi all'accessibilità dei siti web, alle norme di tutela degli utenti e alla corretta concorrenza sul mercato.

Per queste tipologie di utenti, titolari di CNS, non vi sono particolari ostacoli al suo utilizzo. Sul mercato, sono disponibili da tempo, lettori di carte dotati di librerie software per interfacciare gli ambienti operativi Linux e MacOS X. Entrambi i sistemi operativi consentono di connettersi ai lettori con le stesse modalità utilizzate in ambiente Windows (cfr. la sezione 3.1.2 del presente documento). Tale funzionalità è offerta da pacchetti open source che hanno raggiunto un adeguato livello di stabilità e che sono in grado di funzionare nelle applicazioni tradizionali.

In tale contesto è anche necessario disporre delle librerie software che garantiscono il colloquio con browser come Netscape e Mozilla/Firefox. Tale libreria è in genere realizzata dal produttore della CNS, dal certificatore accreditato che genera i certificati di autenticazione o da una generica terza parte, avendo a disposizione le specifiche funzionali e del file system della CNS.

Capitolo 10

L'ambiente di accesso sul server

Il modello di autenticazione introdotto dalle carte di accesso ai servizi si basa su meccanismi di “strong authentication” che sfruttano i certificati digitali X.509 all'interno dei meccanismi di sicurezza SSL/TLS. Questi meccanismi di sicurezza, nelle situazioni funzionali più comuni, sono associati al protocollo http.

Il modello funzionale dei certificatori di firma digitale accreditati secondo la normativa vigente in Italia, realizza un modello di tipo paritario, nel quale il singolo certificatore, non è in relazione gerarchica con altre infrastrutture ma opera in un dominio indipendente e interoperabile con gli altri.

Questo modello, particolarmente efficiente all'interno del dominio del singolo certificatore, introduce criticità rispetto all'interoperabilità pressoché assenti in un modello gerarchico. In particolare, deve essere gestito il numero massimo di certificati root che il server web può gestire come pure la modalità di verifica di validità del certificato a fronte di CRL emesse da certificatori diversi.

In questo contesto è bene descrivere i principi generali ai quali attenersi per garantire le funzionalità necessarie all'ambiente di controllo dell'autenticazione sul server, per utilizzare i certificati di autenticazione installati nelle carte di accesso.

Le problematiche di dettaglio delle configurazioni del web/application server sono specifiche dei singoli prodotti ma comunque non si discostano in modo significativo da quanto esposto nel seguito.

Qualora necessario verrà garantito il supporto per specifiche architetture.

10.1 L'ambiente di accesso in modalità web

Per non appesantire il documento con informazioni non strettamente pertinenti ai suoi scopi, non viene inserita una descrizione, seppur sintetica, del protocollo SSL/TLS. Tale conoscenza deve essere quindi un prerequisito per la lettura del seguito.

Si ipotizza quindi che il processo di autenticazione “forte” avvenga mediante i meccanismi standard previsti dalle applicazioni basate sulle tecnologie web ovvero mediante il protocollo SSL/TLS.

Come evidenziato in un precedente capitolo, l'autenticazione “forte” è un meccanismo di sicurezza che, nelle architetture considerate, utilizza i certificati digitali. Praticamente significa che una postazione utente (il client) quando richiede l'accesso a una applicazione accessibile esclusivamente a seguito di autenticazione, invia tramite il protocollo SSL/TLS le credenziali dello specifico titolare in forma di certificato digitale. Il server web è in grado di gestire le informazioni presenti nel certificato e in particolare quelle presenti nel campo “common name”. La presenza del codice fiscale in questo campo rende immediatamente disponibile questa informazione ai meccanismi di sicurezza e qualora le verifiche siano positive, il server web connette l'utente all'applicazione da lui richiesta.

Come si vede il codice fiscale è indispensabile per attivare l'associazione tra il titolare della carta e l'applicazione alla quale egli è autorizzato ad accedere (nel seguito daremo dei dettagli sul processo di

autorizzazione). In altre parole, il codice fiscale costituisce lo username dell'utente. La sua unicità è indispensabile e questa viene garantita mediante i meccanismi stabiliti nella legislazione vigente.

E' bene ricordare che, per completare il processo di scambio delle credenziali di sicurezza, il titolare della carta di accesso deve digitare il PIN di sblocco. Inoltre, poiché vengono prima completate le operazioni di crittografia tra client e server e poi si prosegue con lo scambio di credenziali per l'autenticazione, tutte le informazioni non viaggiano in chiaro sulla rete nella tratta coinvolta.

10.1.1 Il processo di autorizzazione

Una volta che il server web ha autenticato il titolare della carta di accesso, si devono definire le autorizzazioni alle quali il titolare ha diritto. Ovviamente le cosiddette ACL (Access Control List) sono fortemente dipendenti dalla realizzazione dell'ambiente di accoglienza sul server e dalle modalità di accesso alla banca dati da parte delle applicazioni invocate dagli utenti.

Ovviamente esistono dei principi di carattere generale sempre applicabili quando si descrive un ambiente operativo dotato di controllo d'accesso. In particolare è possibile, senz'altro in tutti i contesti, considerare gli utenti singolarmente o per gruppo omogeneo. Prendendo come riferimento l'ambiente Java 2 Enterprise Edition (J2EE) possiamo considerare quanto segue (non esistono differenze sostanziali in ambiente .Net, salvo ovviamente la non interoperabilità di alcune componenti).

La sicurezza, nel contesto Web Application Server J2EE consiste di due parti principali: autenticazione e autorizzazione (il termine autenticazione va inteso nella sua espressione tecnica classica per evitare ambiguità con l'ordinamento giuridico dove "autenticazione" ha un altro significato). L'autenticazione viene delegata in modo pressoché totale ai certificati digitali e al protocollo http nell'ambito delle funzionalità tipiche dei server web di front-end. I meccanismi differiscono in base al server utilizzato. I più diffusi tra i server web sono I-Planet, Apache e Internet Information Server. Ognuno di loro utilizza modalità specifiche di gestione dei certificati digitali, anche se i vari ambienti non differiscono in modo sostanziale. La parte più critica è quella della gestione delle liste di revoca (CRL) o, in alternativa, dell'interrogazione di server OCSP (Online Certificate Status Protocol). Non è obiettivo di questo documento fornire i dettagli tecnici di queste operazioni. Naturalmente a richiesta verrà fornito tutto il supporto necessario per l'armonizzazione delle soluzioni che le amministrazioni intendono realizzare.

I meccanismi di autorizzazione sono realizzati all'interno dell'application server.

Il modello di sicurezza J2EE consente di costruire uno schema per le autorizzazioni delle utenze referenziate via web garantendo granularità per l'accesso e l'utilizzo delle singole applicazioni fino alle singole funzioni ("metodi" nell'ambiente J2EE).

Durante la fase di sviluppo dell'applicazione vengono creati ruoli e permessi, in modo tale che i permessi di esecuzione siano assegnati a uno o più ruoli di sicurezza. A questa fase segue, al momento della messa in linea dell'applicazione, l'associazione dei ruoli di sicurezza a utenti singoli o gruppi di utenti.

A un utente possono essere assegnati più ruoli e quindi i suoi permessi sono l'unione dei permessi dei singoli ruoli; l'associazione di un gruppo a un ruolo equivale all'assegnazione di tutti i suoi utenti a tale ruolo.

