Study on Impact assessment for legislation on mutual recognition and acceptance of e-Identification and e-Authentication across borders SMART 2011/0075 IAV

Final Report

Document title:	Final Report
Reference:	D5
Version:	5.0
Status:	Final
Date:	25.06.2012
Author[s]:	Nathan Ducastel, Robbert Fisher, Daniel Gehrt, Theo Hooghiemstra, Luca Alessandro Remotti, Bas van Schoonhoven, Tijs van den Broek, Ron van Paassen
Changes:	-
Reason for Changes:	
Reviewed:	Luca Alessandro Remotti
Authorised:	-

INTRASOFT INTERNATIONAL

TNO innovation for life

Table of Contents

Table of Figures

EXECUTIVE SUMMARY

The purpose of an impact assessment is to help structuring and developing policies, identifying and assessing the problems at stake and the policy objectives pursued.

Impact assessments help identifying the main options for achieving the objectives and analyses their likely impacts in the economic, environmental and social fields. It outlines advantages and disadvantages of each option and examines possible synergies, trade-offs and potential impacts.

The study has taken into account different economic, social and environmental correlations and effects, all considered in relation to eID.

After designing the impact assessment framework, based on a number of assumptions as well as on inquiry questions, indicators and sources, a wide-ranging analysis of the eID domain was undertaken. This analysis focuses on the construction of a conceptual framework of the scenario of cross-border eID and eAuthentication and of the relevant services which build on these enablers.

The analysis has considered different assumptions and impact dimensions:

- The confirmation of the "appropriateness to act" on the part of the EU to regulate cross border eID and eAuthentication
- The demand issue of eID, considering the situation of cross-border services based on eID and in general the demand of EU citizens
- The limitations and obstacles the absence of cross-border regulation will bring about for the take-up of cross-border eID and cross-border eID and services
- The relationship between the take-up of cross-border services requiring eIDs and the development of cross-border eID and eAuthentication itself
- The relationship between trust and the development of cross-border eID, trust being a main factor for the adoption of cross-border eID
- The difference across EU Member States in solving organisational and regulatory issues of eID
- The difference across EU Member States in solving technical issues of eIDs and eAuthentication
- The issue of liability and the way its regulation fosters or hampers mutual recognition and acceptance of cross-border eID and eAuthentication
- The different options for the implementation of cross-border eIDs – eID levels – and the way these could facilitate mutual recognition and acceptance by EU Member States
- The risk of citizens exclusion of businesses or individuals because of the selective acceptance of eID schemes by Member States
- The unique association of one or more eIDs with one physical or legal person and the role of EU Member States in guaranteeing this unique association
- The usability of private sector issued eIDs in the interaction with eGovernment or public online services
- The use of national eIDs by the private sector
- The potential critical mass of use of national eIDs in the private sector
- The trends of diffusion of cross-border eIDs in the short and mid-term
- The assessment of the costs and benefits of a generalised cross-border mutual recognition and acceptance of formal eIDs.
- The issue of "supervision" and the supervision role of the European Commission in matters related to cross-border eID and eAuthentication.

Methodologically, the above impact dimensions have been structured in an assumption matrix which guided the field work and inquiries to:

understand the "phenomenon" of eID and of cross-border eID in Europe;

describe the basic concepts which determine what it is and how it develops;

define from a qualitative and quantitative point of view characteristics, solutions, demand, costs, economic and social impacts;

relate the findings to the policy options

propose the pros and cons of each option and to come to some reasoned conclusion.

The present study has collected fact based evidence to support the impact assessment of the different policy options according to the real-life scenarios of regulation, deployment and use of eIDs and eAuthentication in cross-border public or eGovernment services in the European Union.

The present report provides a comprehensive conceptual framework for eIDs and eAuthentication, and fact-based data and indications on each of the four eID options:

- Option A: keep the status quo, proposing no policy change. This option is also the baseline for the assessment of the other possible policy options and their impacts, to evaluate the socio-economic impact for the digital single market in terms of opportunities missed to create economies of scales and benefits lost for citizens and businesses
- Option B: support the formulation and implementation of legislation on cross-border mutual recognition and acceptance of national eIDs to enable citizens and businesses to use their "national" eIDs not only in their home country but in all other Member States. This option will be developed for different scenarios and implementation options.
- Option C –cease all EU activities in the field of eID, including those already started. This option would also affect eID related initiatives supported in the context of CIP ICT-PSP, such as STORK or future large scale projects concentrated on eID, as well as stop any legal and political action in the field of eID cross-border interoperability and Member State cooperation and coordination.
- Option D: Out of the box measures, including other legal measures or a mix of legal and soft instruments considered appropriate to support the eID interoperability.

The study provides a coherent analysis of regulatory, institutional, organisational and technological issues related to the development of interoperable cross-border eIDs. Furthermore, it considers the four options in terms of their potential impact on the development of the digital single market in general, and of their support to the cross-border access to public services. The different options are compared with the specific development goals of current policy initiatives.

1 INTRODUCTION

1.1 Purpose

The present study has the purpose to identify and analyse different policy options for the cross-border use of eID and eAuthentication in the European Union.

A set of possible options and sub-options have been identified in the terms of reference. these are:

1) Keep the status quo and refrain from any specific regulation of eID interoperability and mutual recognition (Option A)
2) Provide a comprehensive set of rules which would allow the smooth cross-border use of eIDs for EU services (Option B), in particular considering
    a. The mere regulation of eIDs (B1)
    b. The cross-sector use of eIDs (B2)
    c. To guarantee a eID to every citizen in Europe (B3)
3) Cease all eID-related activities in Europe, not only refraining from regulating its cross-border ues, but also ceasing any policy support to pilot activities and experimental and validation actions of eID systems and the related cross-border services, leaving the implementation to the initiative of the Member States of the EU and the private organisations wishing to invest in cross-border services at large
4) Work some out of the box policy options.

It needs to be clarified that eID is needed only in association with online services. For the EU, the cross-border dimension of these services is of absolute importance, according to the subsidiarity principle. The importance and urgence to have an interoperable system of mutually recognised eIDs is therefore not important in itself, but in relation to the availability of cross-border (public) services.

The demand of eIDs is therefore directly dependent on the availability of these services.

1.2 Structure of the report

Apart from this introductory section, this final report follows the structure of the Study Terms of References.

- Section 1 presents the methodologies and approaches used in the analysis and the different sources and techniques used. In this section some references to analysis activities are made, but for any in-depth discussion of the field work the reader should refer to the subsequent sections.
- Section 2 addresses the problem definition, i.e. the fundamental concepts of the study on eID, the qualification of what eID is. Furthermore it presents the policy setting within which the eID-related policy action is embedded, starting from the more general EU policy documents and proceeding to the more particular, specifically focusing on eID and the related cross-border services. The more general principles of the EU policy making, such as
    - The cross-border focus, of the policy action;
    - The subsidiarity principle of the interventions,

  Were given for granted.

  The policy documents relevant to the issue of eID are the Europe 2020 strategy, the Digital Agenda for Europe, the Single Market Act, the European eGovernment Action Plan. Following these policy documents, the section also discusses the role of eID and eAuthentication as key enablers for cross-border services, and in particular of services of public interest, their setting at the European Union level and reflections of the cross sector use of eID. Section 2 also discusses

the STORK project in depth, on of the large-scale pilots supported by the CIP ICT-PSP programme[1], since in its different editions it a key European initiative focused on cross-border eID and the relevant policy making. Furthermore the report provides and overview of national eID systems, in particular considering on those participating in the STORK Large Scale Pilot.

- Section 3 presents the Objectives of the eID and eAuthentication study, as well as the associated general policy objectives and the specific operational objectives.
- Section 4 presents the policy options, as set out in the terms of reference, and their EU policy making aspects, a general assessment, reasoning on the effectiveness, as well as overall conclusions.
- Section 5 is focused on the analysis of the impacts of the different policy options.
- Section 6 compares the shortlisted options
- Section 7 proposes an approach to monitoring and evaluation of European eID-related activities
- Section 8 is about the concluding remarks.

The annexes include all the factual and technical material used for the study, a Glossary, as well as the main analytical tools: the assumption matrix developed, the exploratory questions, the approach to the questioning of CIP ICT-PSP large scale pilots (the LSPs), as well as the bibliographic references.

[1] Community Innovation Programme, ICT Policy Support Programme

2 SECTION 1: METHODOLOGY (SUMMARY OF THE METHODOLOGY USED TO YIELD THE STUDY RESULTS).

2.1 Introduction

The methodology developed for this short-term study was essentially based on

a) A structuring tool – the assumption matrix – which has served the purpose to identify the key questions and assumptions related to the policy making issues of eID and eAuthentication and their cross-border mutual recognition in Europe.
b) A desk research methodology, which was used to develop the overall EU policy framework as well as to investigate the key qualitative and quantitative features of the eID and eAuthentication scenario in Europe. The desk research methodology was based on the assumption matrix to identify and analyse the key EU policy documents relevant for the development of the European Single Market, the Digital Single Market, the European eGovernment Sector and the Digital Agenda. It was also used to identify the key data sets highlighting the main quantitative trends in eID and eAuthentication and eGovernment-related services.
c) The analysis of the public consultation on eIDs and eAuthentication as well as the SME panel. The analysis of the public consultation and of the SME panel was based on the quantitative evidence from the questionnaires. Furthermore there were a number of "open" responses which were reviewed and analysed.
d) The focus group technique, which is a well-established method in the social sciences. It is based on a small group guided discussion. Focus groups are an efficient means to collect information by covering a larger number of interviewees in comparison to single face-to-face interviews. The particular strength of focus groups is that participants discuss their opinions and experiences and explain them to each other. The outcome of focus groups is often a kind of 'negotiation' of opinions where group dynamics play an important role. During the focus group session the opinions of participants are articulated, defended and also collectively shaped through the communication with others.
e) Individual interviews, in particular with the managers, the stakeholders and players of the CIP ICT-PSP large scale pilots (LPS):
    a. STORK, specifically aimed at eID and its pilots, ePSOS, eCodex, PEPPOL, SPOCS[2]. Here a a specific analytical approach was developed to capture not only the achievements of the Large Scale Pilots themselves, but also elaborating the points of view on eID and eID-based services and their development.

2.2 Conceptual approach

The methodological guide was the assumption matrix and analysis framework, as included in the appendix. Due to the lack of data directly related to eIDs and eID-related services a cascade approach was adopted to scale up available data. A methodologically sound assessment of cross-border eID is to look at eIDs as enabling factor for the establishment secure cross-border services.

[2] STORK: Secure Identity Across Borders Linked. Cross border eID management
ePSOS: Smart Open Services - Open eHealth Initiative for a European Large Scale Pilot of Patient Summary and Electronic Prescription.
eCODEX: e-Justice Communication via Online Data Exchange.
PEPPOL: Pan European Public Procurement OnLine
SPOCS: Simple Procedures Online for Crossborder Services

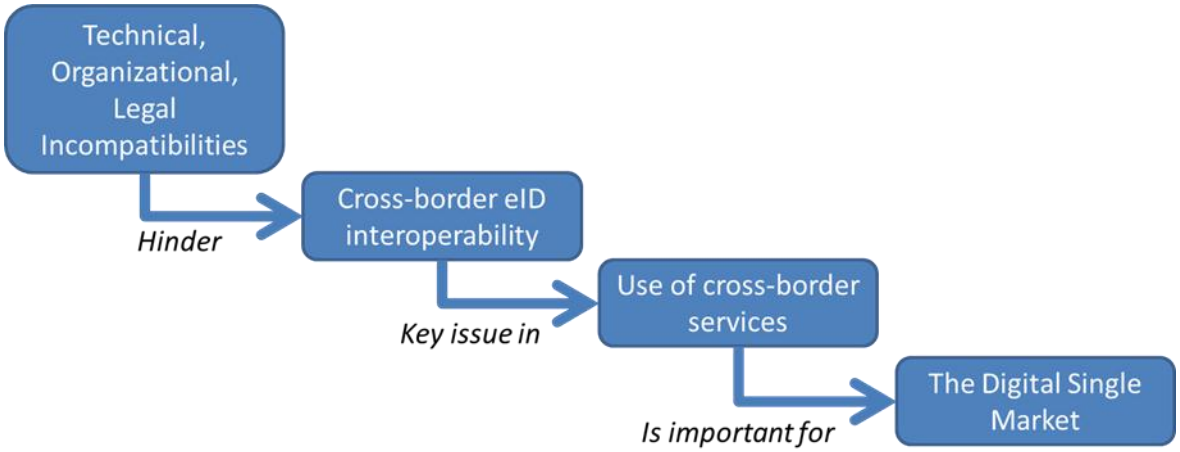


Figure 2-1: The scaling-up model

The scaling-up model was based on existing information and on the projection of available data on a broader scope, as follows:

- Current cross border use of eID: identification and collection of data on use. Identification of and collection of data on eID services. Sources
  - Stork pilots and sub pilots
  - eGovernment applications
- Current bilateral cross-border use of eID: identification and collection of data and of bilateral cross-border eID use and eID based services
  - Estonia
  - Portugal
- National usage statistics of eID and of eID-based applications
- Private and public services based on eID at EU level
  - The Emission trading system
  - online gambling systems, where identity and age verification are needed.
  - EU-level eGovernment services.

The scaling up process included an analysis of the hampering factors, hindering the operation of cross-border eID and the related survey, the analysis of the issue of cross-border interoperability, identifying the key factors – legal, technological, operational, procedural – which are at the basis of interoperability. The next step in the scaling up process concerns the use of cross-border services, which is an important indicator for the completion of the digital single market.

2.3 The Assumption Matrix and the Assessment Framework

The assessment framework is the tool to guide the entire analysis for the impact assessment. It is provided in form of a matrix to construct a hierarchy of assumptions, assessment dimensions, analytical questions, Evidence required/potential indicators, Main analytical method, and Main sources of information.

The matrix is used to map the entire analysis and to ensure consistency and integration of the different analytical and synthesis parts of the assessment work.

The rigorously mapped hierarchy ensures that every assumption is further specified by one or more analytical dimensions and then is related to one or more research questions, to find specific evidence and/or variables.

Each type of evidence or variable is related to a specific analytical method and relates to one or more sources of information.

- The **assumption** describes a all the relevant issues to be examined or a policy objective. It can also concern a general institutional issue, such as, for example the justification for action. Assumptions also concern overall dimensional issues. Assumptions are worked out of the overall policy framework concerned, through a detailed analysis of the statements of policy documents. Assumptions follow a specific hierarchy from the "general" to the "particular".
- The **assessment dimension** helps the additional specification of the assumption, identifying certain elements which constitute the initial assumption. In case of quantitative assumptions the assessment dimensions specify different items to be measured.
- The **analytical question** is the way to explore the issue(s) related to the assumption or the specific assessment dimension(s). It is a concrete question which will be asked directly or indirectly when doing the review of documents or during the field work or case studies.
- The **evidence or the indicator** is the means to qualify the analytical question. For the present study the main sources of information are the documentary and literature reviews, as well as the focus group approach. For these interview and focus group guidelines were developed, which allow for sufficient flexibility in the approach. Indicators will also help to research specific quantitative elements, collecting the relevant available data and information.

2.4 Desk Research

Desk research has been carried out on policy documents and on statistical reviews.

The first set of documents include the main eID-related policy documents

- EUROPE 2020 - A strategy for smart, sustainable and inclusive growth, Communication from the Commission. COM(2010) 2020 final
- A Digital Agenda for Europe. Communication from the Commission. COM(2010) 245 final/2.
- The European eGovernment Action Plan 2011-2015. Communication from the Commission. COM(2010) 743
- Single Market Act. Twelve levers to boost growth and strengthen confidence "Working together to create new growth". Communication from the Commission. COM(2011) 206 final

The second set of documents include statistical and economic data from studies and documents and reports such as the SSEDIC[3] report, the OECD and EUROSTAT[4].

Other important sources of information were the experiences gained in the context of the STORK project which could provide indicators on technical and legal interoperability. However, other

[3] "SSEDIC Deliverable Report" (Final Report of SSECID, Project co-funded by the European Commission within the ICT Policy Support Programme), by is-practice, 2011

[4] "Computer skills in the EU27 in figures", Eurostat news release, 26/03/2012, http://epp.eurostat.ec.europa.eu/cache/ITY_PUBLIC/4-26032012-AP/EN/4-26032012-AP-EN.PDF, last accessed on 28/05/2012
"eIDs in Europe: Not (yet) yielding profits for the cross-border financial services sector", 07/09/2010, http://www.dbresearch.com/PROD/DBR_INTERNET_EN-PROD/PROD0000000000262236.pdf, last accessed on 28/05/2012
"ICT usage in enterprises 2010", Eurostat *Data in focus*, no. 49/2010, http://epp.eurostat.ec.europa.eu/cache/ITY_OFFPUB/KS-QA-10-049/EN/KS-QA-10-049-EN.PDF, last accessed on 28/05/2012
"The Role of Digital Identity Management in the Internet Economy", 2009, OECD

authoritative sources not directly related to STORK that may or may not take the same views were utilised, in order to get a complete picture .

A number of other sources, other than those mentioned above, the Public Consultation and the SME panel are discussed hereinafter

- European Business Test Panel on Cross-Border Public Procurement (2011). In so far eIdentification is one of the key enablers for cross-border public eProcurement; this survey has provided indicators of untapped demand due to lack of cross-border eIdentification.
- European Business Test Panel on Business Obstacles in the EU Internal Market (2011). In so far a lack of cross-border eIdentification (or services for which eIdentification is a key enabler) is mentioned as an obstacle to the Single Market, this has provided relevant indicators.
- The OECD report on the role of eIDM in the Internet Economy (June 2009) was used to get some indication on the potential untapped demand for eIdentification.
- The Copenhagen Economics report "The Economic Impact of a Digital Single Market" (2010) provides information on the potential economic impact of cross-border eIdentification.
- IPTS did a study in 2010 on "The State of the Electronic Identity Market" that has provided indicators on demand for cross-border eIdentification-enabled services.
- Related to STORK, some projects such as the PROCURE project has provided information about how cross-border eIdentification – or the lack thereof – is an obstacle to services such as cross-border eProcurement in Europe[5].