E' ovvio che questo tipo di approccio a due fasi consente elevati gradi di portabilità e flessibilità nell'amministrazione della sicurezza. I responsabili dell'applicazione possono controllare come gli utenti o gruppi di utenti sono associati ai ruoli di sicurezza definiti per l'applicazione e sui meccanismi di autorizzazione e di autenticazione usati per determinare l'appartenenza ai ruoli.

La gestione della sicurezza effettuata in questo modo consente di gestire le politiche relative a una applicazione in modo tale che possano essere realizzate senza vincoli all'interno del codice applicativo (sicurezza di tipo dichiarativo). Da questo aspetto si deduce che possono essere radicalmente cambiati gli aspetti di sicurezza senza che sia necessario agire sul software applicativo.

In alcune transazioni può accadere che il livello di autorizzazione all'azione su una specifica funzione si debba spingere fino a considerare il contenuto del dato trattato. Il modello di autorizzazione J2EE prevede che l'applicazione possa ottenere informazioni, sia sul ruolo sia sull'identità di chi sta richiedendo una certa operazione, al fine di prendere le opportune decisioni derivanti dalle politiche di si-

curezza da garantire. Questo tipo di approccio viene generalmente indicato come sicurezza di tipo programmatico.

10.1.2 Tecnologie per un'identità federata

Si stanno diffondendo alcune architetture tecnologiche per la gestione di identità federate. Una fa riferimento all'ambiente Microsoft e si chiama Passport.

L'altra è la Liberty Alliance Project supportata da un consorzio di industrie con la specifica di realizzare un protocollo per le funzionalità di autenticazione e autorizzazione tra le istituzioni coinvolte, indipendentemente dai meccanismi di sicurezza interni alle istituzioni stesse.

L'utilizzo di questi meccanismi in un ambiente federato può essere opportuno nei seguenti casi:

- pubblica amministrazione centrale o locale non dotata di meccanismi in grado di verificare le credenziali degli utenti;
- integrazione con la verifica dell'identificativo elettronico fornito dalle carte di accesso.

Il primo caso rappresenta lo scenario tipico in cui una pubblica amministrazione non è in grado di identificare gli utenti perché non possiede i dati di autenticazione. Attraverso un processo di federazione dell'identità si stabilisce una relazione di fiducia tra diverse istituzioni in modo che una o più organizzazioni possano fornire i dati d'autenticazione a un terzo ente che li richiede.

Il secondo caso rappresenta lo scenario più diretto a risolvere, nell'utilizzo delle carte d'accesso, il problema della non immediata disponibilità delle informazioni sull'identità dell'utente attraverso il meccanismo dei certificati digitali. In questo caso, uno o più enti possono fungere sia da "Authentication authority" che da "Attribute authority" per fornire i dati relativi all'identità e eventuali altre informazioni sull'utente, come ad esempio il codice fiscale.

Tali processi si basano su meccanismi standard di sicurezza (Liberty/SAML) che rispettano i principi di riservatezza/privacy, integrità e disponibilità dei dati.

Il SAML (Security Assertion Markup Language) è uno standard aperto per la realizzazione delle funzionalità di autenticazione, autorizzazione e single sign on sul web. Esso si basa sul linguaggio XML e utilizza un modello di servizio composto da 5 entità:

- Principal
- Authentication authority
- Attribute authority
- Policy decision point (PDP)
- Policy enforcement point (PEP)

Alcuni dei principali fornitori di application server utilizzano questo tipo di tecnologia e, in particolare, delle estensioni del SAML.

Capitolo 11

La sicurezza del circuito della CNS

Ai fini della sicurezza del circuito, l'intero ciclo di vita della CNS deve essere opportunamente tracciato, dal momento di inizio della produzione della carta, fino al ritiro della CNS. Ciascuna attività elementare (produzione, inizializzazione, registrazione, emissione del certificato, personalizzazione, ecc.) deve essere registrata in appositi registri che devono essere sottoscritti dal responsabile dell'attività e conservati in modo protetto.

11.1 La sicurezza della fase di produzione

La produzione delle smart card destinate ad operare come CNS deve avvenire con criteri che garantiscano la segretezza delle informazioni presenti nelle carte inizializzate.

E' opportuno scegliere produttori che abbiano provata esperienza nella produzione di carte con elevati requisiti di sicurezza (ad esempio carte di credito e di debito).

Di seguito vengono esposti alcuni criteri di sicurezza che dovranno essere seguiti dal produttore delle CNS. Tali criteri devono essere considerati come indicativi e non esaustivi, per cui il rispetto di tali criteri non solleva il fornitore dalle responsabilità circa la sicurezza del processo produttivo.

11.1.1 Fasi di lavorazione della carta

Durante l'intero processo di lavorazione, le strutture interne della smart card devono essere protette mediante opportuni codici (PIN, codici di trasporto, ecc.) finalizzati a consentire al solo personale autorizzato la modifica di tali strutture.

I codici di protezione devono essere generati in modo casuale, quindi trasmessi e memorizzati in forma cifrata, con modalità tale da rendere possibile il loro utilizzo esclusivamente agli apparati preposti alla lavorazione della carta.

Questi apparati devono inoltre poter operare unicamente sotto il controllo di operatori muniti di opportuna smart card personale (smart card operatore, di seguito specificata) ovvero di altri sistemi di controllo accesso di paragonabile sicurezza.

Il sistema di sicurezza che governa il processo produttivo (fasi di produzione ed inizializzazione) deve assicurare:

- l'autenticazione certa dell'operatore;
- la registrazione di tutte le operazioni effettuate e dei dati utili alla tracciatura del processo;
- la protezione delle informazioni di tracciatura in modo tale da garantirne integrità e non ripudio.

11.1.2 Conservazione e trasporto delle carte

Quando le carte non sono in lavorazione, devono essere conservate in locali (di tipo caveau) in grado di assicurare adeguati livelli di sicurezza. Ogniqualvolta le carte devono transitare tra siti diversi, devono utilizzare un trasporto con regolare bolla di consegna che deve essere verificata dal responsabile della Sicurezza della sede di arrivo.

11.1.3 Gestione degli scarti

Ogni lavorazione deve tenere traccia degli eventuali scarti ed i moduli utilizzati per tracciare le attività devono riportare sia il numero delle smart card utili, sia il numero degli scarti non utilizzabili. Sia le smart card utili che le non utilizzabili devono essere conservate nel Caveau. Al centro di emissione devono pervenire sia le smart card utili che gli scarti in modo da poter verificare la corrispondenza con il numero delle carte complessive previste. La distruzione degli scarti può essere effettuata solo da un'apposita commissione con procedura verbalizzata.

11.1.4 Generazione delle chiavi

Il software presente sul sistema di personalizzazione dovrà provvedere a tale operazione in modalità sicura.

A tal fine il sistema dovrà leggere l'identificativo della carta ed accedere all'archivio cifrato contenente i PIN di personalizzazione.

A questo punto sarà possibile attivare la generazione delle coppie di chiavi RSA relative all'autenticazione e, eventualmente, alla firma digitale.

Durante questa operazione saranno creati i PIN utente di attivazione delle relative chiavi private.

Tali PIN dovranno essere memorizzati in un archivio cifrato.

11.1.5 Tracciatura delle operazioni

Tutte le operazioni di inizializzazione dovranno essere tracciate in appositi registri elettronici o cartacei. I registri dovranno essere conservati per un periodo non inferiore a 10 anni a decorrere dalla data dell'ultima registrazione inserita. In particolare, il registro di entrate/uscite delle smart card dovrà essere compilato per ogni singolo movimento, con indicazione della data ed dell'ora e dovrà essere firmato sia dal Responsabile della Sicurezza sia dal Responsabile della fase produttiva.

11.1.6 Protezione delle informazioni di tracciatura

La smart card operatore dovrà essere dotata anche di una coppia di chiavi con relativo certificato di crittografia. Occorrerà predisporre un archivio protetto in grado di contenere tutti i record relativi alle carte prodotte, cifrati con la chiave di crittografia presente nella smart card operatore.

La chiave utilizzata per proteggere tali record dovrà essere tenuta in modalità "memorizzazione protetta" all'interno della smart card dell'operatore.

Gestione della smart card dell'operatore

La Smart Card Operatore deve essere generata, attraverso l'uso di software dedicato di generazione, mediante una procedura che assicuri la massima sicurezza del processo. In fase di generazione della carta, saranno registrate su di essa le informazioni di sicurezza (chiavi crittografiche) necessarie per l'accesso ai file protetti e la firma elettronica dei record di tracciatura.

Tale smart card dovrà essere consegnata al responsabile del processo produttivo, od a persona da lui delegata, e conservata in cassetta di sicurezza all'interno di un locale accessibile solo dal responsabile della sicurezza.

L'apertura della cassetta di sicurezza contenente tale smart card di firma dovrà avvenire con una procedura che preveda la presenza congiunta del responsabile della sicurezza e del responsabile del processo produttivo ovvero della persona da lui delegata..

Ogni accesso alla cassetta contenete la smart card dovrà essere documentato firmando opportuni registri.

11.1.7 Misure organizzative

Dovranno essere previste opportune misure organizzative finalizzate a gestire in modo efficace la sicurezza dei siti.

In particolare, dovrà essere presente in ogni sito una opportuna organizzazione della sicurezza che deve prevedere almeno un Responsabile di Sicurezza per turno che risponderà al Responsabile della Sicurezza dell'Organizzazione.

I responsabili della sicurezza dovranno garantire il rispetto di tutte le procedure e le norme previste dall'organizzazione.

11.1.8 Misure di sicurezza fisiche

L'esterno dello stabilimento deve essere recintato e controllato tramite telecamere.

I cancelli devono essere sempre chiusi e gli utenti, i fornitori e gli spedizionieri non devono avere accesso ai locali interni se non dopo essersi presentarsi alla *reception* per il riconoscimento.

Nel caso di ingresso automezzi, il personale addetto alla *reception* deve avvertire il Responsabile di Sicurezza o il magazziniere, i quali ricevono all'esterno gli automezzi dopo che il personale addetto alla *reception* ha azionato il pulsante di apertura cancelli che si richiuderà automaticamente dopo un tempo predeterminato.

Tutti i dipendenti, anche quelli facenti capo ad uffici non inerenti la produzione o la personalizzazione, devono avere a disposizione un badge di ingresso con accesso limitato ad aree ben definite. Gli uffici devono essere protetti da intrusioni esterne, almeno tramite sensori alle finestre.

Gli impianti di sicurezza devono essere attivati dopo l'orario di chiusura e disattivati prima dell'orario di apertura degli uffici.

Nel caso in cui si debba protrarre l'orario di chiusura o anticipare l'orario di apertura, si dovrà necessariamente avvertire il Responsabile di Sicurezza che opererà di conseguenza.

L'accesso all'edificio in cui si svolge la produzione delle carte dovrà essere possibile solo dopo aver superato una bussola di sicurezza. Dovrà inoltre essere previsto un servizio di guardiania che consentirà l'accesso ai reparti o agli uffici solo dopo le operazioni di riconoscimento o registrazione.

L'ingresso dovrà essere suddiviso tra:

- dipendenti con badge nominativi il cui passaggio è registrato dalla bussola e dal sistema di monitoraggio basato su telecamere;
- visitatori che si qualificano al citofono e accedono alla hall tramite la bussola operata dalla guardiola.

La qualificazione e la registrazione in guardiola dei visitatori deve basarsi su un documento di identità valido, di cui deve essere prodotta una fotocopia che sarà archiviata per un anno. Il personale addetto alla *reception* dovrà avvertire il dipendente a cui il visitatore fa riferimento. Questi dovrà prendere in consegna il visitatore, che verrà munito di un badge personale che verrà restituito alla fine della visita. Su apposito registro verrà registrato l'orario di ingresso e di uscita che verrà firmato dal dipendente con funzione di accompagnatore.

11.2 La sicurezza della fase di emissione

La fase di emissione comprende la personalizzazione della carta, la verifica dei dati anagrafici e la consegna della carta al titolare, unitamente ai codici segreti PIN e PUK.

Queste attività possono essere svolte con modalità e tempi diversi, in ogni caso devono essere seguiti criteri di sicurezza volti ad evitare il furto e la personalizzazione criminosa di carte inizializzate o la consegna della carta a persone diverse dal legittimo titolare.

Presso i centri di personalizzazione e di emissione dovranno essere attuate le misure tecniche ed organizzative previste per la tutela dei dati personali (Codice in materia di protezione dei dati personali – DL 30 giugno 2003, n. 196).

In particolare, il documento programmatico per la sicurezza dovrà indicare le azioni messe in atto per proteggere le carte nei confronti del rischio di furto o di utilizzo improprio.

11.2.1 Protezione delle carte inizializzate

E' necessario predisporre opportune misure di sicurezza fisica per la protezione delle carte. Nel caso di spostamento delle carte tra locali o siti diversi, deve essere utilizzato un trasporto con regolare bol-la di consegna che deve essere verificata dal responsabile della Sicurezza della sede di arrivo

Tutte le operazioni di personalizzazione dovranno essere tracciate in appositi registri elettronici o cartacei. I registri dovranno essere conservati per un periodo non inferiore a 10 anni. In particolare, il registro di entrate/uscite delle smart card dovrà essere compilato per ogni singolo movimento con data ed ora e firmato dal responsabile della struttura di personalizzazione.

11.2.2 Protezione dei flussi di dati

I flussi informativi che durante il processo produttivo si generano tra la struttura di registrazione, il certificatore e la struttura di personalizzazione, devono utilizzare esclusivamente canali sicuri, utilizzando sistemi di crittografia simmetrica di lunghezza almeno pari a 128 bit..

Nel caso di utilizzo di una sessione SSL, dovranno essere impiegati sia i meccanismi di autenticazione del server, sia quelli relativi alle postazioni client.

Capitolo 12

Conclusioni

Con l'avanzare degli sviluppi dei "cantieri" dell'e-government, aumenta con significativa consistenza il numero dei progetti che intende utilizzare la CNS. Per concludere queste linee guida facciamo il punto sullo stato di avanzamento lavori dei progetti al momento della pubblicazione del presente documento. Naturalmente lo stato dell'arte costituirà un paragrafo in costante evoluzione. Di tale evoluzione si darà evidenza nell'ambito delle riunioni istituzionali previste nell'ambito della "visione condivisa".

12.1 Lo stato dell'arte

Al momento vi sono in corso vari progetti di rilascio di CNS. Oltre al progetto del Sistema Informativo Socio Sanitario della Regione Lombardia che completerà la distribuzione delle smart card entro la primavera del 2005, sono in fase di sviluppo una serie di altri progetti di distribuzione della CNS nell'80% delle regioni italiane.

Importanti progetti sono stati sviluppati anche nei comuni di Bologna, Verona e S. Giorgio a Cremano e altri sono in fase di studio di fattibilità.