2.4.1 Statistical sources

1) Eurostat
   a. *eGovernment*
      i. E-government on-line availability (up to 2010) http://epp.eurostat.ec.europa.eu/tgm/table.do?tab=table&init=1&language=en&pcode=tsiir120&plugin=1
      ii. Individuals using the Internet for interaction with public authorities (up to 2011) http://epp.eurostat.ec.europa.eu/tgm/table.do?tab=table&init=1&language=en&pcode=tin00012&plugin=1
      iii. Individuals using the Internet for interaction with public authorities, by type of interaction (up to 2011) http://epp.eurostat.ec.europa.eu/tgm/table.do?tab=table&init=1&language=en&pcode=tin00013&plugin=1
      iv. E-government usage by individuals by gender (up to 2010) http://epp.eurostat.ec.europa.eu/tgm/table.do?tab=table&init=1&language=en&pcode=tsiir130&plugin=1
      v. Enterprises using the Internet for interaction with public authorities (up to 2010) http://epp.eurostat.ec.europa.eu/tgm/table.do?tab=table&init=1&language=en&pcode=tin00107&plugin=1
      vi. Enterprises using the Internet for returning filled in forms to public authorities (up to 2010) http://epp.eurostat.ec.europa.eu/tgm/table.do?tab=table&init=1&language=en&pcode=tin00108&plugin=1

[5] In this respect eProcurement is among the

vii. Enterprises using the Internet for submitting a proposal in a public electronic tender system to public authorities (up to 2010) http://epp.eurostat.ec.europa.eu/tgm/table.do?tab=table&init=1&language=en&pcode=tin00109&plugin=1

b. eCommerce

i. Individuals using the Internet for ordering goods or services (up to 2011) http://epp.eurostat.ec.europa.eu/tgm/table.do?tab=table&init=1&language=en&pcode=tin00096&plugin=1

ii. Individuals using the Internet for ordering goods or services from other EU countries (up to 2010) http://epp.eurostat.ec.europa.eu/tgm/table.do?tab=table&init=1&language=en&pcode=tin00003&plugin=1

iii. Individuals using the Internet to buy or order online content (up to 2010) http://epp.eurostat.ec.europa.eu/tgm/table.do?tab=table&init=1&language=en&pcode=tin00080&plugin=1

2) OECD. "The Role of Digital Identity Management in the Internet Economy: A Primer for Policy Makers"

3) eGovernment Benchmark[6]: 7th eGovernment Benchmark Measurement), by Capgemini; 8th eGovernment Benchmark Measurement), by Capgemini, Rand Europe, IDC, Sogeti and DTI, for the European Commission, DG InfSo, 2009; 9th eGovernment Benchmark Measurement), by Capgemini, IDC, Rand Europe, Sogeti and DTI

2.5 The Analysis of the Public Consultation on eIDs and eAuthentication

As a starting point, the SME[7] Panel on eSignature and eID and the Public Consultation on eID, eAuthentication and eSignatures organized by the European Commission was analysed. However, other sources were considered to verify the assumptions.

The detailed analysis and presentation of the statistical results of the consultations is included in the annex (see chapter 9).

2.5.1 The Public Consultation

The Public Consultation on electronic identification, authentication and signatures was aimed at key players from civil society, industry, business sector, academia and public administrations closely involved in the development and deployment of e-identification, e-authentication and e-signatures. The purpose of the public consultation was "to provide input for policymakers on how electronic identification, authentication and signatures can contribute to deliver the European digital single market."

It was held from February-April 2011, and received a total of 434 contributions. Of these, 417 respondents contributed via the online tool and 17 respondents contributed via email; only the respondents that used the online tool were used for statistical analysis. Little less than half of these responses were on behalf or an organization such as a large or small private company, a public authority or an industry association. The rest of the responses received were by individuals.

An analysis of the consultation results was made available. This analysis was further refined to develop some indicators for the present study, using the full data set of the survey.

[6] "Digitizing Public Services in Europe: Putting ambition into action" (9th eGovernment Benchmark Measurement), by Capgemini, IDC, Rand Europe, Sogeti and DTI, for the European Commission, DG InfSo, 2010

[7] Small & Medium Enterprises

The Public Consultation contained six specific questions (18-22 and 25) on eIdentification and eAuthentication. The remaining ones concerned the wider issue of eSignatures, eIdentification and eAuthentication as a whole.

2.5.2 The SME Panel

Another survey launched by the Commission explicitly aimed at small to medium enterprises (SMEs). This survey provided an opportunity for enterprises to give their opinion on how new legislation on eIdentification and eSignatures could meet their needs.

The SME Panel was held from October-December 2011, and had a higher response than the Public Consultation: 1251 responses were received, of which 11% were by companies consisting of 1 person (i.e. individual entrepreneurs). 3 questions were exclusively about eIdentification, but no specifically on cross-border eIdentification. The detailed analysis of the results of the SME Panel are provided in chapter 10.6.4 . Furthermore the figures of the elaborated statistical data are referenced in the paragraphs assessing the different options.

2.6 The focus group with the European Commission

As mentioned, the method of focus groups is based on a small group discussion and well-established in social sciences. Focus groups can be efficiently used to collect information by covering a larger number of interviewees in comparison to single face-to-face interviews. The risk of bias is reduced by the involvement of different stakeholders. Within a short period of time rich and varied information on the topic is distilled. Possibly, the different opinions of participants lead the discussion to a new perspective and open up linkages which would not have been identified in more quantitative approaches such as surveys.

The focus group serves was useful to gather viewpoints and opinions from policy experts of the European Commission and to exchange views on the key assumptions on eIdentification and eAuthentication, related issues and on possible solutions.

2.6.1 The questions discussed

The study team established a comprehensive set of questions according to the overall evaluation objectives set out. these objectives concerned the different policy options and The analysis has been developed along the following different.

1) Option C: No eID EU policy at all and halt of any eID-related initiative
   a) Could a generic infrastructure on cross-border formal eID still arise?
   b) Will there be impacts on the internal market?
   c) In terms of social impacts, could the policy approach lead to exclusion of specific groups of EU citizens?
   d) Which groups, and how?
   e) Would this policy approach have an effect on administrative burdens?
2) Option A: Maintaining the status quo
   a) How would the approach put in place by STORK / STORK II / LSPs develop?
   b) Would there be impacts on the internal market?
   c) Will the landscape face increasing fragmentation?
   d) Could this policy approach lead to exclusion of specific groups of EU citizens? Which groups, and how?

e) Could this policy approach lead to a reduced potential for empowerment of EU citizens? In other terms, will the absence of an EU eID regulation lead to a limited EU citizenship? If so, how?
f) How could bilateral agreements impact administrative burdens relating to services based on the cross-border use of eID?

3) Option B: Revision of regulation
   a) Is there a need for a EU-level or MS budget for keeping up and operating the eID approach?
   b) Will there be a real effect on user inclusion?
4) Option D: Soft measures
   a) Partnership with the telecom sector (telecom/internet service providers), to utilize the trend towards identification using mobile technologies
   b) Setup an expertise centre on eIAS
   c) Support standardization of technical, semantical, organizational matters
   d) Operationalize the "building blocks" developed in STORK (i.e. technology push)
   e) Incentivize public administrations – make an inventory of incentives, focus on developing the strongest incentives
   f) Partnership with the banking sector (or the part of it that is government-owned).

2.7 Individual interviews

An interview guideline was developed to ensure the consistency of the interviews and interaction with the key players of the CIP ICT-PSP Large Scale Pilots. The purpose was not to limit the analysis to Pilot achievements and agreements within the consortia, but rather engage the experts in a scenario-building exercise on the perspectives of eID and eID cross-border services. The analysis and interview guidelines included:

1) Documentation on service development scenarios, of demand and demand dynamics
2) The use of eIDs in the service, it's degree of criticality, down to the point that in absence of a general eID availability or regulation proprietary solution will have to be delivered
3) Impact of mutually recognised eIDs on service provision on the service viability
4) The effect of non-regulation on the service provision
5) Cross border dimension of the service
6) The cost model
   a) Investment made
   b) Implementation costs
   c) The operation costs
7) Business model
   a) Number of transactions estimated
   b) Development of transactions
   c) Associated value for each transaction (if any) or procedures that can be completed electronically
8) Economic impacts of the service
9) Estimates on impact on the administrative burden
   a) Cost savings due to simplification
   b) Liability costs
10) For PEPPOL
   a) Impact on public procurement
11) For EPSOS
   a) eHealth transactions and cross-border transactions
   b) Potential cost savings

12) For SPOCS
    a) Impact on business mobility
13) For eCodex
    a) Volumes of transactions per type, and cross-border
    b) Estimate for increase
14) For STORK
    a) Volumes per pilot service trialled
    b) Value per transaction
    c) Economic impact associated

3 SECTION 2: PROBLEM DEFINITION

3.1 What is eID

e-identification and e-authentication (referred to as 'eIAS services' together with eSignatures) are the electronic equivalent of personal identification and validation of personal identification. In simple terms, these perform the same functions in an electronic environment as in the paper world: a person provides his/her name (identification) and proves through the presentation of evidence (such as a passport or identity card) the correctness of the data provided (authentication). Electronic identification and electronic authentication have not yet been unequivocally defined in EU-acquis, but relate respectively to processes that aim to determine who a person is (identification) and to confirm that a person is who he claims to be (authentication)[8].

eIDs are systems which have specific institutional, procedural and technological characteristics which vary from country to country. This means that they operate according to national rules: the "definition" of personal identity, the concerned institutions issuing eIDs, managing the database(s) and the underlying authentication and security technologies. Creating interoperable eIDs and mutual recognition and acceptance of national eIDs requires a common regulatory framework, on recognition and acceptance between all Member States. The willingness to create interoperability and mutual recognition across borders is the subject of our analysis. Institutionally, the eID systems are usually closely related to traditional ID management, and, subsequently, most likely share some of the procedures and technological resources.

3.2 The EU Policy Setting

The study team elaborated a comprehensive scenario on eID and eAuthentication in relation to cross-border transactions and the hierarchy of EU policies which range from overall integration of the European Union to specific internal market and the digital single market goals.

At EU level, Commission launched initiatives to:

- provide a stable legal framework that stimulate investments in an open and competitive high speed internet infrastructure and in related services. The regulatory initiative includes the review of the eSignature directive. Furthermore, the Connecting Europe Facility for Telecommunications and ICT foresees a huge investment to support investment in fast and very fast broadband networks and pan-European digital services.
- develop an efficient spectrum policy;
- facilitate the use of the EU's structural funds in pursuit of this agenda;
- create a true single market for online content and services (i.e. borderless and safe EU web services and digital content markets, with high levels of trust and confidence, a balanced regulatory framework with clear rights regimes, the fostering of multi-territorial licences, adequate protection and remuneration for rights holders and active support for the digitisation of Europe's rich cultural heritage, and to shape the global governance of the internet;
- reform the research and innovation funds and increase support in the field of ICTs so as to reinforce Europe's technology strength in key strategic fields and create the conditions for high growth SMEs to lead emerging markets and to stimulate ICT innovation across all business sectors;

[8] See e.g. the definitions established in the Modinis IDM terminology paper; https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/pub/Main/GlossaryDoc/modinis.terminology.paper.v2.01.2005-11-23.pdf

- promote internet access and take-up by all European citizens, especially through actions in support of digital literacy and accessibility.

At national level, Member States are entrusted with:

- drawing up operational high speed internet strategies, and target public funding, including structural funds, on areas not fully served by private investments;
- establishing a legal framework for co-ordinating public works to reduce costs of network rollout;
- promoting deployment and usage of modern accessible online services (e.g. e-government, online health, smart home, digital skills, and security).

Current trends show signs of integration fatigue and disenchantment regarding the single market. The Commission's vigilance and a shared sense of responsibility among Member States have prevented a drift towards disintegration. But a new momentum – a genuine political commitment - is needed to re-launch the single market, through a quick adoption of the initiatives mentioned below. Such political commitment will require a combination of measures to fill the gaps in the single market.

Specific actions tackle bottlenecks in the single market by,

- Reinforcing structures to implement single market measures on time and correctly;
- Pressing ahead with the Smart Regulation agenda, including considering the wider use of regulations rather than directives, launching evaluations of existing legislation;
- Carry forward an appropriate set of legislative measures on eSignatures and mutual recognition and acceptance of eIDs as outlined in the Single Market Act
- Monitoring markets, reducing administrative burdens, removing tax obstacles, improving the business environment, and supporting entrepreneurship;
- Adapting EU and national legislation to the digital era so as to promote the circulation of content with high level of trust for consumers and companies. This requires updating rules on liability, warranties, delivery and dispute resolution;
- Facilitate the contract conclusion in other Member States, specifically considering consumer contracts, EU model contract clauses and by making progress towards an optional European Contract Law;
- Making it easier and less costly for businesses and consumers to enforce contracts and to recognise court judgments and documents in other EU countries.

3.2.1 Europe 2020

The Commission launched the Europe 2020 strategy to react to the economic and financial crisis by "preparing Europe's economy for the next decade"[9]. The three main mutually interrelated drivers identified are:

- Smart growth (knowledge and innovation based economy).
- Sustainable growth (resource efficient, greener and more competitive economy).
- Inclusive growth (high-employment economy delivering social and territorial cohesion).

3.2.2 The Digital Agenda for Europe

The DAE aims at defining the key role of ICT to pursue and achieve the development and integration objectives set out in the Europe 2020 strategy. It defines a plan of action to maximise the impact on the use of ICT. The DAE measures various criteria, some of which are relevant to our study:

- The integration of digital market, of regulations, services and standards
- Interoperability, a legal framework and standards for smooth cross-border electronic exchange;

[9] http://ec.europa.eu/education/focus/focus479_en.htm

- Trust-building in networks and services;
- Increase the exploitation of opportunities of the Digital Single Market.

According to the DAE a digital single market needs to be constructed to make available the benefits of the digital era to the European Union as a whole. In the EU, and globally multiple affect not only access to networks, but also to global internet services and content, thus hampering the potential development of network services and content. The Digital Agenda for Europe identifies a set of Key Priorities tackling these issues. The most significant for the purpose of the present study are

- The revision of the eSignature Directive and legislation on mutual recognition and acceptance of electronic identification across border
- The creation of a straightforward and open environment for online cross-border transactions, eliminating technical and legal constraints
- Building digital confidence, guaranteeing citizens the same rights in the digital and in the physical environment
- Interoperability and standards between devices, applications, data repositories, services and networks to improve ICT standard-setting, promoting better use of standards and enhance interoperability through coordination
- Reaping the benefits of eGovernment for efficient and cost-effective services for citizens and businesses and for a participatory open and transparent government. The DAE particularly emphasises the cross-border dimension of eGovernment. The DAE requires improved administrative cooperation to develop and deploy cross-border public online services as well as practical e-identification and e-authentication cross border services, including mutual recognition of security levels for authentication.

3.2.3 The Single Market Act

The Single Market has been one of the foundations of the European integration and of its economic and social growth. The current policy initiatives have three broad goals[10]

1) Complete the single market
2) Support and promote the functioning single market
3) Launch initiatives to contribute to the completion of the single market.

The policy measures put in place have the objective to increase citizen's confidence in the internal market and disseminating the awareness that the freedom of activities is combined with rules and controls which ensure the certainty of transactions and the guarantee the rights of the involved parties, in particular of the "contractually weaker" parties, such as the individual consumers. A better integrated and regulated market bears not only benefits for individuals, but also constitutes a platform for European competitiveness. The Single Market Act makes a specific reference to the need to ensure the mutual recognition of electronic identification and authentication across the EU with the objective to enable secure, seamless electronic interaction possible between businesses, citizens and public authorities, thereby increasing the effectiveness of public services and procurement, service provision and electronic commerce (including the cross-border dimension). At the same time it stresses that trusted electronic services need to respect privacy, provide legal certainty, ensure that transactions are secure, work across borders and be recognised by all sectors of activity.

[10] A NEW STRATEGY FOR THE SINGLE MARKET. Report by Mario Monti. 9 May 2010.

3.2.4 The Digital Single Market

The DSM is an important element of the EU Single Market which aims at providing citizens and businesses the benefits of a pervasive integration of the digital and the physical world. It caters for the real-time provision of information, of products and services, and has important potential impacts on the overall public and private sectors as well as on the ICT sector, which has a horizontal, cross-sector support function. The development of the Digital Single Market is hampered by the uncertainties in payment security and the enforcement of consumer rights in cross-border transactions, which undermine consumer confidence, but also create serious limitations on the offering on the part of service providers and merchants.

3.2.5 The European eGovernment Action Plan 2011-2015[11]

eGovernment is considered one of the key areas where digital technologies can effectively be deployed to deliver advanced, efficient and effective eServices and providing benefits to citizens and enterprises. In a time of constrained public resources, ICT-enabled online public services can support citizens and enterprises in an innovative way in a more efficient and cost-effective way.

A joint and coordinated action at European level can lead to a more efficient use of resources and to sharing experiences and practices. The four policy priorities of the eGovernment Action Plan are:

- User Empowerment through user-centred and inclusive services
- The creation of the EU internal market, providing seamless cross-border services
- Increase of Efficiency and Effectiveness of Governments and Administrations, Improving Organisational Processes, reducing Administrative Burdens
- Creating the pre-conditions for developing eGovernment, jointly putting in place technical and legal pre-conditions necessary for the diffused deployment of eGovernment services in Europe.

One of the actions envisaged by the Action Plan is that Member States should apply and roll out the eID solutions, based on the results of STORK and other eID-related projects.

3.2.6 eIdentification and eAuthentication as key enablers

The eGovernment Action Plan identifies a number of technical and legal pre-conditions which will enhance the development of seamless European cross border services and enable their implementation. Key enablers such as electronic identification are required to guarantee interoperability, which is the ability of systems and machines to exchange, process and correctly interpret information. It is not limited to technical issues but involve legal, organisational and semantic aspects. One of the actions identified foresees that the Commission will table legislative measures to ensure mutual recognition and acceptance of electronic identification and authentication across Europe.