Tra i sottoscrittori del protocollo d'intesa del 13 maggio 2003, solo due soggetti supportano le specifiche previste da tale protocollo. Altri quattro prevedono di supportarle nel breve periodo, mentre ulteriori due, utilizzando tecnologia dei primi due citati possono di fatto definirsi conformi.

I restanti soggetti stanno predisponendo un piano di convergenza.

Nell'attesa di alcune decisioni del Ministro dell'Interno sulla CIE, si stanno valutando le migliori soluzioni per interfacciare dal terminale utente la CNS. Ovviamente, tali soluzioni sono conformi a quelle descritte nel presente documento.

Come più volte ribadito nel documento non sono stati approfonditi alcuni aspetti tecnici non perché di scarsa rilevanza nell'ambito dei progetti, ma a causa delle numerose specificità dei progetti territoriali. In ogni caso non è certamente oneroso gestire le eccezioni per garantire, nel quadro complessivo, la loro coerenza con le specifiche di riferimento del progetto.

Appendice 1

Profilo di certificato digitale per l'autenticazione mediante Carta Nazionale dei Servizi (CNS)

Per ragioni di chiarezza nell'interpretazione del profilo il testo è stato redatto secondo le indicazioni della specifica pubblica RFC 2119.

1 Scopo

Nel presente documento viene definito il profilo del certificato di autenticazione per l'utilizzo nell'ambito dell'emissione della Carta Nazionale dei Servizi (CNS) [9].

Il profilo proposto consente di individuare lo specifico circuito di emissione che ha generato il certificato.

2 Riferimenti

I seguenti documenti contengono definizioni e indicazioni di riferimento che sono citate all'interno del testo e che costituiscono parte integrante della proposta.

I riferimenti sono specifici (identificati dalla data di pubblicazione e/o numero di versione o dal numero di versione) oppure non specifici. Per i riferimenti specifici le revisioni successive non sono applicabili mentre lo sono per i riferimenti non specifici.

- [1] CIRCOLARE n. AIPA/CR/24, "Linee guida per l'interoperabilità tra i certificatori iscritti nell'elenco pubblico di cui all'articolo 8, comma 3, del decreto del Presidente della Repubblica 10 novembre 1997, n. 513", 19 giugno 2000, (G.U. 30 giugno 2000, Serie generale n. 151).
- [2] RFC 1778, "The String Representation of Standard Attribute Syntaxes", IETF, March 1995.
- [3] RFC 2119, "Key words for use in RFCs to Indicate Requirement Levels", IETF, March 1997.
- [4] RFC 2246, "The TLS Protocol Version 1.0", IETF, January 1999.
- [5] RFC 2255, "The LDAP URL Format", IETF, December 1997.
- [6] RFC 2560, "Online Certificate Status Protocol – OCSP", IETF, June 1999.

- [7] RFC 3039, “Qualified Certificates Profile”, IETF, January 2001.
- [8] RFC 3280, “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile”, IETF, April 2002 (rende obsoleto l’RFC 2459).
- [9] CNS/CIE, documentazione tecnica per la Carta d’Identità Elettronica (CIE) e per la Carta Nazionale dei Servizi (CNS), <http://www.cartaidentita.it>, <http://www.cnipa.it>.

3 Introduzione

Le parole chiave “*DEVE*”, “*DEVONO*”, “*NON DEVE*”, “*NON DEVONO*”, “*E’ RICHIESTO*”, “*DOVREBBE*”, “*NON DOVREBBE*”, “*RACCOMANDATO*”, “*NON RACCOMANDATO*” “*PUO*” e “*OPZIONALE*” nel testo del documento debbono essere interpretate come descritto nel seguito, in conformità alle corrispondenti traduzioni contenute nel documento IETF RFC 2119 [3].

Le parole chiave “*DEVE*” o “*DEVONO*” o “*E’ RICHIESTO*” stanno a significare che l’oggetto in questione è un requisito assoluto della definizione.

Le parole chiave “*NON DEVE*” o “*NON DEVONO*” stanno a significare che l’oggetto in questione è un divieto assoluto per la definizione.

Le parole chiave “*DOVREBBE*” o “*RACCOMANDATO*” stanno a significare che, in particolari circostanze, possono esistere valide motivazioni per ignorare la particolare specifica, ma le complete implicazioni di tale scelta debbono essere comprese e pesate con cautela prima di scegliere per un’altra soluzione.

Le parole chiave “*NON DOVREBBE*” o “*NON RACCOMANDATO*” stanno a significare che, in particolari circostanze, possono esistere valide motivazioni perché la specifica sia accettabile o anche utile, ma le complete implicazioni debbono essere comprese e pesate con cautela prima di implementare una soluzione corrispondente.

Le parole chiave “*PUO*” o “*OPZIONALE*” stanno a significare che una specifica è puramente opzionale. Un soggetto può scegliere di includere l’oggetto perché un particolare mercato lo richiede o perché ritiene che il prodotto finale ne risulti migliorato, mentre è possibile che un altro soggetto ometta tale oggetto. Un’implementazione che non include una particolare opzione, *DEVE* essere preparata ad interoperare con un’altra implementazione che la include, anche se con ridotte funzionalità. Allo stesso modo, un’implementazione che include una particolare opzione, *DEVE* essere preparata ad interoperare con un’altra implementazione che non la include (eccetto per la particolare funzionalità che l’opzione consente).

Così come definito in IETF RFC 3280 [8], si rammenta che per ogni estensione usata all’interno di un certificato va definito se essa vada marcata “critica” oppure “non critica”. Un sistema che utilizzi il certificato *DEVE* rifiutare il certificato stesso se esso incontra un’estensione marcata “critica” che non riconosce od interpreta correttamente, d’altra parte un’estensione non marcata “critica” può essere ignorata.

4 Certificato di autenticazione

Nel presente documento viene definito il profilo del certificato di autenticazione per l’utilizzo nell’ambito dell’emissione della Carta Nazionale dei Servizi (CNS) [9].

Il profilo del certificato di autenticazione è basato sugli standard IETF RFC 3039 [7] e RFC 3280 [8].

5 Certificato di autenticazione per CNS

5.1 Informazioni relative al titolare (subject)

Le informazioni relative al titolare del certificato *DEVONO* essere inserite nel campo Subject (Subject DN).

In particolare l'attributo *commonName* (Object ID: 2.5.4.3) *DEVE* contenere il codice fiscale del titolare (nel seguito: *codiceFiscale*). Esso *DEVE* inoltre contenere l'identificativo univoco del dispositivo (*ID_Carta*) e il valore dell'hash calcolato sul file elementare contenente i dati personali del titolare così come memorizzato nel dispositivo (*EF_Dati_Personali*).

La valorizzazione dei sottocampi relativi all'identificativo del dispositivo e ai dati personali *DEVE* essere effettuata in conformità con le specifiche della CNS e con lo scopo di garantire l'interoperabilità con la CIE.

In conformità con quanto definito per la CNS e per compatibilità con i certificati inseriti all'interno della CIE (CNS/CIE [9]), il carattere separatore dei sottocampi *codiceFiscale* e *ID_Carta* dell'attributo *commonName* *DEVE* essere il carattere "/" (slash, ASCII 0x2F) mentre il carattere separatore dei sottocampi *ID_Carta* e *hashDatiPersonali* *DEVE* essere il carattere "." (dot, ASCII 0x2E).

(ad es.: "DMMRNT63H14H501T/123322123123.cd3fdfdfeH2Duowf5oasookDHo=" è un valore corretto per il *commonName*).

L'attributo *countryName* *DEVE* contenere il *Country Code* ISO 3166 dello Stato in cui è residente il titolare.

L'attributo *organizationalUnitName* *DEVE* contenere la denominazione dell'Amministrazione che ha rilasciato la carta.

La valorizzazione di altri attributi nel Subject DN *DEVE* essere eseguita in conformità allo RFC 3280 [8].

5.2 Estensioni del certificato

Le estensioni che *DEVONO* essere presenti nel certificato di autenticazione sono:

Key Usage, Extended Key Usage, Certificate Policies, CRL Distribution Points, Authority Key Identifier, Subject Key Identifier;

L'estensione Basic Constraints *NON DEVE* essere presente.

La valorizzazione delle estensioni elencate per il profilo descritto è riportata nel seguito.

L'estensione Key Usage (Object ID: 2.5.29.15) *DEVE* avere attivato il bit di *digitalSignature* (bit 0) e *DEVE* essere marcata critica. L'estensione *PUO'* contenere altri bit attivati corrispondenti ad altri Key Usage, purché ciò non sia in contrasto con quanto indicato in RFC 3280 [8] e in RFC 3039 [7]. L'estensione *NON DEVE* avere attivato il bit di *nonRepudiation* (bit 1).

L'estensione Extended Key Usage (Object ID: 2.5.29.37) *DEVE* contenere l'object id previsto per lo scopo di "TLS WWW Client Authentication" (Object ID 1.3.6.1.5.5.7.3.2) e *NON DEVE* essere marcata critica. L'estensione *PUO'* contenere altri valori che indicano altri scopi, purché non in contrasto con quanto indicato in RFC 3280 [8].

L'estensione Certificate Policies (Object ID: 2.5.29.32) *DEVE* contenere l'object id della Certificate Policy (CP) e l'URI (Uniform Resource Identifier) che punta al Certificate Practice Statement (CPS) nel rispetto del quale il certificatore ha emesso il certificato. Detto object id è definito e pubblicizzato dal certificatore. A far data dal mese di maggio 2005 l'estensione *DEVE* inoltre contenere l'object id "1.3.76.16.2.1" e il qualifier "userNotice" di tipo "explicitText" con il seguente contenuto: "Identifies X.509 authentication certificates issued for the italian National Service Card (CNS) project in according to the italian regulation".

Considerato che la regione Lombardia, nell'ambito del progetto CRS SISS, ha già emesso certificati di autenticazione e smart card comunque conformi alle norme sulla CNS, che dette carte costituiscono quindi delle CNS, si rendono pubblici i valori che l'object id può assumere nei suddetti certificati: "1.3.159.6.1.3.2.10" e "1.3.76.12.1.1.10.2.2.10".

Nel caso specifico di certificati emessi per il circuito della CNS la correttezza del valore contenuto nel campo codiceFiscale viene sempre verificata dall'ente emettitore (la Pubblica Amministrazione) come specificato in CNS/CIE [9].L'estensione Certificate Policies *NON DEVE* essere marcata critica.

L'estensione CRL Distribution Points (Object ID: 2.5.29.31) *DEVE* contenere l'URI che punta alla CRL/CSL pubblicata dal certificatore e utilizzabile per effettuare la verifica del certificato. In conformità a quanto definito in IETF RFC 3280 [8] par. 4.2.1.14 e par. 5.2.5, l'URI *DEVE* configurare un percorso assoluto per l'accesso alla CRL e non un percorso relativo ed inoltre *DEVE* specificare anche il nome del server.

Lo schema da utilizzare per l'URI *DEVE* essere l'http oppure l'ldap (IETF RFC 1778 [2] e RFC 2255 [5]) e consentire il download anonimo della CRL.

Costituiscono esempio valido i seguenti valori possibili:

“http://www.cns_crl.it/CRL/Autenticazione/crlauth”

“ldap://dir.cns_crl.it/cn=CA%20Autenticazione,o=Servizi%20di%20Certificazione,c=IT?certificatesRevocationList;binary”

L'estensione CRL Distribution Points *NON DEVE* essere marcata critica.

L'estensione Authority Key Identifier (Object ID: 2.5.29.35) *DEVE* contenere almeno il campo keyIdentifier e *NON DEVE* essere marcata critica.

L'estensione Subject Key Identifier (Object ID: 2.5.29.14) *DEVE* contenere almeno il campo keyIdentifier e *NON DEVE* essere marcata critica.

Se il certificatore mette a disposizione delle cosiddette “relying parties” (i terzi che effettuano la verifica della validità del certificato) un sistema di Online Certificate Status Protocol (OCSP, definito in IETF RFC 2560 [6]), ha la necessità di indirizzarle correttamente sui sistemi che forniscono tali informazioni (OCSP Responders).

In tal caso il certificato *DEVE* contenere l'estensione Authority Info Access (Object ID: 1.3.6.1.5.5.7.1.1). Tale estensione *DEVE* contenere almeno un campo AccessDescription valorizzato con l'OID 1.3.6.1.5.5.7.48.1 (id-ad-ocsp) nel campo accessMethod e l'URI che punta all'OCSP Responder del certificatore, utilizzabile per effettuare la verifica del certificato stesso, nel campo accessLocation. In conformità a quanto definito in IETF RFC 3280 [8] par. 4.2.2.1 e IETF RFC 2560 [6], l'URI *DEVE* configurare un percorso assoluto per l'accesso all'OCSP Responder ed inoltre *DEVE* specificare anche il nome del server.

Lo schema da utilizzare per l'URI *DEVE* essere almeno l'http e consentire l'interrogazione mediante il protocollo OCSP definito in IETF RFC 2560 [6].

Nel caso vengano valorizzati più di un AccessDescription per l'estensione, tali indicazioni debbono configurare diversi percorsi alternativi per lo stesso risultato, ossia l'interrogazione tramite OCSP dello stato del certificato al momento della richiesta.

Il valore “http://www.cns_ocsp.it/OSCPResponderOne” costituisce un esempio valido per l'accessLocation.

L'estensione Authority Info Access *NON DEVE* essere marcata critica.

L'aggiunta delle altre estensioni anche private non contenute in questo documento è *OPZIONALE* purché in conformità allo IETF RFC 3280 [8].

APPENDICE A. Esempio

Nel seguito è riportato un esempio di certificato digitale di autenticazione conforme.

a. Certificato per CNS in versione annotata

L'esempio riporta un certificato per CNS, i valori in esso contenuti sono immaginari e uti-

lizzati a puro scopo di esempio.