The eGovernment action plan calls for a better administrative cooperation to develop and deploy cross-border public online services based on robust practical eIdentification and eAuthentication solutions. The Stork large scale pilot co-funded by the Commission in the context of the CIP ICT-PSP programme has developed an identification and authentication platform which enables the cross-border use electronic identifications used in the STORK environment. The platform was tested successfully by setting up real time pilot applications.

[11] COM (2010) 743. 15 December 2010

3.2.7 eID and eAuthentication in the European Union

From the analysis of the principal policy initiatives of the European Union, it clearly appears that eIdentification and eAuthentication services are considered key enablers for the construction of the Digital Single Market.

The Digital Agenda for Europe has recognised that most public online services do not work across borders. In fact, the Second Interim (Final) evaluation of the CIP ICT-PSP programme has demonstrated that the amount of cross-border transactions in the context of the relevant Large Scale Pilots (Pilot As) co-funded under the programme is still limited[12].

However the construction of the Digital Single Market is proceeding, and thus the integration of public services provided across border, also of those which require the use of eID and "national" eIDs.

In the course of the study a number of proxy indicators were identified, which show the current situation in eGovernment services and other public services, as well as in related cross-border services, and which provide indications on the future developments, also related to eID-based services.

These proxy indicators indirectly concern the take-up and development of eID, include:

- eGovernment availability and sophistication
- eGovernment online availability trends
- eGovernment availability per country
- eGovernment services sophistication
- eGovernment take-up
- Percentage of interaction with public authorities
- Percentage of interactions with the purpose of sending filled forms
- eGovernment take-up gap, 2010, by country
- Percentage of interaction with public authorities (in general)
- Percentage of interactions with the purpose of electronic tender submission
- eGovernment services for which eID is optional or mandatory
- Geographical scope of eProcurement platforms
- Sectoral scope of eProcurement platforms
- eProcurement visibility
- eProcurement pre-award process availability

3.2.8 Cross-sector use of eID

The cross-sector use of national eIDs has several faces. On the one hand the policy maker has to decide whether the private sector at large can take full advantage of the "national eID, this "opening up" the eAuthentication systems, i.e.: allowing challenges by private entities. This has a cost and it needs also to be considered that there is a trade-off against using private eID systems. Furthermore there might be additional costs to open up "national eIDs to the private sector which the private sector should be willing to bear, eventually preferring the "national" eID to the private ones. This is related to several factors:

a) the [potential] amount of additional national transactions. This potentiality indicator is related to the increase of available online services which will be enabled by the full establishment of cross-border eID and eAuthentication
b) the additional cross-border transactions and their trend over time, determined by the increased offer of cross-border services as well as the increased mobility of citizens and enterprises with the progress towards the internal market;

[12] http://ec.europa.eu/cip/files/cip/docs/cip_ict_psp_interim_evaluation_report_2011_en.pdf

c) the overall development policies of the private organisation in respect to cross-border transaction (the estimation of the potential catchment area). In other terms the cross-sector development of eID-based services depends on the market drivers and on the incentives, which are the policy measures which induce businesses or individuals, with rules or subsidies, to develop eID-based services.

The use of formal eIDs by the private sector does not face particular issues. It however requires that the formal eID systems introduce procedures to allow the eAuthentication of requests by private entities and develop the appropriate interfaces and applications, as well as the security measures which are needed for open systems.

The key factors for the private-sector take up of formal eIDs therefore depends on:

a) the availability of open technical systems
b) the establishment of clear rules for use of eIDs and for eAuthentication processes
c) the establishment of clear liability rules[13].

The actual potentiality of the private sector use of eID systems however will become clearer once a number of business cases will be developed. At present, JRC/IPTS recognises that there is a "lack of a compelling, well-defined and accepted business case for federated eID. Few organizations or governments are willing to speculatively invest"[14].

3.3 STORK

The CIP ICT-PSP Pilot A Stork

STORK was launched to develop and pilot solutions for the cross border use of eIDs. Thanks to the extensive analytical and policy scenario setting work undertaken by STORK, the Pilot will be used as an extensive case study for the impact assessment.

STORK - Overview

STORK has delivered a solution which facilitates the EU-wide mutual recognition and acceptance of national electronic identifications used in the participating European countries and their authentication (eID via electronic cards or other means). The common specifications which are freely available enable eID-interoperability. It enables businesses and citizens of countries to participating in STORK to securely use their national electronic identifications in the context of the life demos established by STORK.

The pilot project pursues the EU-wide recognition and acceptance of electronic IDs, without imposing one single solution but allowing national systems to work together.

Some real time pilot applications were set up in order to demonstrate cross-border feasibility and interoperability of eIDs of participating countries.. STORK set up the following 6 test pilots:

- 'Cross border authentication platform for electronic services' (a common service architecture allowing citizens of participating countries to use their national eIDs to access e-Government portals across borders),
- 'Safer chat' (a platform for safer online communication for children using eIDs),
- ' Students mobility' (a service facilitating students' mobility across Europe,
- 'eDelivery' (use of eID for cross-border electronic delivery for citizens and businesses),
- 'change of address' (electronic change of address for EU citizens that move to other Member State)s.

[13] Article 23 of the Austrian "Signaturgesetz" foresees the liability as well as the burden of proof for the certification provider (Zertifizierungsdiensteanbieter)

[14] The state of the Electronic Identity market: technologies, infrastructure, services and policies, 2010, JRC/IPTS

- STORK-ECAS integration: The pilot integrates STORK with ECAS, enabling Member States to use their national eIDs to provide authentication and access electronic services delivered by the European Commission (EC)[15].

All European countries, including the Reference Group of those not participating in the project, were consulted during the preparation of the common specifications so that the project with the aim to increase the impact. Industry was involved through the Industry Group and has equal and free access to the common specifications.

Security and privacy were one of the top priorities. As authentication levels for a given application differ across Member States, the project developed "circles of trust" at European scale.

The project has demonstrated the smooth cross-border operation of several key public services tested in the context of the 6 pilot demonstrations. The solution is scalable to all EU Member States, technology-transparent, robust, with measurable benefits, and has been implemented in such a way that it is sustainable beyond the life of the pilot.

As a building block towards the realisation of a digital single market, this project allows to save time and money with safer transactions, less fraud, better control over personal data and simplified procedures.

The contributions of STORK to the cross-border analysis of eIDs

Based on the available STORK documentation the present IA-eID-study will investigate further additional existing material and undertake direct field analysis with the aim to provide an in-depth assessments of the strategic "market" scenarios and concrtee interoperability issues. It will consider

- The potential demand for cross-border public services requiring eID
- The potential demand for cross-border private services requiring eID
- The acceptability of cross-border eIDs and the requirements for recognitions and interoperability
- The actual feasibility of a common level of interoperability of eIDs.

An important part of the analysis for the impact assessment was based in a set of interviews with STORK participants and stakeholders to examine different points of view on the progress made with regard to interoperability, solutions found and the remaining barriers to remove.

Situational Analysis

A comprehensive situational analysis of e-Government and the strategic role position of STORK should effectively address both the internal and external environments as relating to the project so as to better recognize its strengths and weaknesses as well as opportunities and risks. In other words, the study team assessed the potential of Stork to provide a global response to open eID policy issues.

The fact that a significant number of Member States who participate in STORK, that the solution was looked at by the Artcle 29 Working PartyWell, quite a few MS built it together, the solution was looked at by article 29, stork2.0 is based on it and the eSense pilot is supposed to maintain it together with ISA programme. I would think that that is a strong indication.

[15] The STORK-ECAS pilot provides Member States with greater convenience, with the STORK interoperability layer enabling them to use national eIDs to authenticate themselves and gain secure access to electronic services provided by the EC. At the same time this multi-factor authentication will improve the security of these critical important services.
The first phase of the pilot is enabling STORK authentication with CIRCABC - a platform to support collaborative groups with sharing documents and resources in private workspaces – to gain operational experience of the STORK-ECAS integration in a challenging but not business-critical environment. The second phase will introduce further applications including the IMI, the eJustice portal, participants portal for research grants and the Community Independent Transaction Log (CITL) for the EU emission trading system.

A survey conducted by the European Commission in 2007, and published in 2009[16] showed that a majority (28 out of 32) of the countries use or plan to use an electronic ID scheme. While some countries have signed agreements on mutual recognition, eID systems are very heterogeneous and interoperability across borders is almost non-existent. There is an exception represented by the eID mutual recognition of eID: German and Polish pension and social care services now provide for recognition of each other's e-ID, providing an example of a bilateral cross-border mutual recognition. This provides a lower level of functionality compared to EU-wide mutual recognition, but shows the value of such services for communities living close to each other but on either side of national borders[17].

- Out of 32 countries, 15 are issuing national electronic credentials to non-nationals
  - 12 of these countries are creating certificates to non-nationals
  - 1 is planning to start issue certificates to non-nationals.
- Out of 32 countries, 17 are not issuing any form of electronic credentials to non-nationals
- Out of 32 countries, 7 countries are accepting non-national credentials
- Out of 32 countries, 25 are not accepting any form of non-national credential in eGovernment systems

Nonetheless, taking advantage of the latest developments regarding eIDs at Member State level and promoting mutual recognition of electronic identities between Member States moves us closer to seamless online services and higher digital mobility in the EU.

The study has also focused on research and development activities concerning the use of eID and the technical implementation of the eAuthentication systems. These projects include:

- Modinis eID Paper on eID good practices[18]
- eEPOCH[19]: The aim of eEpoch is to demonstrate interoperable and secure smart card based digital identification systems, which provide the levels of trust and confidence necessary for citizens to interact digitally with their national and municipal administrations and other European institutions.
- Government User IDentity for Europe - creating an European standard for interoperable and secure identity management architecture for eGovernment FP6[20]
- "Electronic and Secure Municipal Administration for European Citizens " FP6[21]
- FIDIS[22] (Future of Identity in the Information Society) is a NoE (Network of Excellence) supported by the European Union under the 6th Framework Programme for Research and Technological Development within the Information Society Technologies (IST) priority in the Action Line: "Towards a global dependability and security framework".
- PRIME[23] addresses this issue via an integrative approach of the legal, social, economic and technical areas of concern to build synergies about the research, development and evaluation of solutions on privacy-enhancing identity management (IDM) that focus on end-users. The work plan supports this integration over the project lifetime through multiple iterations of increasing ambition. PRIME elaborates a framework to integrate all technical and non-technical aspects of privacy-enhancing IDM. During and after the project, the framework will act as a lingua franca between all actors and reinforce their roles and responsibilities for full effectiveness. FP6

[16] http://ec.europa.eu/idabc/en/document/6484.html
http://ec.europa.eu/idabc/servlets/Doc2ba1.pdf?id=32521
[17] http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/12/403&
[18] http://ec.europa.eu/information_society/activities/ict_psp/documents/eid_good_practices_modinis_study.pdf
[19] http://cordis.europa.eu/search/index.cfm?fuseaction=proj.document&PJ_RCN=5876687
[20] http://cordis.europa.eu/search/index.cfm?fuseaction=proj.document&PJ_RCN=6526790
[21] http://cordis.europa.eu/search/index.cfm?fuseaction=proj.document&PJ_RCN=6536825
[22] http://www.fidis.net/home/
[23] http://cordis.europa.eu/search/index.cfm?fuseaction=proj.document&PJ_RCN=6569384

- IDA(BC)[24] Authentication Policy. With electronic exchanges of information taking place across Europe every day, security is becoming an increasingly important issue. Security can be tackled by ensuring that exchange takes place over a secure channel, but also by guaranteeing that the identity of the persons exchanging information is known and authenticated. In order to facilitate the exchange of information over sectoral networks or Projects of Common Interest (PCIs) in a reliable and secure manner, IDA has set up a horizontal security measure to develop an authentication policy.

An important line of analysis aimed at identifying how to incorporate the findings of the EU co-funded project STORK into the A2A online applications operated by the European Commission. Several of these are described in the following by way of example with particular attention to the European Commission Authentication System (ECAS) (see chapter 3).

The Commission A2A Services identified were

- Internal Market Information System (IMI).
- Communication and Information Resource Centre for Administrations, Business and Citizens (CIRCABC).
- Electronic Exchange of Social Security Information (EESSI).
- DG SANCO Reference Database System (SANREF).
- Consumer Protection Cooperation System (CPCS).
- LISFLOOD-ALERT.
- European Competition Network - Electronic Transmission (ECN-ET).
- European Database for Medical Devices (EUDAMED).
- Secure Exchange and Storage of Agricultural Data (SESAD).

3.4 The National eID systems and the relevant issues

3.4.1 Overview

Most EU Member States have implemented some form of eID system. However, these systems differ in many aspects. Many eIDs are issued by governments, but some are issued by the private sector. The technologies used for authentication also differ between countries: Public Key Infrastructure (PKI, e.g. using a smart card), a login & password, or an enhanced form of login (e.g. involving sms to a mobile phone number).

Based on the STORK documentation and other sources[25], there is the following table provides an overview of the different technologies and approaches used by the different member states:

Country	Public sector IDP	Private sector IDP	Name of system	Type of authentication
Austria	Yes	No	Bürgerkarte	PKI
Belgium	Yes	No	E-id	Login+PWD Enh.Login/pwd

[24] http://ec.europa.eu/idabc/en/document/3519/5927.html

[25] Source: STORK Deliverable 5.1 ("Evaluation and assessment of existing reference models and common specs"), chapter 3. The European Commission commissioned studies sketching the per country landscape for eID and eSignature in detail and highlighting interoperability issues. Overall study: D2.1 Report on analysis and assessment of similarities and differences;D2.2 Report on impact on eID interoperability (http://ec.europa.eu/idabc/servlets/Doc2ba1.pdf?id=32521) and country profiles on the eID Interoperability for PEGS website: (http://ec.europa.eu/idabc/en/document/6484.html)

Country	Public sector IDP	Private sector IDP	Name of system	Type of authentication
				PKI
France	Yes	No	Idénum	Login+PWD PKI
Germany	Yes	No	Epa (elektronischer Personalausweis)	PKI
Greece	Yes	No	Syzefxis PKI	Login+PWD PKI
Iceland	Yes	No		Login+PWD PKI
Italy	Yes	No	Carta d'Identità Elettronica (CIE)	PKI
Lithuania	Yes	No		PKI
Netherlands	Yes	No	DigiD/eHerkenning	Login+PWD Enh.Login/pwd
Slovakia	Yes	No		Login+PWD PKI
United Kingdom	Yes	No		Login+PWD Enh.Login/pwd PKI
Luxembourg	No	Yes (1)	LuxTrust	Login+PWD
Sweden	No	Yes (4)	BankID, Nordea, TeliaSonera and Steria	PKI
Estonia	Yes (1)	Yes (1)	Government IDP and bank IDP	Login+PWD Enh.Login/pwd PKI
Finland	Yes (1)	Yes (1)	Government IDP (FINEID) and bank IDP (TUPAS)	Enh.Login/pwd PKI
Portugal	Yes (1)	Yes (4)	Government IDP and 4 private IDPs: Lawyer's bar association, Solicitor association, notaries order	Login+PWD Enh.Login/pwd PKI
Slovenia	Yes (1)	Yes (3)	Government IDP and: Halcom CA, AC NLB CA, PostaCA	PKI
Spain	Yes (2 central government, 3 regional)	Yes (7)	Central: DNIe, FNMT Regional: CATCERT, INZEPE, ACCV Private: Camerfirma, ANF, ANCERT, Firma Profesional, ACA, Banesto, SRC	PKI

The following table provides more detailed information on IDs and eIDs in the European Economic Area (Source Deutsche Bank Research[26]).

The table shows in first instance that all EEA countries provide their citizens an ID card, with the exception of Latvia and to some extent of the UK, the IC card is compulsory in all countries except in Austria, Finland, Hungary, Sweden, the UK, and Switzerland.

All countries have implemented an eID card, except Denmark, France, Germany, Hungary, Latvia, Malta, Poland, Romania, Slovakia, Slovenia, and Switzerland. Of these, France plans an eID card along with Germany (11/2010), Hungary, Latvia, Malta, Poland Romania, Slovakia, Slovenia. The UK does not plan the introduction of an eID card.

Lastly, of the countries having implemented or currently implementing eIDs, all but Hungary, Latvia, Malta, the Netherlands, Poland, Romania, Slovakia do not integrate a Qualified electronic Signature Certificate.

[26] Deutsche Bank Research. eIDs in Europe. September 7, 2010
http://www.dbresearch.com/PROD/DBR_INTERNET_EN-PROD/PROD0000000000262236.pdf

ID and eID cards in the European Economic Area (EEA)

Country	ID card	Compulsory ID card	eID implemented	Compulsory eID	eID costs	eID planned	QES
Austria*	Yes	No	Yes (since 2004)	No	-	Already exists	Yes
Belgium	Yes	Yes	Yes (since 2004)	No, compulsory as of 2012	EUR 15.00	Already exists	Yes
Denmark	Yes	Yes	No	-	-	No	Yes
Estonia	Yes	Yes	Yes (since 2002)	Yes	EEK 250 (around EUR 16)	Already exists	Yes
Finland	Yes	No	Yes (since 2003)	No	Adults: EUR 51.47; children: EUR 25.73	Already exists	Yes
France	Yes	Yes	No	-	-	Yes	-
Germany	Yes	Yes	No	No, as of 2012	Aged over 24: EUR 28.80; aged up to 24: EUR 19.80; aged 16-18: Free	Yes (from November 2010)	Yes
Hungary	Yes	No	No	-	-	Yes	No
Italy	Yes	Yes	Yes (since 2000)	Yes	EUR 44.66	Already exists	Yes
Latvia	No	-	No	-	-	Yes (2010)	No
Lithuania	Yes	Yes	Yes	Yes	-	Already exists	Yes
Luxembourg*	Yes	Yes	Yes	No	EUR 15.00	Already exists	Yes
Malta	Yes	Yes	No	-	-	Yes	No
Netherlands*	Yes	Yes	Yes (since 2005)	Yes	EUR 42.85	Already exists	No
Poland	Yes	Yes	No	Yes, for over-18s	-	Yes (from start of 2011)	No
Portugal	Yes	Yes	Yes (since 2007)	Yes	EUR 12.00	Already exists	Yes
Romania	Yes	Yes	No	-	-	Yes	No
Slovakia	Yes	Yes	No	-	-	Yes	No
Slovenia	Yes	Yes	No	Yes	-	Yes	Yes
Spain	Yes	Yes	Yes (since 2006)	Yes	EUR 10.10	Already exists	Yes
Sweden*	Yes	No	Yes (since 2005)	No	SEK 400 (around EUR 42)	Already exists	Yes
United Kingdom	Yes, partly	No	Yes, partly (since 2006)	No, abolition planned	-	No	-
Switzerland	Yes	No	No	-	-	-	-
Iceland*	Yes	Yes	Yes	-	-	Already exists	Yes

* eID cards are issued by private Certificate Service Providers with a public mandate.