VERSION: 3
SERIAL: 7510 (0x1d56)
INNER SIGNATURE:
 ALG. ID: id-sha1-with-rsa-encryption
 PARAMETER: 0
ISSUER:
 Country Name: IT
 Organization Name: Certificatore accreditato
 Organizational Unit Name: Servizi di certificazione
 Common Name: Certification Authority Cittadini
VALIDITY:
 Not Before: Oct 28, 03 09:59:55 GMT
 Not After: Oct 27, 09 09:58:42 GMT
SUBJECT:
 Country Name: IT
 Organization Name: *Nome convenzionale di progetto*
 Organizational Unit Name: *Nome dell'amministrazione*
 Common Name: LGRDNT63H14H501T/1234567890123456.hRfo7thkjYF45tF40v0t8DkgilG=
PUBLIC KEY: (key size is 1024 bits)
ALGORITHM:
 ALG. ID: id-rsa-encryption
 PARAMETER: 0
MODULUS: 0x00a209b4 65f57559 1f699938 e29a27b3
 13a30893 7379cb22 37a6380e 9dd48c4d
 c9057d01 1039dd56 a55e9940 76c68c50
 069a25b5 d777ffc4 d8c56ca2 fc3163e0
 279d919f 0bb1d22d bb07d923 9e972ff3
 252ed27a 4781bccd 99d7b76d 149d08cd
 057f4b9d 9b04ddcb 76e1029e 16e0067f
 f7407553 01aa513e 126ae6b1 2977ea16
 b3
EXPONENT: 0x010001
EXTENSIONS:
 Authority Information Access:
 Method: id-ad-ocsp
 Location:
 Uniform Resource ID: <http://www.capki.it/OCSP/ResponderOne>
 Certificate Policies:
 Policy 1:
 ID: 1.3.76.16.2.1
 Qualifier 1: unnotice (id-qt-unnotice)
 userNotice:
 explicitText: Identifies X.509 authentication certificates issued for the italian National Service Card (CNS) project in according
to the italian regulation
 Policy 2:
 ID: OID del Certificatore
 Qualifier 1: cps (id-qt-cps)
 CPS uri: <https://www.capki.it/PrivateCA/CNSCPS>
 Key Usage*: Digital Signature
 Extended Key Usage: Client Authorization
 Authority Key Identifier: 0xea3e2ce0 c724083f 97563685 e8b85cbd 4bba9e30
 CRL Distribution Points:
 Distribution Point 1:
 Uniform Resource ID: <https://www.capki.it/Certificatore/CRL3>
 Subject Key Identifier: 0x44a0ff7c f5592ca6 63da6059 490ac1ce 337ecc2a
SIGNATURE:
 ALG. ID: id-sha1-with-rsa-encryption
 PARAMETER: 0
 VALUE: 0x6c3e208d 1d9bea97 31757b54 b752678f
 1002426b a5e403d5 f5368d51 fce72a97
 4040731e e0601ead e1c34a46 a7d0c305

Appendice 2

Protocollo d'intesa del 13 maggio 2003

Protocollo d'intesa per la realizzazione dei progetti Carta d'identità elettronica e Carta nazionale dei servizi

Vista la legge 16 giugno 1998, n.191 e, in particolare, l'art.2, comma 4, che ha sostituito l'art.2, comma 10, della legge 15 maggio 1997, n.127;

Visto il regolamento, emanato con decreto del Presidente del Consiglio dei Ministri 22 ottobre 1999, n. 437, che disciplina le caratteristiche e le modalità per il rilascio “della carta di identità elettronica e del documento elettronico” ;

Visto il decreto del Ministro dell'interno 19 luglio 2000, recante: “Regole tecniche e di sicurezza relative alla carta d'identità e al documento d'identità elettronici”;

Visto il decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, recante: “Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa” e, in particolare, l'art.36, concernente la carta di identità e i documenti elettronici;

Vista la direttiva 1999/93/CE del Parlamento europeo e del Consiglio del 13 dicembre 1999 relativa ad un quadro comunitario per le firme elettroniche;

Visto il decreto legislativo 23 gennaio 2002, n.10, recante: “Attuazione della direttiva 1999/93/CE relativa ad un quadro comunitario per le firme elettroniche”

Considerato che:

- il Governo ha posto la realizzazione dell'e-Government tra gli obiettivi primari da raggiungere;
- la prima fase di sperimentazione del progetto "Carta d'identità elettronica", nel corso della quale sono state rilasciate 170.000 carte, si è conclusa con successo nel 2001 e il Ministero dell'interno ha varato la seconda fase;
- il Ministro per l'innovazione e le tecnologie ha avviato il progetto "Carta nazionale dei servizi" per accelerare la diffusione dei servizi in rete, offrendo agli Enti pubblici l'opportunità di fornire ai cittadini carte a microcircuito che consentano l'identificazione "on line" e siano pienamente compatibili con la carta d'identità elettronica

Ritenuto che:

- è essenziale, per lo sviluppo dei progetti di e-Government, l'identificazione in rete dei cittadini attraverso carte a microcircuito (carta d'identità elettronica e carta nazionale dei servizi);
- è necessario assicurare l'accesso ai servizi in rete attraverso l'utilizzo di carte diverse, prodotte secondo i principi della libera concorrenza, assicurando, nel contempo, la piena interoperabilità tra le funzioni proprie delle carte e i servizi;
- il progetto pilota Netlink ha posto le basi per lo sviluppo della carta sanitaria, che consentirà di usufruire dei servizi sanitari nazionali utilizzando le carte a microcircuito;
- in ambito comunitario, nel contesto del piano d'azione eEurope, l'iniziativa eEurope Smart Cards (eESC) ha studiato le problematiche inerenti le carte a microcircuito multi-uso e ha prodotto la documentazione "eESC Common Specifications for interoperable multi-application secure smart cards v2.0";
- le imprese che hanno sottoscritto il presente Protocollo d'intesa rappresentano il mercato europeo delle carte a microcircuito e sono impegnate a sostenerne la crescita, nonché ad assicurare l'interoperabilità tra le carte partecipando attivamente ai lavori in materia di standardizzazione in ambito europeo e nel più ampio contesto internazionale.

tutto ciò premesso e considerato

IL MINISTRO PER L'INNOVAZIONE E LE TECNOLOGIE

Dott. Lucio Stanca

IL SOTTOSEGRETARIO DI STATO ALL'INTERNO

Sen. Antonio D'Alì

e

la società CardNet Group S.p.A. , Via Marconi, 8 - 20020 Arese (MI),
nella persona del Presidente, Dott. Stefano Camilleri, nato a Joppolo Gianca-
xio (AG) il 1 gennaio 1935, residente in Milano;

la società Gemplus SA, Avenue du Pic de Bertagne, Parc d'activité de Gemenos, 13881 Gemenos (France),
nella persona del FSS Sales Manager Italy, Dott. Paolo Magri, nato a Milano il 16 settembre 1960, residente in Milano;

la società Ghirlanda S.p.A., Via Gonzaga, 7 - 20123 Milano,
nella persona dell'Amministratore Delegato, Sig. Ettore Ghirlanda, nato a Magenta (MI) il 15 giugno 1967, residente in Milano;

la società Giesecke & Devrient GmbH, Prinzregentenstrasse, 159, D-81677 München,
nella persona dell'Executive Senior vice President, Dott. Jürgen Moll, nato a Urach-Wittlingen (Germany) il 27 ottobre del 1952, residente in Sauerlach;

la società Incard S.p.A., Via F. Caracciolo, 15 - 80122 Napoli,
nella persona dell'Amministratore Delegato, Ing. Simone Cavallo, nato a S. Nicola la Strada (CE) il 19 giugno 1962, residente in Caserta;

la società Oberthur Card Systems Italia s.r.l., Via Monte Spluga, 58 - 20021 Baranzate di Bollate (MI),
nella persona dell'Amministratore Delegato, Dott. Angelo Giuseppe Cogliati, nato a Milano il 28 settembre 1966, residente in Milano;

la società Orga Card Systems (Italia) s.r.l., Via Benedetto Croce, 19 - 00142 Roma,
nella persona dell'Amministratore Delegato, Dott. Gilberto Tonali, nato a Roma il 24 agosto 1948, residente in Roma;

la società SEMA S.p.A., Viale Carlo Viola, 76 – 11026 Pont-Saint-Martin (AO),
nella persona del Vice President & Managing Director Mediterranean Geo-Market, Ing. Luigi Giacalone, nato a Firenze il 20 novembre 1955, residente in Roma;

la società Siemens Informatica S.p.A., Via Vipiteno, 4 – 20128 Milano,
nella persona dell'Amministratore Delegato, Sig. Valentino Bravi, nato a Pavia il 10 marzo 1957, residente in Pavia.