Sources: Enisa, IDABC, Ministries of Interior of the respective countries 1

Figure 3-1 ID and eID cards in the European Economic Area

3.4.2 Trust levels of national eID systems in STORK

One of the assumptions which have been guiding the present study on eID, eAuthentication and cross-border recognition is that different eID classes (levels) will facilitate the integration process and the acceptance by the MS's (assumption 8). The eID and eAuthentication mutual recognition and interoperability could benefit from the definition of quality levels such as the Quality Authentication Assurance (QAA) as developed by the STORK project.

The Stork QAA model, which is described in the Quality Authenticator Scheme deliverable[27] defines the different trust levels, and maps them on nationally used eID schemes. It defines 4 levels of STORK-trust:

1) No or minimal assurance: is the lowest assurance level, only minimal confidence (if any) in the asserted identity is available. Identity credentials are accepted without verification. This is appropriate when negative consequences are negligible
2) Low assurance: identities must be validated and a token issued by a government-approved body (with no need of physical presence). Identity tokens must be treated with security care, non-insecure protocols must be used in the electronic authentication phase. However, damages from a misappropriation of identities are low
3) Substantial assurance: The identity registration must unambiguously identify the claimant. Identity providers must be supervised by the government. The credentials delivered are certificates. The authentication mechanisms used in the remote authentication phase must be robust. At this level, substantial damages can result from identity misuse
4) High assurance: The registration requires at least once the physical presence of the claimant or trusted e-signatures. This level is achieved if the national legal requirements for issuing a qualified certificate have been met. The identity provider must be a qualified entity. The certificates must be hard certificates qualified according to the e-signature Directive. The most robust authentication mechanisms available must be used during the authentication phase. Damage caused by an identity misuse has a heavy impact.

Four different levels are used to balance costs and required authentication levels, in order to make maintainable both authentication information processes and the underlying infrastructure, along with a sufficient granularity for different business requirements resulting in a complete coverage of the risks.

The STORK trust levels are influenced by a number of assurance factors that are displayed in figure 4 below:

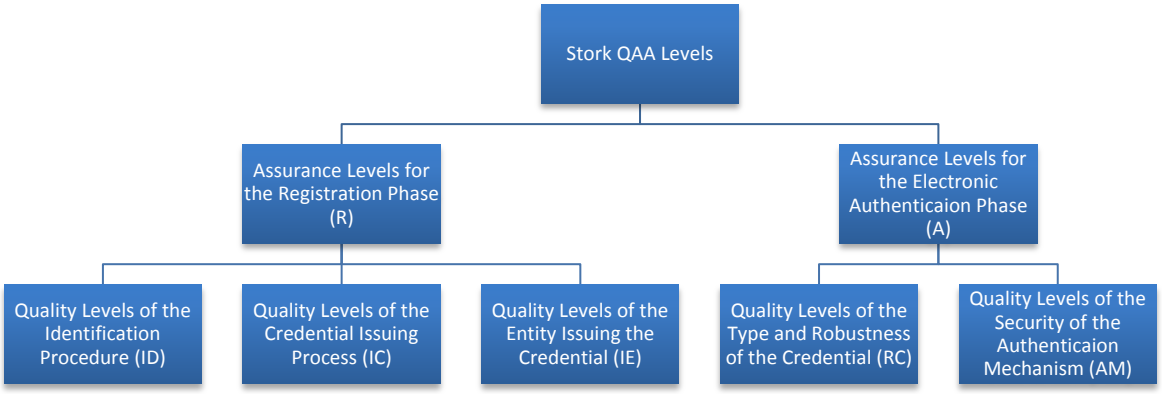


Figure 3-2 The Stork QAA Levels

Figure 1: (based on STORK deliverable D5.1 - Evaluation and assessment of existing reference models and common specs) Graphic representation of the different quality levels that constitute the assurance levels, that compose the QAA level.

In addition to defining the STORK trust levels, these levels have also been mapped onto member state's current eIDs. This mapping is shown in the table below. The horizontal axis shows the STORK assurance level.

[27] "Deliverable D2.3 - Quality authenticator scheme", 2009, STORK (http://www.eid-stork.eu/index.php?option=com_processes&act=list_documents&id=312&s=1&Itemid=60)

	STORK QAA Level 1	STORK QAA Level 2	STORK QAA Level 3	STORK QAA Level 4
Austria				Level 1
Belgium	Level 1	Level 2	Level 3	Level 4
Estonia		Level 1 (username and rotating passwords)	Level 1 (one-time password token)	Level 1 (with ID-card or Mobile-ID)
France			Level 1	Level 2, Level 3
Germany	Level 0	Level 1	Level 2	Level 3
Iceland	Level 1	Level 2	Level 3	Level 4
Italy		Level 1 (PIN + password)		Level 1 (digital certificate in smart card)
Luxembourg				Level 1, Level 2
The Netherlands		Level 1	Level 2	
Portugal		Level 1	Level 2	Level 3
Slovenia	Level 1		Level 2	Level 3
Spain	Level 1	Level 1	Level 2	Level 3
Sweden			Level 1	Level 2
UK	Level 0	Level 1	Level 2	

Table 1: Mapping of member state eID quality level on Stork QAA level ***(based on STORK deliverable D5.1 - Evaluation and assessment of existing reference models and common specs)***

The table shows that:

- Today, not all countries participating in STORK would have an eID system taking into account all of the STORK levels. There are countries that do not support the highest levels of trust (e.g. Netherlands), and there are countries that do not support the lowest levels of trust (e.g. Estonia);
- There is not always a 1-to-1 relationship to STORK QAA level and national level (e.g. in the case of Spain, where Spain's level 1 maps onto STORK level 1 and 2, or France, where France's levels 2 and 3 both map onto STORK level 4);

It is possible that a Member State does not provide a sufficient level of authentication to access services from a service provider. Take for example the case of an Austrian service provider requesting authentication at QAA level 4, and a Dutch customer/end user. The Dutch scheme does not go beyond Stork QAA level 3. Therefore this citizen will not be able to use these cross-border eID services, unless either the Service provider decides that QAA level 3 is enough for the particular service, or a Dutch QAA level 4 is introduced.

3.5 eID related issues

eIdentification and eAuthentication are key building blocks for trusted cross-border online services and for a smooth functioning of the digital single market. They are needed to provide the electronic equivalent of personal identification and the validation of personal identification, performing the same functions in the electronic environment as in the physical world.

The current state of development of the national eIDs shows they are still heterogeneous in terms of:

a) Setup of the service provision: QAA level, IDP and type of authentication, Security issues (levels of assurance)
b) Institutional, organisational and technological governance
c) Regulatory arrangements on responsibility, assurance of unique association of an eID to a physical and legal person and eAuthentication procedures: -Some EU Member States have regulated and are issuing eIDs and eAuthentication (the "formal" eIDs)
d) Interoperability, as a direct consequence.

This fragmented and unregulated scenario hinders the access to public online services for which identification is needed by non-nationals in the cross-border context. The lack of mutual recognition and acceptance of means of electronic identification and authentication is a serious hampering factor to the cross-border provision, and use of public online services.

Similarly, there are serious concerns on liability issues of service providers and on the protection of individual rights, such as privacy.

Other barriers to the deployment and take-up of eID-based cross border services relate to absence of cross-border interoperability of technical solutions.

This presents the serious case of officially issued identification instruments which nevertheless have no value in cross-border service use.

The issues raising from an unregulated and fragmented regulatory landscape for electronic identification and authentication therefore includes

1) The insufficient scope of the current legal framework
    a. At present there is no basis for Interoperability, mutual recognition and acceptance and therefore no legal certainty for interested parties
    b. The EU is promoting one large initiative in cooperation with a significant number of Member States: the STORK pilot and subpilots, which is looking into regulatory matters in its second edition (STORK 2.0). As it stands now it has a formal legal endorsement by EU Member States but no cross-border regulatory foundation. Therefore,
    c. The leveraging of the STORK results is still in its beginning, also because it would require the completion of STORK 2.0 as well as the new Large Scale Pilot integrating all the service building blocks developed in ICT-PSP
    d. Liability: With respect to liability, the primary issue is that eIDs are made available under a set of guarantees and warranties that are appropriate for the use in a specific context. In this respect there are national level liability rules, which foresee full liability of administrations and their employees for the operation of IT systems and places the burden of proof. However, normally this liability is waived if administrations can prove that there was no wilful misconduct or gross negligence[28].
2) The uneven eID landscape across the EU: not all EU Member States are equally advanced in the reasoning, regulation and development of their national eID systems. This means that not all

[28] Codice dell'Amministrazione Digitale, D. Lgs. 7 marzo 2005 (Italy)
Artikel 23 Austrian "Signaturgesetz" (SigG)

Member States offer eID and eAuthentication to their citizens and that the development of national eID shows very different stages of development. This leads to different options for regulation, for example

   a. The immediate implementation of mutual recognition, or
   b. The progressive implementation of regulation and gradual integration of Member States

3) The trust and confidence issue, which is at the basis of the whole reasoning, regulation and implementation of eID based services. Service providers and administrations have to trust eID and eAuthentication systems, citizens need to be aware of services based on eID and their benefits, as well as of their security levels. For this purpose a reasoning on several issues is necessary:
   a. Supervision, both at Member State level and at Community level. Supervision requires the establishment of independent bodies, rules and procedures. They can be of significant benefit to the trust and confidence issue, but also require a coordination and agreement, as well as a significant level of investment to establish and run the supervisory bodies;
   b. Quality assurance levels, which provide a certain information on how security and safety are handled when managing eID and eAuthentication systems. STORK has four quality assurance levels. They are closely related to the third party supervision issue, since stakeholders need to rely in independent certification of the quality assurance levels;
   c. Trust and confidence are related to technological solutions which are related to the overall mutual recognition and interoperability issue as well as to the more trust and security-related aspects. STORK has been developing solutions for the interconnection and for security, a clear support to their diffusion would leverage proven technical and operational solutions for the benefit of interoperable eID systems. In other words further promoting the STORK solutions with a clear policy support will speed up the solutions of security and interoperability issues:
4) User awareness: citizens, businesses and institutions
   a. There is a huge potential in the development of cross-border eID-based information systems. All stakeholders need to be aware of this potential, of the benefits and also of the possibility to secure systems. However, the complexity behind the technologies used in online transactions and the key role played by trusted third parties result in an environment where it is difficult to assess trust (problem 2). Particularly end users (citizens and SMEs) who generally do not have sufficient expertise must be able to rely on rules which establish clear rights and responsibilities of all stakeholders (online service providers, end users and governance bodies such as supervisory authorities).
   b. User needs satisfaction
5) The scale of eID and eID-related cross-border and cross-sector services. The demand of eID is not self-sustaining: it requires the availability of eID cross-border public services, but not only. Electronic identification is an issue with a large number of private sector online services, from the basic access to email, to the access to banking and financial services. the scale of eID adoption in the public services will be more related to the overall population using them, rather than the frequency of use. Therefore the integration of public and private eID-based services will be a key factor for the diffusion of electronic identity.
6) The cross-sector dimension: eIDs can be issued by private or public sector parties, and/or their use may be specific to a sector, such as social security, e-payment or eHealth. In both cases, the absence of a general framework for eID recognition and acceptance makes it hard to use an eID outside of its context, mainly because of liability and data protection challenges.
   a) Efficient and fast integration of private sector players with significant networking and technological capabilities: the banking sector and the telecommunications sector.

All these issues will be addressed in the proposed options and sub-options in the subsequent sections of the document.

3.6 A case study: Cross-border opening of a bank account[29]

The following case study was developed by Deutsche Bank Research:

When opening a bank account, there are several legal requirements with which the banking institution is obliged to comply, including identification of the client using an official identification document[30].

Furthermore, a signature must be supplied to conclude the contract. Up until now it has usually been necessary for the customer to physically present himself or to complete an alternative procedure

(in Germany, for example, the so called PostIdent procedure).

Identification could instead be provided by an eID. The Qualified Electronic Signature, by contrast, can be used for qualified acknowledgement, for example, of information or for giving consent for a creditworthiness check. To open a deposit account the eID on its own would be sufficient. Opening an account with an overdraft facility online or taking out a loan online would require the eID and the QES. An account opened online would be usable "offline" but would be subject to some restrictions (for example, it would not be possible to execute a paper-based credit transfer, as the bank would not have a specimen signature from the client).

In order for eIDs to help in establishing a cross-border internal market for financial services, the legal stipulations and standard business practices when an account is opened would also have to be harmonised. Many banks require, for example, a check to be made by a credit register; in some countries proof of address (for example the submission of a heating bill) or the applicant's tax number is required.

Also, compatible technical standards would have to be established, so that the information contained in a Romanian eID that is read via a card reader on a computer in Finland is accepted by a bank in Portugal as proof of identity. In addition, differing legal systems and redress and enforcement mechanisms, diverse deposit insurance systems and language barriers have hitherto made it unattractive to open an account in a foreign country.

E-banking with an eID facility is already in use in a number of countries (for example, Austria, Estonia and Spain), but it is not yet possible to open an account using an eID in these countries either. An eID user test is currently being conducted in Germany with the participation of banks and insurance companies. A draft EU regulation on establishing an end-date for the parallel use of national direct debits and SEPA direct debits and SEPA credit transfers contains an article that would ban discrimination based on nationality and residence when an account is opened. Although this sends out a signal and is a step in the right direction, it will, however, have no fundamental impact on the ease of opening an account online in a foreign country because of the above-mentioned impediments.

4 SECTION 3: OBJECTIVES

The problem definition shows that eIAS technologies are a fundamental building block for the Digital Single Market, and in particular electronic identification and authentication. The fragmentation of the current eID and eAuthentication scenario and the review of the activities of the stakeholders show that it

[29] Study by Deutsche Bank Research : "eIDS in Europe" (2010)

[30] Anti-Money Laundering Act and EU Directive 2005/60/EC

is highly unlikely that market forces alone will be able to pave the way towards harmonised, mutually recognised electronic identification schemes and their authentication.

The eID and eAuthentication policy objectives aim to lead to a legal framework which allows the smooth development and operation of these building blocks and their availability for public online services.

4.1 The General Policy Objectives

The general policy objectives concern the need to work towards the Digital Single Market and to ensure that the fundamental building blocks are in place to enable Digital Single Market eServices and transactions.

The digital single market, aiming at borderless and secure online services with high levels of trust and confidence is rooted in the Europe 2020 strategy.

The Digital Agenda for Europe

a) identifies the Digital Single Market as crucial driver to fully reap the benefits of the digital era. The purpose in particular is to create a straightforward and open environment for online cross-border transactions, eliminating technical and legal constraints. Electronic identification and authentication services are essential enablers for private and public sector online transactions.
b) puts a great emphasis on the online safety and security of users and transactions. There are highly sensitive services and applications – such as eBanking and eHealth – which would not exist without the prerequisite of reliability. Often, IT-networks and end-user terminals are still too vulnerable and exposed to security threats.

In particular, Key Action 16 is orientated to ensure mutual recognition of e-identification and e-authentication across the EU based on online 'authentication services' to be offered in all Member States.

The Single Market Act makes a specific reference to the need for legislative measures to ensure the mutual recognition of electronic identification and authentication across the EU. At the same time it stresses that trusted electronic services need to respect privacy, provide legal certainty, ensure that transactions are secure, work across borders and be recognised by all sectors of activity. Furthermore, digital services and their security applications need to be cheap and easy to use and transaction parties need to keep full control over the proceedings

The European eGovernment Action Plan 2011-2015 identifies a number of technical and legal pre-conditions which will enhance the development of seamless European cross border online services and enable their implementation. These pre-conditions include the promotion of interoperability across borders to allow sharing of information, deployments of one-stop-shop approaches and the Europe wide use of (national) electronic identification solutions and payment schemes.

Open specifications and key enablers such as electronic identification are required to guarantee interoperability, which is the ability of systems and machines to exchange, process and correctly interpret information. It is not limited to technical issues but involve legal, organisational and semantic aspects.

The actions of the eGovernment action plan are set out to define a common strategy for achieving interoperability between Member States. Electronic

identification and authentication are identified as essential key enablers of eGovernment services, in particular in the cross-border context. One of the actions identified foresees that the Commission will table legislative measures to ensure mutual recognition and acceptance of electronic identification and authentication across Europe.

4.2 The Specific/Operational Policy Objectives

Electronic identification and authentication and their cross-border diffusion are based on the existence of eID-based cross border public services. although this might sound tautological, in itself eID and eAuthentication are not needed except in combination with online services.

The implementation and diffusion of eID is therefore motivated by the demand by public online services. A cross-border regulation is needed as an enabler for cross-border public services, which in turn require eIdentification.

At present the cross-border development of public services is limited as is the development of services which require eID[31].

In respect to electronic identification and authentication, the specific and operational objectives need to consider the fact that their usage is in most cases limited and allows only the access to national online services. As stated by JRC/IPTS, there is a "lack of a compelling, well-defined and accepted business case for federated eID. Few organizations or governments are willing to speculatively invest"

The absence of regulation is one of the key hampering factors for the development of services which require eID and eAuthentication. This brings about the need to:

- Create a legal and regulatory framework enabling the interoperability of the different technical solutions used by Member States to allow their secure and trusted use in cross-border eServices
- Create a framework of reference to enhance the reliability of the issuer of the eID, the legal certainty on the cross-border use of eIDs
- Provide for clear liability for the security, correctness and unique correspondence of the eID to the physical person when used in online transactions
- prevent discrimination of non-nationals when they access online services and in case some MSs do not issue eIDs to their citizens.