CONVENGONO QUANTO SEGUE

ART. 1 – AMBITO DI APPLICAZIONE

Il presente Protocollo d'intesa riguarda la fornitura di carte a microcircuito destinate ad essere utilizzate nei progetti Carta d'Identità Elettronica (di seguito denominato "CIE") e Carta Na-

zionale dei Servizi (di seguito denominato “CNS”), nonché in ogni altro progetto che faccia riferimento alle specifiche tecniche relative alla CIE e alla CNS.

Il presente protocollo è aperto all’adesione di tutti i soggetti interessati.

ART. 2 – OGGETTO DELL’ACCORDO

Il Ministero dell’interno e il Ministro per l’innovazione e le tecnologie e le imprese firmatarie stabiliscono di avviare una comune azione per lo sviluppo di servizi nel campo della identificazione e della autenticazione elettronica.

A tal fine:

- il Ministero dell’interno e il Ministro per l’innovazione e le tecnologie si impegnano a sostenere lo sviluppo di progetti concernenti la CIE e la CNS, promuovendone la diffusione e offrendo un supporto ai fini dell’efficienza dei servizi connessi da erogare
- le imprese firmatarie si impegnano a garantire l’indipendenza tra i servizi e i dispositivi (carte a microcircuito), al fine di incoraggiare il più possibile l’adesione generale ai sistemi di identificazione e di autenticazione in rete, nonché ad altri servizi basati su carte a microcircuito evitando, in pari tempo, di vincolare sviluppatori e utenti all’uso di specifici dispositivi.

ART. 3 – GRUPPO DI LAVORO

Le imprese firmatarie concordano sull’opportunità che il Ministero dell’interno e il Ministro per l’innovazione e le tecnologie istituiscano un apposito Gruppo di lavoro - del quale saranno chiamate a fare parte - con il compito di sviluppare regole comuni orientate a garantire l’indipendenza tra le applicazioni e i sistemi operativi delle carte e l’efficacia dei servizi connessi.

Nello svolgimento della propria attività detto Gruppo di lavoro organizzerà periodiche riunioni che si svolgeranno a Roma.

Le decisioni del Gruppo di lavoro terranno conto degli *standard* disponibili e degli orientamenti propri di altri progetti presenti nell’ambito dell’Unione europea relativi allo stesso settore, nonché dei vincoli che hanno caratterizzato la fase di avvio dei progetti CIE e CNS.

I risultati conseguiti dal Gruppo di lavoro potranno essere utilizzati ai fini della definizione di ulteriori specifiche relative ai progetti CIE e CNS che dovranno, comunque, essere rispettate per poter partecipare alle procedure di gara per la fornitura di carte a microcircuito per i progetti CIE e CNS.

ART. 4 – SPECIFICHE DEL SISTEMA OPERATIVO DELLE CARTE A MICROCIRCUITO

Le imprese firmatarie convengono di implementare le specifiche del sistema operativo della carta a microcircuito (APDU) riportate in allegato.

Le imprese firmatarie riconoscono che i documenti allegati accolgono le indicazioni del Gruppo di lavoro previsto dal precedente art.3 e tengono, altresì, conto dello stato dell'arte della tecnologia e degli orientamenti del mercato.

Il Ministero dell'interno, il Ministro per l'innovazione e le tecnologie e le imprese firmatarie, si impegnano a promuovere la diffusione delle specifiche allegate, quali modello per la realizzazione di progetti cooperativi nell'ambito dell'Unione europea.

ART. 5 – DIRITTI E OBBLIGHI DELLE IMPRESE FIRMATARIE

Le imprese firmatarie che intendono partecipare alla realizzazione dei progetti CIE e CNS devono pianificare le attività concernenti la realizzazione e la fornitura delle carte a microprocessore in accordo con le indicazioni che verranno date dal Gruppo di lavoro previsto dal precedente art.3 e in conformità alle specifiche APDU allegate.

Le imprese firmatarie cooperano al fine di raggiungere e garantire la piena interoperabilità tra i servizi che si basano su differenti carte a microcircuito.

Le imprese firmatarie riceveranno dai gruppi di progetto governativi informazioni in merito ai tempi di realizzazione e alle linee di indirizzo dei progetti.

Le imprese firmatarie, in sede di partecipazione a procedure concorsuali per la fornitura di carte a microcircuito relative a progetti CIE e CNS potranno dichiarare di aver sottoscritto il presente Protocollo d'intesa, attestando, con l'occasione, l'elevato livello di conoscenza del progetto e la sua aderenza alle specifiche tecniche riportate in allegato.

Le imprese firmatarie saranno debitamente e tempestivamente informate dai gruppi di progetto governativi in merito ad eventuali modifiche relative alle specifiche tecniche riguardanti i progetti CIE e CNS.

ART. 6 – RECESSO

Ciascuna impresa può recedere unilateralmente dall'adesione al presente Protocollo d'intesa dandone formale comunicazione al Ministero dell'interno e al Ministro per l'innovazione e le tecnologie, nonché a tutte le altre imprese firmatarie.

In esito al recesso vengono meno i diritti e gli obblighi previsti al precedente art.5.

ART. 7 – PERIODO DI VALIDITA'

Il presente Protocollo d'intesa sarà efficace per 36 mesi, a partire dalla data di sottoscrizione.

Roma, 13 maggio 2003

IL MINISTRO
PER L'INNOVAZIONE E LE TECNOLOGIE
Dott. Lucio Stanca

IL SOTT. DI STATO ALL'INTERNO
Sen. Antonio D'Alì

La SOCIETA' CardNet Group S.p.A.
(Il Presidente)
Dott. Stefano Camilleri

La SOCIETA' Gemplus SA
(per l'Amministratore Delegato)
Dott. Paolo Magri

La SOCIETA' Ghirlanda S.p.A.
(L'Amministratore Delegato)
Sig. Ettore Ghirlanda

La SOCIETA' Giesecke & Devrient GmbH
(L'Executive Senior vice President)
Dott. Jürgen Moll

La SOCIETA' Incard S.p.A.
(L'Amministratore Delegato)
Ing. Simone Cavallo

La SOCIETA' Oberthur Card Systems Italia S.r.l.
(L'Amministratore Delegato)
Dott. Angelo Giuseppe Cogliati

La SOCIETA' ORGA Card Systems Italia s.r.l.
(L'Amministratore Delegato)
Dott. Gilberto Tonali

La SOCIETA' SEMA S.p.A.
(per l'Amministratore Delegato)
Ing. Luigi Giacalone

La SOCIETA' Siemens Informatica S.p.A.
(L'Amministratore Delegato)
Sig. Valentino Bravi

Appendice 3

Dati presenti sulla CNS

Vengono definiti i dati presenti sulla CNS, descrivendone il contenuto e la codifica. Vengono descritti i presenti all'emissione. Non viene descritta la parte relativa alla struttura Netlink. Tali strutture dati e codifiche sono sviluppate in conformità con le specifiche della Carta d'Identità Elettronica (CIE) al fine di garantire l'interoperabilità tra le due carte.