5 SECTION 4: POLICY OPTIONS

The following policy options have been indicated in the Study Terms of Reference and have been the object of study and verification applying the different approaches and methodological tools, as described in Section 1: Methodology (summary of the methodology used to yield the study results). This paragraph describes the different options, their main drivers and features, as well as the impacts on EU policy making and a general assessment. Where foreseen, the study has examined possible sub-options.

Furthermore, a number of out-of-the-box options have been proposed and assessed.

5.1 Option A – baseline scenario: keep the status quo, proposing no policy change. Continuation of eID-related activities, but no specific legislative measures

5.1.1 Description of the Option

The selection of Option A entails

a) The continuation of EU-funded eID-related development and validation activities through several community instruments such as CIP ICT-PSP, the R&D Framework Programme within the eGovernment thematic programmes and the technological programmes;

[31] The state of the Electronic Identity market: technologies, infrastructure, services and policies, 2010, JRC/IPTS

b) No specific legislative measures would be introduced, leaving the regulation to the initiative of Member States through bilateral or possibly multilateral agreements between governments or directly service providers.

5.1.2 Aspects related to EU policy making

This option differs from Option C in that eID-based public and private services are developed in the current regulatory and operational framework. For the eID issue, this means that the ICT-PSP Programme will continue to support policy-related large scale pilots which may be directly or indirectly related to electronic Identification and authentication.

It needs to be emphasised that

a) There are limits to the "fundability" of pilot initiatives directly related to eIDs, concretely that there are limitations to the continued support of pilots like STORK, for which eID is a core element. In other terms, after having funded the first STORK pilot and after the on-going funding of the STORK 2.0 and their sub-pilots, it is likely that support to eID pilots might be stopped by the European Commission;
b) The Framework Programme evaluation criteria clearly state that the Science and Technology quality needs to address Soundness of concept, and quality of objectives, Progress beyond the state-of-the-art; Quality and effectiveness of the S/T methodology and associated work plan[32]. Also demonstration and piloting activities have a limited support from EU R&D Framework Programmes;
c) On the other hand, Member State stakeholders participating in STORK have clearly stated that without a regulatory and financial intervention, the STORK eID is not sustainable beyond the projects.

This means that even if CIP ICT-PSP will continue eID related experimentations, in the medium term – after STORK 2.0, and maybe after the completion of the Large Scale Pilot developing the cross-border building blocks included in the 2012 Work programme – direct support to eID is likely to stop.

Of course CIP ICT-PSP may well continue to fund Large Scale Pilots of eServices based on eID. But in this case the situation may even be worse than Option C, since the EU will continue to fund pilots of cross-border services not taking any care of the overall regulatory and operational context.

Not only the "mandate" to take care of the development of the DSM and of eGovernment would be disregarded, but the EU would continue a support activity which would further increase fragmentation and uncertainty.

This means that new public cross-border eServices might be developed, that these services need to rely on interoperable electronic Identities and their authentication. This will increase uncertainty and fragmentation, since every pilot project might look for its own avenues to solve the issues related to the cross-border use of eIDs.

The CROBIES study has determined that lack of interoperable eID is barrier to interoperability of eSignatures.

In paragraph 3.4, Figure 3-1 ID and eID cards in the European Economic Area presents an overview of the current status of ID and eID cards in the European Economic area. Clearly eID is a clear priority in the majority of EEA states.

[32] http://cordis.europa.eu/fp7/ict/fet-open/docs/gfastrepv2.pdf: GUIDE FOR APPLICANTS: Information and Communication Technologies ICT.

Out if 24 EEA countries, 13 have already implemented the eID card and 9 are already planning the implementation. Therefore only 2 EEA countries, the United Kingdom and Switzerland are not planning to adopt an eID card.

It seems therefore quite obvious that eID cards are a key issue in Europe and that their cross-border use needs to be addressed by the European Union.

Furthermore, Paragraph 6.1.1.2 presents several tables on Services for Immigrants and Commuters, and specifies the relevant eID requirements. Figure 6-2: Moving and residence related services shows that there is mandatory eID requirement for registering a change of domicile, to request a residence card, to enrol as a student to pay vehicle tax, to order a birth certificate and to register a death.

Similarly, eIDs are mandatory for electronic prescriptions, and to access a patient summary (Figure 6-3: Health related services), to submit an income tax declaration and to register for a pension Figure 6-4: Employment Services).

Paragraph 6.1.1.3 presents a set of eID enabled cross-border services: tender for public procurement (Figure 6-5: Procurement Services), registration of a new legal entity, corporate/business tax declaration, VAT registration, submission of VAT declarations, new vehicle registration (Figure 6-6: Business and start-up services).

There are disputes on the obligation of eID in eProcurement procedures, however it needs to be emphasised that the identification of the bidder, whether individual or as the legal representative is mandatory according to the public procurement rules in certain countries[33]: in 8 countries it is not mandatory, in 5 countries it is mandatory.

5.1.3 General Assessment of the Option

On-going activities would continue, such as:

- The CIP ICT-PSP eID activities like STORK, STORK 2.0 and the project sub-pilots
  - Pilot 1: A demonstrator showing that cross-border electronic services can operate in a number of Member States. The applications include national portals from Austria (help.gv.at), Estonia (eesti.ee), Germany (mein-service-BW), Portugal (portaldocidadao.pt) and the UK, one regional portal from Catalonia in Spain and one specific service for compliance activities for working in Belgium (limosa.be)
  - Pilot 2: Safer Chat - To promote safe use of the Internet by children and young people.
  - Pilot 3: Student Mobility - To help people who want to study in different Member States.
  - Pilot 4: Electronic Delivery - To develop cross-border mechanisms for secure online delivery of documents.
  - Pilot 5: Change of Address - To assist people moving across EU borders.
  - STORK 2.0 Pilots, focused on strategic eLearning and Academic Qualifications, eBanking, Public Services for Business and eHealth areas
- Policy and technological studies like the recent Managing multiple identities (2011), Mapping Security Services To Authentication Levels (2011), Mobile Identity Management (2010), Security Issues in Cross-border Electronic Authentication (2010), Privacy and Security Risks when Authenticating on the Internet with European eID Cards (2009)
- R&D activities in the field of R&D.

[33] Figure 10-23: Businesses' services for which eID is optional or mandatory, 2010, by service

These actions however will miss a general framework within which they could be implemented as real-life services. Their regulation will – as said – be left to the interested parties, and most likely rely on their limited scope of actions and initiative. The selection of Option A entails

a) The division of operational activities from their cross-border regulation, i.e.: the regulatory framework will not adjust to the changes induced by societal and organisational developments due to the results of piloting and demonstration activities;
b) The development of autonomous regulations, increasing fragmentation and uncertainty;
c) An increase of uncertainty and of barriers to a uniform development of the eID-based services landscape, such as technological incompatibilities, institutional differences, lack of regulatory arrangements on liability
d) bilateral agreements are unlikely to overcome identified barriers

A major obstacle is the lack of regulatory arrangements on liability for cross-border eID providers, as most service providers are not willing to depend on the accuracy of an eID issued and authenticated by a party that is not liable for errors. While maintaining the status quo will result in some bilateral agreements handling these issues between some Member States, producing a fragmented legal landscape on liability arrangements.

To this end it is important to quote article 23 of the Austrian "Signaturgestetz", which in Article 23 provides for liability of the certifier on the processes and products (catch 1, catch 2).

However, if the certifier can demonstrate that no fault can be attributed to the certifier or their employees, liability is waived[34].

Similar developments are to be expected with regards to technological incompatibilities, as these are also unlikely to be overcome in such a way that interoperability of eID at the EU-level will be reached. The unsustainability of STORK components in the face of lack of regulation on liability means that the building blocks for cross-border solutions developed in this project will not be effectively used in practice.

Overall this option is not effective in overcoming the identified barriers and in creating a level playing field at the EU level for cross-border eID use.

It will not be possible to develop the past and current pilot services and scale them up at EU level. The development of cross-border eID-based services will need to rely on bilateral or multilateral agreements between Member States developing the public service, who will agree on how they will use their eID and eAuthentication systems according to specific arrangements.

Other Member State's public service providers will then have to negotiate their second stage access to a pre-arranged setting, creating an uneven and unbalanced playing field across the EU.

Keeping the status quo will make it impossible to provide a structured response to the needs of intra-EU immigration needs, as shown in Figure 6-1: Intra-EU immigration. The more important immigration flows

[34] http://www.ris.bka.gv.at/Dokument.wxe?Abfrage=Bundesnormen&Dokumentnummer=NOR40014445
"(3) Der Zertifizierungsdiensteanbieter haftet nicht, wenn er nachweist, daß ihn und seine Leute an der Verletzung der Verpflichtungen nach den Abs. 1 und 2 kein Verschulden trifft. Kann der Geschädigte als wahrscheinlich dartun, daß die Verpflichtungen nach den Abs. 1 und 2 verletzt oder die zur Einhaltung der Sicherheitsanforderungen dieses Bundesgesetzes und der auf seiner Grundlage ergangenen Verordnungen getroffenen Vorkehrungen kompromittiert wurden, so wird vermutet, daß der Schaden dadurch verursacht wurde. Diese Vermutung ist widerlegt, wenn der Zertifizierungsdiensteanbieter als wahrscheinlich dartut, daß der Schaden nicht durch eine Verletzung bzw. Kompromittierung der im zweiten Satz genannten Verpflichtungen und Vorkehrungen verursacht wurde".

come not only from the larger European Member States, but also from those countries which have a higher level of development of public services at national level and therefore should have a more significant drive towards the development of cross-border public services. Figure 10-5: Full Online Availability, By Member State confirms that the countries with a more significant intra-EU immigration are those who have a highly developed eGovernment development.

5.2 Option B: legislation on cross-border and cross-sector mutual recognition and acceptance of eIDs to enable citizens and businesses to use their "national" eIDs not only in their home country but in all other Member States.

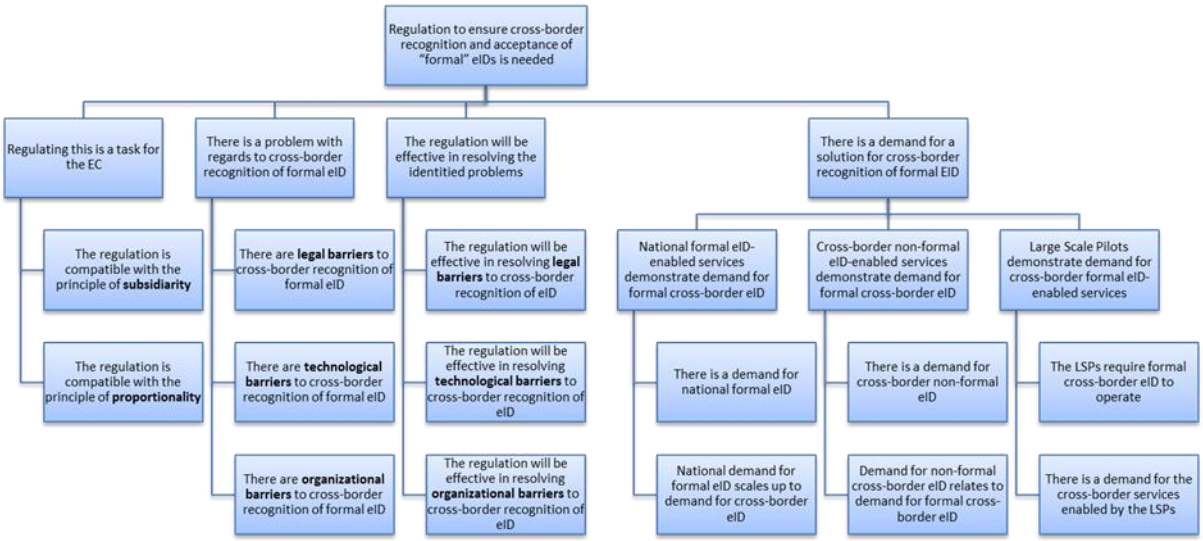


Figure 5-1: Conceptual Overview of the Policy Assumptions

5.2.1 Aspects related to EU policy making

The choice of regulating mutual recognition and acceptance of national eIDs is the appropriate consequence of the current policy initiatives in support of a better functioning Internal Market, the creation of the Digital Single Market, the implementation of the Digital Agenda for Europe and the eGovernment Action Plan 2011-2015.

The analysis has shown that regulating the eID landscape in Europe is a task for the European Union according to the principle of subsidiarity and of the coverage of cross-border aspects of society, in particular for the better functioning of the EU Single Market. In the Electronic identity (eID) technologies and authentication services are essential for transactions on the internet both in the private and public sectors[35]. Key Action 3 requires the Commission to "**Key Action 3**: In 2011 propose a revision of the **eSignature Directive** with a view to provide a legal framework for cross-border recognition and interoperability of **secure eAuthentication systems**"[36].

[35] A Digital Agenda for Europe. Communication from the Commission. COM(2010) 245 final

[36] Ditto, paragraph 2.1.2 page 10-11

Option B is rooted in the Article 114 TFEU[37]. The intervention logic of the EU with the aim to facilitate the EU-wide use of eID and eAuthentication in the Union is clearly supported by the feedback received in the context of the Public Consultation and the SME panel.

The policy analysis confirms that the EU has to take action since eID and eAuthentication are considered fundamental building blocks for the construction of the Digital Single Market and to develop cross-border public online Services.

In chapter 2.7, page 12 the DSM states that "To this end, the Commission will propose a new legislative framework to ensure confidence in electronic transactions. This framework will propose revision of the Directive on Electronic Signatures in order to clarify its concepts, simplify the use of e-signature and remove interoperability barriers. The framework will also provide for the mutual recognition of electronic identification and authentication services. It will also cover the cross-border functioning of certain other trusted services. The tools proposed in the framework should be general and not linked to a specific sector, especially where electronic identity is concerned. The framework will be technologically neutral and open to all communication channels, including the Internet and mobile communications.

The need for EU action to enable the cross-border use of eIDs is also confirmed by the negative impacts which are expected to occur due to non-action (see chapter 4.1.).

EU legislation on electronic identities is as such no guarantee for the demand of eID based services but it helps to build trust. In relation to trust, the Single Market Act[38] states that (p13) "Strengthening confidence in electronic transactions is a necessary condition for the development of a digital single market, from which citizens, businesses and public authorities could fully benefit. What is needed in order to do this are trusted electronic services that respect privacy, provide legal certainty, ensure that transactions are secure, work across borders and are recognised by all sectors of activity, but which are cheap and easy to use and which are under the strict control of the transaction parties.

The analysis of the feedback received by STORK stakeholders has shown that there is a significant fragmentation between national eID systems. EU legislation should take into account interoperability of systems from the operational and legal points of view.

When considering the liability issue, it is open to discussion whether bi- or multilateral agreements will not be more efficient in solving the liability, starting from mutual trust to solve integration and integration issues. Considering the assumptions which guided the analytical work, Figure 5-1: Conceptual Overview of the Policy Assumptions shows the hierarchy of the different issues to consider, relating the principles lines

5.2.2 General Assessment of the Option

The regulation of cross-border eID and eAuthentication is necessary, because

- eID it is needed for the cross-border access to public services and, once they will be offered, of cross-border commercial and private online services. The SME panel have clearly expressed this

[37] Article 144 TFEU, §1: "*Save where otherwise provided in the Treaties, the following provisions shall apply for the achievement of the objectives set out in Article 26. The European Parliament and the Council shall … adopt the measures for the approximation of the provisions laid down by law, regulation or administrative action in Member States which have as their object the establishment and functioning of the internal market.*"

Article 26 TFEU: "*1. The Union shall adopt measures with the aim of establishing or ensuring the functioning of the internal market, in accordance with the relevant provisions of the Treaties. 2. The internal market shall comprise an area without internal frontiers in which the free movement of goods, persons, services and capital is ensured in accordance with the provisions of the Treaties. 3. …*"

[38] COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Single Market Act Twelve levers to boost growth and strengthen confidence "Working together to create new growth" COM(2011) 206 final

need. At present, 47% of the respondents to the SME panel have indicated that they already now use eIDs to complete procedures with public administrations, with other companies and consumer relations. The growing availability of cross-border services requires a clear framework of rules for the cross-border mutual recognition and acceptance of eIDs;

- 80% of the respondents to the public consultation have indicated that they use eIDs and over 40% associate it to the legal effectiveness of electronic documents
- Nearly 65% of the participants in the public consultation indicate that the regulation of eIDs is transparency and nearly 80% say that is it fundamental for the protection of personal data;
- The public consultation showed that nearly 70% of the respondents believe that the use of eID would reduce the need for numerous UIDs and passwords, thus providing increased security in online access to services, and nearly 90% believes that service access would be significantly simplified.

The assessment of Option B needs to take account of different aspects

a) Most EEA countries have implemented eIDs or are in the process of introducing it (Figure 3-1 ID and eID cards in the European Economic Area)
b) The availability of online public services is high (Figure 10-3: eGovernment online availability, 2010, by country) and the growth trend is high (Figure 10-4: Full online avaialbility trend 2001-2010 shows a growth of business services from about 30% to nearly 90% and of citizen's services from less that 18% to nearly 80%). The majority of EU27 has a very high or a full online availability of public services: the EU average is above 80%, many countries have achieved 100% and most are placed around the European average. Only a few are lagging behind
c) Figure 10-6: Service Sophistication shows that the majority of EU countries has a high or very high eGovernment sophistication. This means that most EU Member States offer public services which offer transaction and targetisation/automation functionalities, the highest levels in the 5-stsge maturity model[39]. Looking at the trend of eGovernment sophistication (Figure 10-7: eGovernment Sophistication, trend 2007-2010), for citizens it has grown from 65% to 90% from 2007 to 2010 and for enterprises it has grown from above 80% to over 90% (Figure 10-9: Sophistication of eGovernment. Citizen vs. business services).
d) The percentage of individual's interaction with public authorities is over 40% in all EU27 Member States, with the exception of 6-7 countries (Figure 10-11: Percentage of Interaction with public authorities) and the trend of the EU average has grown from 36% to over 40% from 2008 to 2011 (Figure 10-12: Increase of online interaction with public authorities). The percentage of individuals using public online services to interact with public authorities to fill in forms has grown from 17% to 21% between 2008 and 2011 (Figure 10-14: Increase of interaction for sending filled forms)
e) The online interaction of enterprises with public authorities in the EU is very high and oscillates between 60 and 95% for most countries (Figure 10-16: Percentage of Interaction with public authorities, by country) and the EU average between 2004 and 2010 has increased from 51% to over 75% (Figure 10-17: Increase of enterprise interaction with public authorities). The percentage of EU enterprises using public online services to return filled in forms has increased from about 27% in 2004 to 60% in 2010 (Figure 10-19 Increase of enterpise Interactions with the purpose of sending filled forms).

The above data shows that the availability and use of public online services at national level is increasing. The increase is stronger for enterprises than for citizens, and this can be explained by the fact that

[39] The 5-stage maturity model: (i) information, (ii) one-way interaction, (iii) two-way interaction, (iv) transaction, and (v) targetisation/automation.

enterprises have many more formal obligations than individuals. The latter are mainly driven by personal needs – even though there are some personal obligations such as tax declarations. It must also be said that for enterprises mobility might be less of an issue than for citizens.

Paragraph 10.6.3.2 shows Figure 10-29:perceived need for additional regulation on eID at the EU-level (Public Consultation): 25% of the large private companies, 32% of SMEs, 16% of industry associations and 37% of public authorities and governments answering the public consultation call for an additional regulation of cross-border eID.

5.2.3 The Sub-Options for Option B: Putting in place a regulatory framework for the mutual recognition and interoperability of eIDs

For Option B a number of sub-options were considered, which are discussed below.

5.2.3.1 Sub-Option B1: focus of the legislation on the assurance of cross-border recognition and acceptance of national eIDs

This option focuses the legislation on the assurance of cross-border recognition and acceptance of formal eIDs. The mere mutual cross-border recognition of formal eIDs might be the most "simple" way of regulating eIDs and their authentication in Europe. This option would require the less heavy effort in mutual recognition.

It would exclude any kind of interference in national systems and technological choices,. One of the main results would be the solution of open liability issues as Member States would assume unlimited liability for the assurance of their national eIDs and for the unique attribution of the eID to the natural or legal person to whom it was issued.

As already mentioned, the liability, many national laws regulate the liabilities emerging from the use of ICT by public administrations.

In most cases the laws foresee full liability[40] of the Public Administrations operating information systems, and thus electronic ID and authentication systems. But in most cases – as in the Italian and the Austrian law – if the Administration can prove the absence of wilful misconduct or gross negligence, liability is waived.

5.2.3.2 *General assessment of option B1*

Option B1 focuses closely on the implementation of a regulation on cross-border mutual recognition and acceptance of national eIDs. The participants in the public consultation have indicated their wish for a comprehensive, all embracing legal framework: Over 50% of the Government participants and over 45% of the businesses (Figure 10-30:opinions on appropriate kind of legislative measures to be taken on eID (Public Consultation)

- Implementation
  - This would be the EU eID regulation
- Pros
  - Efficient and effective policy making, dealing with the core issue of eID regulation

[40] Codice dell'Amministrazione Digitale, D. Lgs. 7 marzo 2005 (Italy)
Artikel 23 Austrian "Signaturgesetz" (SigG)

- Would leave further – complex – regulatory measures to a later stage, where cross-border eID will be more developed
- Would address the expectations of stakeholders[41] for additional regulation
- Would address the expectations of companies who would use cross-border and national eID if it was mandatoryFigure 10-35: Potential reasons for companies to use eID (SME Panel)

- Cons
  - The mere regulation of cross border mutual recognition and acceptance would not consider the cross-sector issues and the issues of citizens excluded because their home countries are not catering for national eIDs

5.2.3.3 Sub-Option B2: Allow the private sector the use of national eIDs, (cross-sector use of national eIDs)

This option allows private use of formal eID, enabling private organizations to use government-recognized or issued eID. There is an evident advantage to broaden the use of formal eIDs, including the private sector: it would support the creation of the necessary critical mass of service demand to justify the implementation and operational expenditure, besides providing a quantitative justification for the "policy making" cost.

Unless there are specific legal or institutional "objections" to the private use of formal eIDs, this seems to be one of the sub-options to consider.

There is an evident advantage to broaden the use of national eIDs, to the private sector: it would support the creation of the necessary critical mass of service demand and, therefore, justify the implementation and operational expenditures, besides providing a quantitative justification for the "policy making" costs.

The policy making costs are those sunk – or hidden – costs, which administrations need to bear to

a) Set up policies, including preparatory studies
b) Run policy and regulatory instruments and incentives, if appropriate, to stimulate and support a consistent behaviour by stakeholders, citizens, businesses and istitutions
c) To fulfil the supervisory role and to control the behaviour those subjects who are the goal of the policy or the regulation
d) To undertake evaluations and assessments of policy and regulatory measures.

The SME panel provides an important indication: those not using eIDs indicate that they would use it if it was mandatory (35,37% of respondents) and if the use was more pervasive: 25,58% if used in the specific business sector and 25,61 if used in all sectors.

The IPTS study in 2010[42] indicates that eID market growth could be encouraged by government stimulating greater use of federated ID schemes across the private sector. The study also concludes that while governments and public authorities do not accept commercial credentials as sole identifiers when authenticating individuals, commercial providers on the other hand will generally trust government-issued credentials even if these are used out of context – a passport is not designed for opening a bank account, but will be accepted for doing so." The same may be true for eID.

The Eurobarometer observatory has determined that Europeans use credit cards (private eID) for electronic identification purposes. Europeans use the following types of credentials: mostly credit cards

[41] Figure 10-29:perceived need for additional regulation on eID at the EU-level (Public Consultation)

[42] The State of the Electronic Identity Market: Technologies, Infrastructure, Services and Policies; IPTS 2010

and bank cards (74%), national identity cards or residence permits (68%), government entitlement cards (65%), or driving licences (63%). 34% of respondents have an account they use on the Internet, such as email, or for social networking or commercial services.

The Eurobarometer shows that privacy is perceived to be an issue in eID usage, as 73% of the respondents consider national identity numbers or cards and passports to be or contain personal information.

This option should be considered because it will increase the effectiveness and fits very well within the EU policies by involving private market players. The formal eID system should however be complementary and not competitive to the private sector eID's.

5.2.3.4 *General assessment of option D1*

- Implementation
  - Under the umbrella of the EU eID regulation
- Pros
  - Will produce favourable benefits on critical mass of the use of eIDs
- Cons
  - Will introduce major operational, legal and technological complexities due to the opening up of eID systems to the private sector

5.2.3.5 Sub-Option B3: provide all citizens with the possibility to obtain an eID

This option introduces the possibility (i.e. right) for each citizen to obtain a formal eID in another Member State. At present this option is available only in Austria.

However, to activate the Bürgerkarte in Austria as a foreign citizen it is necessary to register in the "Ergänzungsregister für natürliche Personen (ERnP)"[43]. For this purpose the natural person needs to provide and proof the following:

- Name and surname
- Gender
- Date of birth and state of birth
- Citizenship
- Address.

The applicant needs to indicate his travel ID document (the passport) and attach a copy to the paper request.

The Italian D.L. 25/6/2008 n. 112 specifies how foreign citizens can apply for an Italian ID (and eID) card. it is necessary that the applicant is present in person to submit the relevant form and provides the passport, a residence permit. The ID card cannot be used for travel purposes.

The unavailability of eIDs in a Member State for internal reasons can be a serious reason for citizen exclusion from the access to cross-border online services, therefore there is a strong rationale for introducing such a rule in the EU regulation. However it needs to be recognised that, despite the positive inclusion impact, this option will have heavy implementation costs at national level, due to major changes to be introduced in the procedures to issue eIDs.

The effectiveness of the option is low and is a kind of substitute measure for countries where no formal eID can be obtained.

Even though this option would be very beneficial to ensure the inclusion of citizens whose country does not issue formal eIDs, its implementation would be extremely complex and raise a large number of issues

[43] http://www.bundeskanzleramt.at/site/6085/default.aspx

among the EU Member States. The effectiveness of the option is low and is a kind of substitute measure for countries where no formal eID can be obtained. The option is not shortlisted.

5.2.3.6 *General assessment of option D1*

- Implementation
  - Under the umbrella of the EU eID regulation
- Pros
  - Would counter the potential exclusion of citizens who do not obtain eIDs from their home country from electronic cross-border public services
- Cons
  - Would require complex negotiations with member states and the national eID award procedures.

5.3 Option C: cease all EU activities in the field of eID, including those already started.

This option would affect eID related initiatives supported in the context of CIP ICT-PSP, such as STORK or future large scale projects concentrated on eID, as well as stop any legal and political action in the field of eID cross-border interoperability and Member State cooperation and coordination.

5.3.1 Aspects related to EU policy making

The analysis shows that no regulatory action on eIDs at EU-level combined with a complete stop of related actvities would go against the ongoing policy initiatives aiming to a stimulation of a better functioning of the European Single Market and the establishment of a prosperous Digital Single Market.

In case of no-action on eID issues the consequences would be

- Leaving the solution of eID interoperability to market or institutional forces, with huge uncertainties in respect to the creation of a level playing field, of creating equal opportunities for European citizens and enterprises
- Some eID-based cross-border public eServices might nevertheless emerge, but lacking a common framework would lead to fragmented and non-interoperable solutions, in fact further increasing the barriers and obstacles to the creation of a single market
- Some institutions might refrain from engaging in the development of cross-border online services because of the effort required to overcome the legal, liability and operational issues of the building blocks of the services they are developing.

This policy option would imply the halt of any eID related initiative supported by the EU such as the Large Scale Pilots funded under the CIP ICT PSP (in particular STORK, but also affecting pilots as SPOCS, eCODEX, epSOS and to a lesser extent PEPPOL) and it will hamper the objectives of the future Connecting Europe Facility (CEF) such as filing the gaps that are needed for the European Digital Single market (in which eID has a pivotal role) as well as the objective of the CEF to act as a catalyst for further funding from the private and public sector by giving infrastructure projects credibility and lowering their risk profiles.

The option will result in leaving the Member States and their administrations on their own in the attempt to create an overall framework for the cross-border use of eID and the take up of seamless cross-border online public services.

5.3.1 Effectiveness of the Option

This option is similar in effectiveness to Option A, maintaining the status quo. In some aspects it may be even less effective in overcoming the identified barriers to EU-level cross-border eID interoperability. Liability issues would not be resolved, or in a fragmented way, and technological solutions would be fragmented along the same lines.

The assessment has led to discarding option C, concerning no further regulation and no recommendation, as well as ceasing all EU activities in the field of eID, including those already started. Option C would create serious issues to mainstream EU policy. It would also go against the policy indications and the strategies of the construction of the Europe 2020 strategy, the European Single Market, the Digital Single Market, the Digital Agenda for Europe and the comprehensive eGovernment strategy.

These strategies and policies clearly state that it is one of the purposes of the EU to deal on the one hand with the development of cross-border public services, and on the other with trust and the eService key enablers, such as eID and eAuthentication.

In the overall framework of EU development policies, the option of stopping any eID-related regulation development, as well as all the practical policy-related implementations do not seem justified and feasible.

Overall this option is not effective in overcoming the identified barriers and in creating a level playing field at the EU level for cross-border eID use. The option is not shortlisted.

5.4 Option D: Additional options and out of the Box options

The study work as led to a number of out-of-the-box measures which could be taken to address the different issues related to eID mutual recognition and acceptance across borders, the supply and demand of eID enabled online services and the integration of public and private initiative and activities on eIDs.

5.5 Out of the box measures

5.5.1 D1: regulation to ensure recognition of QAA levels

This option implies that Member States would have to cater for some or all of the QAA levels, using the QAA levels as one interoperability criterion for the infrastructure. STORK has shown that the eID landscape is extremely fragmented, responding to different rules, different QAA levels, different eID setups and approaches to eAuthentication. In STORK, 6 pilots function following a MW and a PEPS approach, and use different credentials (mobile, smart card, Username password) as well as with different QAA levels.

STORK has worked on and with the QAA levels 1-4 and sees this as one of its important achievements. The QAA levels seem to also have been taken up outside STORK (in the Netherlands) . The QAA levels allowed in STORK for comparison and a basis for exchange of services.

The introduction of different QAA levels may help creating the trust base and relating trust, liability and system assurance and provide a criterion for eID interoperability, in case of different requirements of assurance of the transaction, according to the associated institutional or monetary value.

On the other hand it needs to be recognised that Member States might requires the highest security level for certain levels of transactions or types of services.

The "policy making" cost of introducing different QAA levels for mutual recognition might be very high in respect to the actual benefit for the cross-border use of eIDs.

Despite the complications, this option is proposed for consideration. As it could facilitate the introduction and uptake of cross border eID (by allowing each country to set its own levels and criteria for acceptance, as well as liability).

5.5.1.1 General assessment of option D1

The security of the eID is an issue. The FAQ of the Austrian "Bürgerkarte" indirectly confirms that there needs to be a constant monitoring of the eID system to guarantee the integrity the all the components and processes of qualified signatures[44].

- Implementation
  - Under the umbrella of the EU eID regulation
- Pros
  - Will support the construction of a "trust system" in EU cross-border services of public and private nature, for the benefit of all stakeholders
  - Will provide certainty in the setup of eID systems and in cross-border transactions
- Cons
  - Requires a supervision system, with the relevant procedural, organisational and technological aspects
  - Will require significant investment costs to build and maintain the certification and supervision.

5.5.2 D2: allow private parties to issue formal cross-border interoperable eID

In this option, private parties would be allowed to issue formal eIDs for cross-border use. Governments would need to recognize such private eIDs and allow them to be used in dealings with the state

The analysis has shown that the private sector, in absence of a general regulation and a direct supervision and assumption of liability by a State Administration is not considered sufficiently reliable and trustworthy to confirm the assumption. In Austria, a eID card issued by a private entity can be activated as a *Bürgerkarte* to be used in transactions with Public Administrations, but this activation needs to be approved by the Austrian SourcePIN authority, which is part of the data protection authority.

A study by IPTS – Sevilla has concluded that "in order to fight market fragmentation as a result of the private sector creating piecemeal schemes rather than generic, interoperable infrastructure, governments should provide those components of trusted infrastructures that are too risky or costly for private sector organizations to develop.", thus giving the Public Administration a core role in the establishment of eID systems and in assuring them.

[44] "Kann man Bürgerkarten fälschen? Die konkreten Ausprägungen der Bürgerkarte verwenden signierte Daten auf der Karte. Die Sicherheit der technischen Komponenten und Verfahren für die Erzeugung qualifizierter Signaturen muss nach dem Stand der Technik laufend geprüft und von einer Bestätigungsstelle bescheinigt sein. Dadurch sind Fälschungen praktisch auszuschließen. http://alt.buergerkarte.at/de/hilfe/faq.html#2.05

Given the overall requirement by Member States to mutually recognise formal eIDs and the need to find common regulatory and operational principles to make the cross-border eAuthentication work, allowing private parties to issue formal eIDs would issue additional complexities and would hamper the mutual recognition process of eIDs and eAuthentication. Especially for the risk of fragmentation and a cloudy landscape the option should be discarded.

5.5.2.1 General assessment of option D2

The security of the eID is an issue. The FAQ of the Austrian "Bürgerkarte" indirectly confirms that there needs to be a constant monitoring of the eID system to guarantee the integrity the all the components and processes of qualified signatures[45].

- Implementation
  - Under the umbrella of the EU eID regulation, and upon action of the EU Member States
- Pros
  - Will increase the critical mass of eiD systems development
  - Will improve the engagement of the private sector, favouring the integration of proprietary eID systems with the public eID systems and the development of eID-based applications
- Cons
  - Complex institutional and regulatory setting
  - Liability issues due to long chain of responsibilities
  - Needs to be integrated into the supervision system

5.5.3 D3: supervision at the EU level

In this option, supervision at the EU level, a supervisory body would be created at the EU level. There are two alternatives: maintain eID supervision at national level, leaving it within the comprehensive liability scheme, or create a supervisory body at EU level.

According to the principle of subsidiarity, it does not seem essential to centrally coordinate the mutual recognition and interoperability of eIDs and eAuthentication. It is well possible to leave the supervision and enforcement at Member State level. Even if STORK emphasises the need for maintenance and governance, as well as for appropriate supervision and auditing procedures, there is no case for the institutional solution required.

The SSEDIC report indicates that a majority of experts are in favour of an EU body/agency taking responsibility for eID coordination, certification of identity providers, determination of assurance levels of an eID and for standards.

A supervisory body would be needed, as in the Austrian case, to enable the "formal" use of privately issued eIDs.

Supervision could well reduce the individual liability of Member States and operators of the eID systems.

However it needs to be acknowledged that the "policy making costs" of a EU supervisory body might be quite high, due to the need to monitor national supervisory bodies and to cover the entire EU.

The sub option should however NOT be discarded as it could solve some fundamental issues and in the long run might proof tp be the backbone of a EU wide eID system.

[45] "Kann man Bürgerkarten fälschen? Die konkreten Ausprägungen der Bürgerkarte verwenden signierte Daten auf der Karte. Die Sicherheit der technischen Komponenten und Verfahren für die Erzeugung qualifizierter Signaturen muß nach dem Stand der Technik laufend geprüft und von einer Bestätigungsstelle bescheinigt sein. Dadurch sind Fälschungen praktisch auszuschließen. http://alt.buergerkarte.at/de/hilfe/faq.html#2.05

5.5.3.1 General assessment of option D3

Supervision is about implementing a third party-guarantee for the operation of eID systems and more in general of EIAS services. The third-party certification issue is particularly important in electronic transactions.

- Implementation
  - Under the umbrella of the EU eID regulation, and in cooperation with EU Member States
- Pros
  - Will increase trust and security, not only among citizens and businesses but also between applications and cross-border online services providers
  - If appropriately communicated, it will draw stakeholders towards cross-border services and support their development
- Cons
  - Complex institutional and regulatory setting
  - Requires a significant investment in the development of procedures, in the establishment and operation
  - Not a sufficient number of cross-border online services to justify the costs.