I dati presenti sulla CNS sono:

Dati personali

- dati personali (MF/DF1/EF.DatiPersonali)
- dati personali aggiuntivi (MF/DF2/EF.Dati_Personali_Aggiuntivi)
- certificato utente (MF/DF1/EF.C_Carta)

Dati carta

- Dati processore (MF/DF0/EF.Dati_Processore)
- ID_Carta (MF/DF0/EF.ID_Carta)

Dati di servizio

- Card Status (MF/EF.CardStatus)
- Memoria residua (MF/DF2/EF.MemoriaResidua)
- Servizi installati (MF/DF2/EF.ServiziInstallati)
- InstFile (MF/DF2/EF.InstFile)

Label

- Chiavi di autenticazione

Dati Personali

EF: MF/DF1/EF.DatiPersonali

Dimensione file: 400 bytes

Contiene i dati dell'utente. I campi per identificazione personale (altezza, atto di nascita,...) non sono utilizzati. Alcuni campi sono opzionali nelle specifiche CNS, come indicato dalla colonna (M(obbligatorio)/O(opzionale)/V(vuoto)).

Dato	Codifica	M/O/V	Dimensione Max	Descrizione
Emittitore	ASCII	M	4	Codice derivante dai seriali standard; Es. per la CNS della Lombardia "6030".
Data di emissione del documento	ASCII	M	8	Formato GGMMAAAA
Data di scadenza del documento	ASCII	M	8	Formato GGMMAAAA
Cognome	ASCII	M	26	
Nome	ASCII	M	26	
Data di Nascita	ASCII	M	8	Formato GGMMAAAA
Sesso	ASCII	M	1	'M' per maschio, 'F' per femmina
Statura (cm)	ASCII	O	0	Presente per compatibilità CIE
Codice fiscale	ASCII	M	16	
Cittadinanza (codice)	ASCII	O	0	Presente per compatibilità CIE
Comune di Nascita	ASCII	M	4	
Stato estero di Nascita	ASCII	O	0	Presente per compatibilità CIE
Estremi atto di nascita	ASCII	O	0	Presente per compatibilità CIE
Comune di residenza al momento dell'emissione	ASCII	M	4	
Indirizzo di residenza	ASCII	O	80	
Eventuale annotazione in caso di non validità del documento per l'espatrio	ASCII	V	0	Presente per compatibilità CIE

Tabella 1 - Definizione Dati Personali

Codifica file dati personali

La codifica utilizzata è coerente con quella della CIE.

Ogni dato è codificato con un campo lunghezza (Len) ed un campo valore (Value)

Il campo Len consiste in una stringa di due caratteri ASCII che codifica in esadecimale la lunghezza in byte del campo Value, allineata a destra, con riempimento di zeri a sinistra.

Esempio: la lunghezza di un campo Value di 10 caratteri verrà codificata con la stringa '0A'

Il campo Value viene codificato con una stringa ASCII.

In testa al file è contenuta l'informazione sulla dimensione totale.

La dimensione totale consiste in una stringa di sei caratteri ASCII che codifica in esadecimale la lunghezza in byte dello spazio utilizzato, allineata a destra, con riempimento di zeri a sinistra. Nel calcolo della lunghezza si prendono in conto anche i 6 byte della lunghezza stessa.

I byte rimanenti nel file rispetto all'allocazione massima vengono settati a 00h.

Per compatibilità con l'anagrafica della Tessera Sanitaria, il file Dati Personali presenta delle differenze nella lunghezza massima dei campi Cognome (80) e Nome (86).

Dati Personali Aggiuntivi

MF/DF2/EF.DatiPersonaliAggiuntivi

Dimensione: 100 bytes

Il file, presente per back compatibility con la CIE, è vuoto, con l' intero contenuto è posto a 00h.

Certificato Utente

MF/DF1/EF.C_Carta

Dimensione: 2048

Identifica l'utente in un'autenticazione.

Il formato è PKCS#1, codificato ASN.1.

Il Common Name ha la struttura:

CF/ID.Hash(DatiPersonali)

dove:

CF = codice fiscale

ID = 16 caratteri di ID carta, come definito più avanti in questa specifica

Hash = operazione di hash SHA-1

DatiPersonali = dati personali come presenti nel file EF.DatiPersonali. Vanno considerati solo i dati utili (escludendo quindi la parte finale riempita a 00h), nella stessa sequenza in cui appaiono nel file, includendo tutti i campi Len.

Dati Processore

MF/DF0/EF.DatiProcessore

Dimensione: 54 byte

Questo file contiene i dati di tracciabilità del chip. Una prima parte viene normata per identificare il produttore del chip e del sistema operativo. Altri campi restano a discrezione del produttore della carta.

All'interno del record i campi sono fissi e il loro significato applicativo è definito dalla posizione.

Dato	Codifica	Y/N	Dimensione (bytes)	Descrizione
Chip Manufacturer	ASCII	Y	2	Definita in ISO 7816
OS Manufacturer	ASCII	Y	2	Definita nelle specifiche governative delle APDU per la CNS
Personalizer	ASCII	Y	2	A partire da '01'
Chip Tracing Data	ASCII	Y	2	'00'
Personalizer Specific Data	Libera	Y	10	Dati di competenza del personalizzatore (es stato carta, lotto,...) - TBD
OS Specific Data	Libera	Y	10	Dati di competenza del produttore del sistema operativo - TBD
Free Data	Libera	N	0	Area libera - Assente

ID Carta

MF/DF0/EF.ID_Carta

Dimensione: 16 bytes

L'ID Carta della CNS è opportuno che coincidano con il numero seriale Netlink..

Le informazioni dettagliate su come costruire il numero seriale sono contenute nel documento NK/4/FNS/T/21/1.0 "Gestione del Serial Number delle Carte Sanitarie" pubblicato sul sito Internet del CNIPA:

<http://www.cnipa.gov.it>.

Card Status

MF/EF.CardStatus

Dimensione file: 20

Utilizzato per marcare lo stato della carta. L'intero file è riempito con 00h.

Memoria Residua

MF/DF2/EF.MemoriaResidua

Dimensione file: 2

Mantiene la dimensione della memoria ancora non utilizzata.

Il valore è in byte, e la codifica è binaria.

Questo valore viene inizializzato in emissione con un valore che potrà dipendere dal fornitore e dal lotto di emissione.

Servizi Installati

MF/DF2/EF.ServiziInstallati

Dimensione file: 160

Mantiene la lista dei servizi installati. In fase di emissione il file è riempito con 00h.

Questo file viene utilizzato per visualizzare la lista dei servizi installati e per la gestione delle applicazioni. Viene scritto dalle applicazioni di caricamento servizi.

Il contenuto del file non è definito da questa specifica ma viene lasciato al gestore dei servizi aggiuntivi.

InstFile

MF/DF2/EF.Inst File

Dimensione file: 128

Contiene le chiavi da utilizzare per l'installazione dei servizi aggiuntivi.

Il contenuto di questo file è

$RSA_{InstPubKey}(KIC | KIA)$

Il padding usato è BT02.

La codifica è binaria.

Label

Sulla carta è presente all'emissione solo la coppia di chiavi di autenticazione.

La label delle chiavi di autenticazione deve essere nota per poter essere usata dagli applicativi o dagli strati software intermedi.

Si fissa il valore della label delle chiavi di autenticazione uguale a "CNS0".