5.5.4 D4: immediate implementation of mutual recognition of eIDs

This option involves creating the conditions for an immediate implementation of mutual recognition of eIDs and eAuthentication. The implementation of mutually recognised eIDs in the European Union might be based on a compulsory mutual recognition of other Member States' formal eIDs.

The EU Directive or Regulation might impose the mutual recognition.

5.5.4.1 General assessment of option D4

This option would ensure the immediate establishment of a level, supporting playing field for eID in the European Union.

- Implementation
  - One possible direct purpose of the EU eID regulation
- Pros
  - The mutual recognition would happen in the same time frame, without any Member State lagging behind
  - Fragmentation would be avoided
  - Discrimination would be avoided
- Cons
  - The "cost of policy making" would be quite high both at EU level and at Member State level. In some cases outside of the policy or budget priorities of some States. This option would oblige Member States to set-up their own national eID, regardless of the advance of eID-based online services and the availability of the necessary budget.
  - There could be significant operational, practical and technological issues, which can endanger the operation of the system as a whole.

- The absence of significant levels of cross-border public services in terms of numbers of transaction will result, from some Member States, in a loss of investment.
- The risk of this approach would be an "empty" unimplemented regulation.

5.5.5 D5: progressive implementation of mutual recognition of eIDs

This option consists of basing mutual recognition of eIDs and eAuthentication on a "progressive" implementation of the rule and therefore with a gradual introduction. The option is to create a voluntary group of Member States willing to mutually recognise their national "formal" eIDs.

A key

The procedure would equal to a "notification", where the Member State notifies the adherence to a mutual recognition scheme.

5.5.5.1 General assessment of option D4

The option will cater for a gradual introduction of mutual recognition and interoperability of eID in the European Union, allowing the Member States wishing to develop their eID over time to join the system at a later stage.

- Implementation
  - One possible direct purpose of the EU eID regulation
- Pros
  - The scheme would be quickly operational
  - The "cost of policy making" would be relatively low
  - It could lead to the creation of a nucleus of close Member States which would then create the critical mass to support the implementation of eID-based cross-border services
- Cons
  - The high risk of exclusion and discrimination
  - The risk of permanent exclusion
  - An increased difficulty of accepting the issuance of eIDs to non-nationals.
  - The risk of this approach is a closed club, excluding all the others incapable of complying with its rules.

5.5.6 D6: technology push

This option consists of operationalizing the "building blocks" developed in STORK, relying on the drive provided by the technological and operational solutions developed by the STORK consortium.

STORK has developed several common building blocks. The common basic building blocks include

- Member state package: This package allows new member states to quickly establish their own STORK node. The software, configuration files, etc of both these systems are included in the package. Finally a toolkit is included, with examples, testing tools and test credentials.
- Integration packages: Integration packages are meant for those organisations which want to integrate STORK into their systems. This package is to be used by Service Providers who want to allow foreigners to access the personalised part of their website, using their national credentials, as well as industry partners who want to integrate STORK into their products, and offer this integration to their customers. The package of course includes the software to connect to the national STORK node, and a toolkit with examples, testing tools and test credentials.

These blocks and packages can be operationalized with or without being accompanied by regulatory measures or formal standardisation. By implementing the STORK solutions, one would create a technology push with ad hoc standards as developed in the pilot. This option would give the outcomes of the STORK Large Scale Pilot a central role in the integration of European eIDs. The technology developed and its trust-building functions could be further diffused to come to a mutually recognised system.

There would be significant practical advantages, since the outputs of STORK would be further deployed. From the economic point of view there would be the advantage of technology reuse. And since the STORK stakeholders are the main European players in national eIDs a lot of the sharing and integration work would be already completed.

This option would give the outcomes of the STORK Large Scale Pilot a central role in the integration of European eIDs. The technology developed and its trust-building functions could be further diffused and supported to come to a mutually recognised system.

There would be significant practical advantages, since the outputs of STORK would be further deployed. From the economic point of view there would be the advantage of technology reuse. And since the STORK stakeholders are the main European players in national eIDs a lot of the sharing and integration work would be already completed.

However, further support for these building-blocks is only effective when regulatory arrangements are made with regards to the liability of eID service providers. Infrastructures and technologies developed in STORK will not be used in any significant degree as long as this issue is not resolved. This means that this option is only effective in conjunction with option B, and not with option A or C.

5.5.6.1 General assessment of option D4

The option will allow to leverage the investment by the CIP ICT-PSP programme in STORK and STORK 2.0, supporting the use of operational, procedural, regulatory and technological solutions.

- Implementation
  - A joint decision by the EU and the STORK consortium, possibly embedded into the overall European eID regulation.
- Pros
  - Leveraging the STORK investments
  - Availability of a tested set of solutions, already validated by the Member States participating in STORK
  - Cost savings by Member States and Administrations taking up the solutions developed by STORK (application and software reuse)
- Cons
  - Objections by Member States and Administrations outside STORK
  - Harmonisation issues related to incompatibilities with national systems
  - STORK solutions might be seen as "proprietary" and thus not properly received.

5.5.7 D7: partnership with the telecom sector

The partnership would be with telecom and internet service providers. This would create a significant advantage in using mobile payment systems. It would be based on an existing, secure infrastructure and applications.

This option implements a relationship with private sector entities. There could be significant benefit in involving entities with high technological capabilities and managing high volumes of identities, electronic identities, authentication processes and transactions, taking advantage of economies of scale and deployment capabilities.

However, the private nature of these players is a new factor in the management of eIDs and eAuthentication and this will create increased problems of mutual recognition and integration. This is why this option is not shortlisted.

5.5.7.1 General assessment of option D7

The option will allow to leverage the skills of the Telecom sector in mobile electronic Identification and payments. Due to the diffusion of mobile phones it would support the creation of a critical mass of users, which is beneficial for the development of electronic public services.

- Implementation
  - Mainly by Member States operating eID schemes
  - Supervision by the EU
- Pros
  - Helps achieving critical mass of users
  - Significant implementation effectiveness
  - Ease of practical integration
  - Ease of integration into services
- Cons
  - Significant policy and management effort by Member States
  - Risk of lack of independence by the Telecom sector
  - Excessive length of the operational chain and therefore of the liability chain
  - Complex liability regulation actions

5.5.8 D8: partnership with the banking sector

It has already been recognised that many European citizens use bank cards and credit card for e-identification purposes. This would further integrate the private and public sector use of eIDs leveraging the high security levels of bank card networks and applications. Banks provide and/or manage one of the most used eID means: credit cards and bank cards. Telecommunications providers, and in particular mobile telecommunication providers, have the potential to be important players in eIDs. This option involves setting up a partnership with the banking sector (or the part of it that is government-owned). It has already been recognised that many European citizens use bank cards and credit card as eIDs. This would further integrate the private and public sector use of eIDs leveraging the high security levels of bank card networks and applications.

However, the private nature of these players is a new factor in the management of eIDs and eAuthentication and this will create increased problems of mutual recognition and integration. This is why this option is not shortlisted.

The option will allow to leverage the investment by the CIP ICT-PSP programme in STORK and STORK 2.0, supporting the use of operational, procedural, regulatory and technological solutions.

5.5.8.1 General assessment of option D8

The option will allow to leverage the banking sector in electronic Identification and payments. Due to the diffusion of online and remote banking, it would support the creation of a critical mass of users, which is beneficial for the development of electronic public services.

- Implementation
  - Mainly by Member States operating eID schemes
  - Supervision by the EU
- Pros
  - Helps achieving critical mass of users
  - Significant implementation effectiveness
  - Ease of practical integration
  - Ease of integration into services
- Cons
  - Significant policy and management effort by Member States
  - Risk of lack of independence by the banking sector
  - Excessive length of the operational chain and therefore of the liability chain
  - Complex liability regulation actions

5.6 Conclusions

The above discussion of the different policy options is summarised in in two tables.

First there are the policy options from the Terms of Reference:

Short name	Description	Shortlisted?	Reason for (not) shortlisting
A: Maintaining the Status Quo	Keep the status quo, proposing no policy change. Continuation of eID-related activities, but no specific regulation.	Yes	Baseline scenario
B: Regulation on Cross-Border Recognition of formal eID	Support the formulation and implementation of legislation on cross-border and cross-sector mutual recognition and acceptance of formal eID to enable citizens and businesses to use their "formal" eIDs not only in their home country but in all other Member States.	Yes	Anticipated effectiveness and alignment with EU policy objectives
B1: Regulation of cross-border recognition	Legislation to ensure cross-border recognition and acceptance of formal eID.	Yes	May form the basis of pan-EU eID infrastructure (despite some issues)
B2: Allow private parties to use formal eID	Allow private use of formal (cross-border) eID, enabling private organizations to use government-recognized or issued eID	Yes	May increase effectiveness
B3: Regulation to provide each citizen with at least one eID for cross-border use	Legislation to capture the necessity to provide each citizen with at least one “formal” eID which can be used to access cross-border online services.	No	Substitute measure, not effective
C: Do nothing	Full stop of all EU activities in this field including repealing the eSignatures Directive and support projects such as STORK.	No	Not effective

Second, a number of other policy options were considered by the study team, including "out of the box" scenario's:

Short name	Description	Shortlisted?	Reason for (not) shortlisting
D1: Regulation to ensure recognition of QAA levels	Legislation to ensure recognition of some or all of the STORK QAA levels, using the QAA levels as one interoperability criterion for the infrastructure.	Yes	Has complications, but may be effective
D2: Allow private parties to issue formal eID	Allow private parties to issue cross-border formal eID. Governments would need to recognize such private eIDs and allow them to be used in dealings with the state.	No	High risk of fragmentation
D3: Supervision at the EU level	Supervision at the EU level; a supervisory body would be created at the EU level.	Yes	May be very effective, even though "policy making costs" are high
D4: Immediate implementation of mutual recognition of eIDs	Creating the conditions for an immediate implementation of mutual recognition of eIDs and eAuthentication		
D5: Prorgressive implementation of mutual recognition of eIDs	Basing mutual recognition of eIDs and eAuthentication on a "progressive" implementation of the rule and therefore with a gradual introduction.The option is to create a voluntary group of Member States willing to mutually recognise their national "formal" eIDs.		
D6: Technology push	Operationalize the "building blocks" developed in STORK (i.e. technology push)		
D7: Partnership with the telecom sector	Engage in a partnership with the telecom sector (telecom/internet service providers)	No	High complexity
D8: Partnership with the banking sector	Partnership with the banking sector (or the part of it that is government-owned)	No	High complexity

6 SECTION 5: ANALYSIS OF IMPACTS

6.1 General setting: drivers of eID-enabled services

eID is ranked highest and second highest by citizens and business as the most relevant eGovernment service.[46] In first instance formal eID is needed for accessing and using eGovernment services. The use of eID is therefore related to the availability and use of eGovernment services, if citizens and business do not use eGovernment services they will have no or less need for formal eID. The current uptake of (national) eGovernment services (2009[47]) is approximately 35% amongst citizens and 65% amongst businesses (although for large and medium size companies the uptake is over 80%). Especially for citizen services there is scope for increased availability and uptake of eGovernment services (there is 37% untapped demand in the current situation[48]) as well as stimulating uninterested citizens to use online services. It is likely that the figures of uptake of eGovernment services amongst intra EU migrants will likely be higher compared to national citizens.

6.1.1.1 Intra EU Immigrant population as beneficiary of cross-border electronic services

eID cross border recognition and acceptance would affect European citizens and business. Within the EU approximately 12,5 Million EU citizens lived in another EU country in 2009[49], many of them potential beneficiaries from cross border eID usage, while the group that most benefits (those citizens that are in the process of migration counted for 1,2 Million citizens in the same year, as shown in the following table:

	Immigration from EU27 States
Austria	42,265
Belgium	65,611
Bulgaria	380
Cyprus	6,911
Czech Repub.	24,477
Denmark	25,642
Estonia	2,338
Finland	12,637
France	94,482
Germany	167,642
Greece	53,754
Hungary	15,932

[46] RAND, United Nations University, Maastricht University (2009) "Innovative and adaptive PEGS for citizens in 2010 and beyond: Evolution of PEGS: Impact Assessment for cross-border and Pan-European service

[47] Source: Eurostat: http://epp.eurostat.ec.europa.eu/statistics_explained/index.php /E-government _statistics#Use_of_online_services_by_the_citizens

[48] Eurostat: http://epp.eurostat.ec.europa.eu/statistics_explained/index.php /E-government _statistics#Use_of_online_services_by_the_citizens

[49] Eurostat migr_pop1ctz

	Immigration from EU27 States
Ireland	23,211
Italy	152,962
Latvia	1,476
Lithuania	3,845
Luxembourg	14,537
Malta	4,032
Netherland	65,800
Poland	33,675
Portugal	17,866
Romania	2,896
Slovakia	7,552
Slovenia	3,201
Spain	128,246
Sweden	35,233
United Kingdom	198,624
Total	**1,205,226**

Figure 6-1: Intra-EU immigration

Source: Eurostat for population and immigration data[50]

On top of the immigrants, there is a large group of over 500.000 regularly commuting citizens, from the country of citizenship or residency to the country of work, where they need their eID to be recognised in order to access eGovernment services related to their cross border employment.

The 9th Benchmark Measurement on digitizing public services in Europe[51] identified 25 services (14 citizen and 11 business) that would or could require cross border recognition of a formal eID at one or more instances. Many of these services are irregular services (probably only to be used once or twice), often, in the case of immigrants, at the time of immigration or with specific events, whereas others are yearly returning interaction with the government services in the country of residence.

The CAP GEMINI benchmark reports on the relationship between these services and the optional or mandatory usage of eIDs.

For most of these 25 public services eID is horizontal enabler to access the service. In general, 75% of EU countries have eID as key enabler in place. According the eGovernment Benchmark 2008, eID is mandatory for 25 basic public services (see below[52]). The efficiency of the online version of these public services for cross border use will only be realised when cross-border interoperable eID is available. In most EU countries (, public online services for businesses are equally supported by eID. VAT, company

[50] http://epp.eurostat.ec.europa.eu/portal/page/portal/product_details/dataset?p_product_ code=MIGR_IMM5PRV

[51] Digitizing Public Services in Europe: Putting ambition into action. 9th Benchmark Measurement | December 2010. Capgemini, IDC, Rand Europe, Sogeti and DTi

[52] Cap Gemini: Smarter, Faster, Better eGovernment, 8th Benchmark Measurement | November 2009, http://ec.europa.eu/information_society/eeurope/i2010/docs/benchmarking/egov_benchmark_2009.pdf

registration and corporate tax can be accessed with an eID in more than half of the benchmarked countries. However, these services are mostly rooted at national level and since the percentage of cross border branches of EU companies is estimated at around 0,5% (102.000 in 2007[53]) of all EU companies there is little evidence that they will scale up to cross-border use to similar levels[54].

6.1.1.2 Relevant Services for Citizens

Relevant services for (im)migrants and commuters include:

Moving and residence

	Service	eID requirement[55]
1	Register a change of domicile	Mandatory
2	Request ID documents (residence card)	mandatory
3	Enrol as a student	Mandatory
4	Vehicle taxes payment (special declaration)	Mandatory
5	Applying for or transferring a driver's licence	Optional, not listed
6	Order a birth certificate	Mandatory
7	Register a death	Mandatory
8	Register real estate purchase	Optional, not listed
9	Register for Legal Aid	Optional, not listed

Figure 6-2: Moving and residence related services

Health

10	Electronic prescriptions	Mandatory
11	Access to patient summary	Mandatory

Figure 6-3: Health related services

Employment

12	Work permit Application	Optional, not listed
13	Income Tax Declaration	Mandatory
14	Register for a pension	Mandatory

Figure 6-4: Employment Services

6.1.1.3 eID-enabled cross-border services

Cross border Business Services include

[53] http://ec.europa.eu/internal_market/company/docs/business_registers/20110224_impact_en.pdf
[54] Capgemini 2010 - Digitizing Public Services in Europe - 9th Benchmark Measurement
[55] Cap Gemini: Smarter, Faster, Better eGovernment, 8th Benchmark Measurement | November 2009, http://ec.europa.eu/information_society/eeurope/i2010/docs/benchmarking/egov_benchmark_2009.pdf

Procurement

1	Submitting a tender for public procurement	Mandatory

Figure 6-5: Procurement Services

Business and start-up

2	Register a new legal entity	Mandatory
3	Corporate/business tax declaration	Mandatory
4	Register for VAT	Mandatory
5	Submit VAT declarations	Mandatory
6	Register a new employee	Optional, not listed
7	Pay social contributions for employees	Optional, not listed
8	Report termination of employee(s)	Optional, not listed
9	Register a new vehicle	Mandatory
10	Register a real estate purchase	Optional, not listed
11	Consult the business register	Optional, not listed

Figure 6-6: Business and start-up services

Indicative numbers of potential cross border use of eID can be Based on the types of services and type of user (migrant or commuter): 1,2 million changes of domicile and registration for residence card or driver's license transfer per year (immigrants), 1,7 million (immigrants and commuters) income tax declaration, etc.

Based on the above indications and preliminary analysis on cross-border online services there is some evidence of untapped demand (35% of citizens said they are not using eGovernment services but indicate they are interested to do so[56]). It is expected that around 650.000 citizens (including immigrants and commuters) are most likely to use one or more of the above listed eGovernment services for which eIDs are requested for the access to *online* cross-border services.

Subject of our study are national eIDs issued by, on behalf or under the responsibility of a Member State (e.g.e-identity card, citizen cards, public service cards, mobile-IDs) and used in another Member State for the completion of electronic procedures or transactions when e.g. studying, working, travel or do business abroad.

The benefits for using cross border eID are of economic, social and environmental nature: There are significant reductions of cost, increases of efficiencies (time, certification of documents etc) and other benefits regarding mobility, inclusion and citizen participation outside the country of origin combined with environmental impacts (less paper, less travel etc). In the sections below they are further elaborated per policy option.

[56] Eurostat: http://epp.eurostat.ec.europa.eu/statistics_explained/index.php/E-government_statistics#Use_of_online_services_by_socio-economic_groups

6.2 Option A – baseline scenario: keep the status quo, proposing no policy change. Continuation of eID-related activities, but no specific legislative measures

6.2.1 Economic Impacts

The lack of an EU wide regulatory framework would seriously hamper the uptake of cross border eGovernment services and thus the mobility and integration of citizens and businesses within the EU, leading to less (or slower) increase of economic activity and growth. As indicated in the tables in the previous section, eID is required to access and use a number of eGovernment services. Using the online eGovernment services provides benefits (cost and time reduction) for both the eGovernment back office and the citizen or business. For example 1,2 million online domicile registrations each year will save considerate time and cost on the citizen side (travel, waiting, expressing in a foreign language) as well as time and cost on the public administration side (no face to face and front office activities), whereas with a full eID infrastructure and mutual recognition the process can be completed online.

The principal economic impact would be:

- Slow-down of the integration of the EU Single Market and of the Digital Single Market: Copenhagen Economics[57] estimates the cost of failure to complete it is expected to be at least 4.1% of GDP between now and 2020, i.e. EUR 500 billion or EUR 1000 per citizen
- Reduced benefits for the EU ICT sector, due to uncertainty limiting investment in cross-border public eServices.
- Non-achievement of economies of scale
- Risk of loss of part of the investment in eID systems (STORK)
- Risk of loss of the EU investment in eID systems (STORK)
- Increased implementation costs for new and other ICT-PSP pilots, which have to develop their own eID solutions

In addition there will be extra costs for developing national and or regional solutions, extra cost for ensuring interoperability and levels of trust. This also pertains to the issue of liability. If no EU regulation deals with the issue, it will create a major risk and uncertainty for governments and administrations.

The economic impacts for this option would be less negative compared to option C (as a basic infrastructure will be built and maintained, and interoperability issues tackled). This is related to the implementation achievements of eID-related projects supported by the EU, which will produce concrete applicable results, such as eID technologies, eAuthentication technologies, interfaces, pilot applications, etc.. The downside of continued support of the European Union to policy related experimentation could worsen the effects of a lack of coordination, since it would drive forward implementation and piloting activities without ensuring the necessary framework for their take up.

6.2.2 Social Impacts

The social impacts of option A will certainly determine a set of impacts related to the specific implementation activities. These impacts are related to

- The development of skills in the field of technology, of eGovernment applications
- The elaboration and transfer of best practices
- The interconnection and coordination of key players in the domain who will decide about their joint activities.

[57] "Economic Impact of a European Digital Single Market", 2010, Copenhagen Economics

However it needs to be highlighted that a lack of regulatory measures will maintain uncertainty, fragmentation and lack of trust, causing on the one hand an uneven field for citizens and for business players, and on the other the discrimination and exclusion of citizens and enterprises because of decisions of single Member States.

Option A will also determine a set of negative impacts

- Exclusion from access to cross-border online services of the 12.5 Million EU citizens living in another EU country[58]
- Limitation of access to cross-border eServices by citizens and enterprises of Member States which have not entered eID agreements
- Discrimination of citizens having mutually recognised eIDs and citizens unable to obtain such an eID
- Limitation and hampering of the progress towards the European citizenship. In other terms the goal of the creation of the European Single Market are economic and non-economic, but they include the implementation of the European citizenship, which aims at guaranteeing all citizens the freedom to work, live, do business, retire, be cured, vote, access services, regardless of the physical location within the European Union. The European citizenship will not be operational if citizens are physically constrained by their country of origin or by the services available in the geographical areas in which he is currently in.

6.2.3 Impacts on the administrative burden

The lack of common legislation for the cross-border use of national eIDs can hinder the diffusion and take-up of services, most of all of those services requiring economies of scale and a certain critical mass for their effective deployment.

Reduction of administrative burden (ABR) is an essential element of EU policy. ABR has to be realised both at the public administration and the user (citizen and businesses) side. The digitisation of government services is partially driven by the need to reduce the burden and operate more efficiently. As indicated above, eID is required for the access and activation of several services. Some of these services are essential for cross border activities. Without cross border recognition of eID, these services cannot be provided and used in their online version and have to be provided and used in the traditional manner, thus not contributing to ABR. Several current CIP ICT PSP projects (such as ISAC6+ and Rural Inclusion) are currently developing methods to measure the actual ABR. The Rural Inclusion project for instance as measured up to 90% time savings for business registration processes and 25-30% for tax registration, each of these services are supplied at national level using eID. In a cross border environment, the lack of operating cross-border eIDs can thus lead to inability to use cross-border public eServices and therefore ABR for these cross border services cannot be realised (to its full potential) burden.

The continuation of the baseline scenario might paradoxically lead to an increase of administrative burden for public administrations. In some countries (as Luxembourg) for example certain services as VAT declarations are only provided online. If due to the lack of cross border eID these services cannot be used by cross border companies (branches), the Public Administration will have to deal with multi-channel delivery and multichannel processing of the service thereby increasing the administrative burden..

[58] Eurostat migr_pop1ctz

6.2.4 Impacts on environmental sustainability

In case of Option A the lack of harmonisation and integration would not allow to achieve the expected environmental sustainability benefits. Citizens will have to travel, correspond and work with paper dossiers.

This means that

- the impossibility to use electronic forms and applications will require to use paper forms which need to be handed in and stored. This will consume paper, require the use of storage space
- citizens and businesses will have to use public and private transport means to interact with administrations, and
- that citizens and enterprises will have to travel back to their home country to obtain certain services.

The benefits will concern

- less need for mobility for administrative reasons
- more time to work or for leisure do to faster on-line interaction with administrations.

6.3 Option B: legislation on cross-border and cross-sector mutual recognition and acceptance of eIDs to enable citizens and businesses to use their "national" eIDs not only in their home country but in all other Member States.

Responses to the Public Consultation on eSignatures and eID indicate a clear support for regulation on the cross-border use of eID. Although SME's are slightly less positive than larger companies or governments, overall there appears to be a clear support.

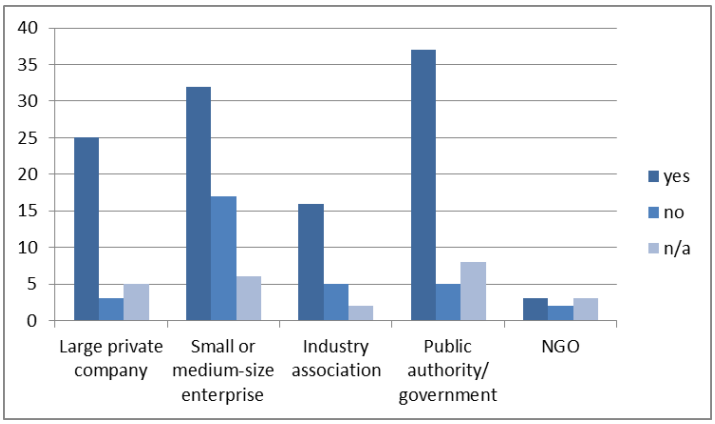


Figure 6-7: Perceived need for additional regulation on eID at the EU-level (Public Consultation)

The chart shows how the vast majority of companies, of public authorities and governments would require a specific regulation of cross-border eID in Europe.

6.3.1 Economic Impacts

The Economic impact of eID-enabled applications depends in the supply of cross-border public services, on the number of cross-border transactions and on the service demand by citizens and enterprises. First of all cross-border public services need to be available. In itself eID and eAuthentication are only necessary in relation to actual (cross-border) public services and to significant amounts of cross-border transactions, which are related to the actual demand and thus to the mobility of citizens:

- Number of cross-border services
- Number of cross-border service requests (demand)
- Development of the national interconnection module implementation: in other terms, the development and operation of a national eID infrastructure and of the interfaces with the EU-level eID interoperability infrastructure.

Indirect economic impacts will be captured by:

- the reduced cost and barriers and therefore increased mobility of people and businesses
- the contribution to growth in the EU by facilitating the increase in economic cross border activity

Responses to the Public Consultation on eSignatures and eID indicate that both governments, public authorities and businesses expect a reduction in barriers because of increased user convenience and simplification of access to online services.

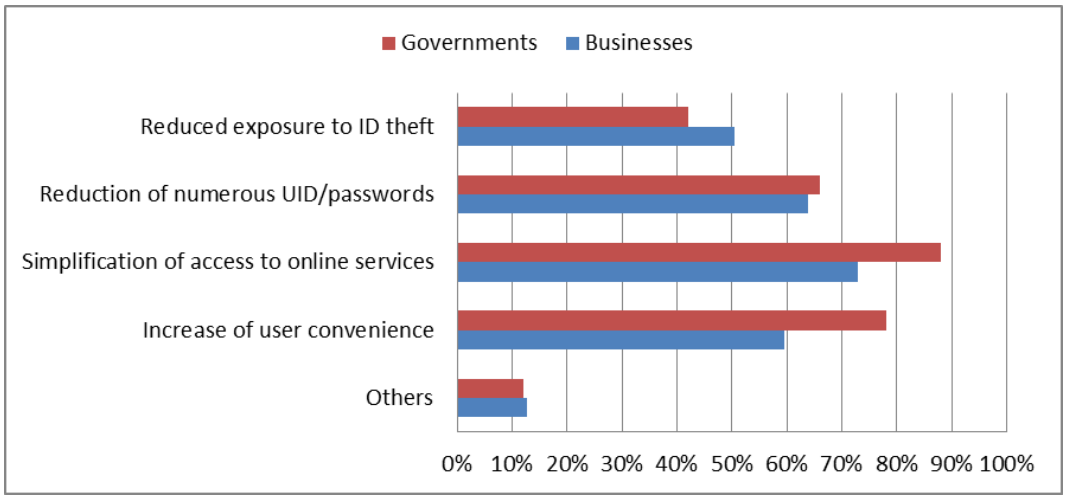


Figure 6-8: Expectations with regard to cross-border recognition of eID (Public Consultation)

In this respect the numbers depend on the availability development of online services (the number of cross-border online services provided and the number of requests per service per year) that require eID and cross border recognition. The eGovernment study states that cross-border eProcurement still plays a minor role in most countries (estimated at 3% in 2004). [59]. The pilot applications of STORK, although non-representative for the potential demand, have shown that personal register services are the most requested, even if most pilots saw a relatively low number of unsolicited service requests. The reasons for this may be related to the relatively low awareness of users and to the fact that the first edition of STORK mainly focused on the technical interoperability layer.

The European Commission focus group confirmed a potential demand for personal registry services. The dimension of this demand is however difficult to estimate.

In any case the demand for cross-border eServices is potentially high and is directly correlated to the demand for internal mobility.

[59] A report on the functioning of public procurement markets in the EU: benefits from the application of EU directives and challenges for the future;
http://ec.europa.eu/internal_market/publicprocurement/docs/concessions/SEC2011_1588_en.pdf

- For eProcurement there seems to be a limit to the amount of cross-border transactions (3% of total procurement)[60].The cross-border access to this market is still limited, even if there should be a high growth potential once barriers such as language, regulations, qualification and dispute resolution are solved
- For eHealth the demand seems directly related to temporary residence in another Member State. At present it is related to tourism and possibly to temporarily defined business mobility; the potential number of cross border prescriptions is estimated at 4,3 Million per year[61].
- For eJustice, demand depends on the numbers of cross-border legal procedures. eCodex is now automating the procedures through semantic interoperability. The demand of eID for eJustice largely depends on cross-border disputes
- For Business mobility, relevant eServices such as SPOCS receive the demand of mobile businesses which have the objective to operate in other Member States (102.000 cross border EU branches, cross border service delivery estimated at 650000 requests per year, assuming a conservative estimate that each business will not cover more than 1,5 countries and that repeated requests will be handled.
- For citizen registry services we have identified several relevant cross border services (domiciliation, birth, death, marriage, real estate transfer etc.) ; the total number of transactions is estimated at around 1,4 million per year

The overall economic impact furthermore stems from the effort of the ICT industry and from the benefits for citizens when using cross-border services instead of having to access administrations directly. These dimensions are strictly related to investment, service availability and demand.

JRC/IPTS[62] has ascertained that eID infrastructure technologies, embedded in operational applications and services, will be critical to the development of broader eID applications, which are likely to emerge as a 'critical mass' of infrastructure becomes available. Increased portability of credentials and use of federated identity schemes would result in higher take-up and more extensive use of eID solutions, thus contributing to market growth. However it confirms that there is a lack of a compelling, well-defined and accepted business case for federated eID. Few organizations or governments are willing to speculatively invest.

As shown by Figure 10-32: usage of eID by companies (SME Panel)Low, Medium or High-level Identification is used by over 80% of the large companies of the SME panel as well as the medium sized ones. The small and micro enterprises use IDs respectively in 70% and 60% of the cases.

6.3.2 Social Impacts and administrative burden

The potential social impacts impact of the regulation of cross-border eIDs is huge, since it is a strong enabler of the European Union citizenship. Once the range of cross-border eServices will have been expanded and once they will fully operate, there will be significant social impacts. Actually eID and related cross-border services will be extremely useful to support the emergence of new business and personal lifestyles, and, in turn, the new styles will create the demand for new services.

[60] idem

[61] based on the average number of prescriptions of 0,048 per day (only UK data available, and used as assumption for all EU 27) and the number of bednights in another EU Member State: 500 Million (source Eurostat tour_occ_arnraw)

[62] The State of the Electronic Identity Market: Technologies, Infrastructure, Services and Policies; IPTS 2010, page 4

The figure of 12.5 million EU citizens living in another EU country has already been mentioned and referenced. The absence of a working European interconnected eIDs will lead to the exclusion of part or all of these citizens from accessing the public services they need.

The dimensioning of the social impacts is, as for the economic impact, dependent on demand, with the associated difficulties.

The indicators of the economic impacts are

- Number of potential requests by migrating or commuting citizens which cannot be followed up due to the non-usability of online cross-border public services
- Number of hours spent to deal with administrations in person
- Number of trips (and Kgs of CO_2 produced) to deal with administrations on cross-border relationships
- Number of excluded citizens, due to the lack of access to electronic cross-border public services for the non-availability of interoperable eID systems
- Additional expenses to travel to interact with administrations because of the unavailability of cross-border services or because of the unavailability of interoperable eIDs and eAuthentication
- Number of working hours spent by businesses dealing with administrations in cross-border relations
- Number of leisure hours lost by citizens to deal with cross-border service issues, unavailable because of the non-existence of interoperable cross-border eID.

There is also the need to protect personal data and ensure the security of transactions. It is necessary to cater for appropriate regulations and references to existing rules.

As shown by Figure 10-33: Purpose of eID use by companies (SME Panel), enterprises use eID for internal procedures (30%) in case of large enterprises, in 35% of the cases to complete procedures of public authorities, in 15% of the cases to manage customer relations and in about 18% of the cases to interact with other companies.

Figure 10-35: Potential reasons for companies to use eID (SME Panel) shows that the main reasons for enterprises to use eIDs is its cross-sector usability. Many other enterprises use it because it is mandatory.

Figure 10-36: Use of Government Services shows that citiznes in Austria, Denmark, Germany, the Netherlands, Portugal and Slovenia are particularly using eGovernment, while a total of 70% for the Bulgariam Cypriot, Danish, Estonian, Finnish, German, Greek, Irish, Luxemburgish, Maltese and Dutch, Slovenian, Spanish and British citizens are either intense eGovernment users or are strongly interested in becoming users.

6.3.3 Impact on cross-border public services

6.3.3.1 Introduction

The present section makes an in-depth analysis of services for citizens and businesses identified in paragraph 6.1.1.2.

For each of the service the main benefits and impacts have been identified, as well as the approach to measurement, the sizing and the weighting.

It is important to emphasise that the present impact assessment concerns the potential cross-border services which can be used by citizens permanently or temporarily abroad.

The benefits are considered

a) For private citizens
b) For businesses
c) For administrations

6.3.4 Citizen services

6.3.4.1 Register a change of Domicile

On 1 January 2010 1,057,666 non-Belgian citizens were registered in the country's National Register. There were 2,520,045 new residence permits issued in EU-27 Member States in 2008 for non-EU members (EC, DG Employment, Social Affairs and Inclusion, 2011). It is reasonable to assume that all 1.205 million immigrants from EU27 Member States shown in Table 4 will require to register as domicile.

Description	An online service allowing citizens a change of domicile when abroad
ID	An identification is mandatory, since in most countries the requester takes personal responsibility in the change of domicile declaration, which has a legal value (for correspondence, for example)
Implications	The domicile has a legal value for fiscal and taxation reasons, for registering a car, for economic and financial relationships with banks
Cross-border value of public service	Low. The change of domicile has a typically local character and it is unlikely that the change will occur without a physical presence in the place of domicile. Typical local online public service
Potential market volume	Low. An exception might concern the registration of expatriates. Citizens will unlikely change domicile at a high frequency (more than once a year)
Main benefits and impacts for private citizens	- Cost savings due to the reduced need for mobility - Time savings due to the possibility to access the service remotely, avoiding travel and queues
Main benefits and impacts for businesses	- Cost savings due to reduced employee leave (not applicable to free professionals
Main benefits and impacts for administrations	- Increased efficiency of administrative workflow - Increased effectiveness of citizens services
Measurement and sizing indicators	Demand calculation - Statistics on changes of domicile on a yearly basis - Statistics on migrants Frequency - On average, less than once a year

6.3.4.2 Request of ID documents, passport and residence card

More than half of the respondents had experienced some form of administrative difficulty after arriving in their new Member State. The main issues that people encountered were the length of administrative procedures and a lack of clarity about what is required from citizens moving to another EU Member State. Problems are arising in the early state of move to another EU country. it is reasonable to assume that all 1.205 million immigrants from EU27 Member States shown in Table 4 will request ID documents.

Description	An online service allowing the request of

	- The ID card - The residence card - The passport
ID	Mandatory, it is necessary to have certainty on the identity of the requester
Implications	The legal value of the issued document
Cross-border value of public service	Medium-high: many foreign residents might need to renew the ID card or the passport
Potential market volume	Medium. In the case of passports it can be estimated that one third of the 12.5 million intra EU emigrants will need a passport every ten years, creating a yearly volume of 400.000 requests
Main benefits and impacts for private citizens	- Cost savings due to the reduced need for mobility - Time savings due to the possibility to access the service remotely, avoiding travel and queues - Fast delivery
Main benefits and impacts for businesses	- Cost savings due to reduced employee leave (not applicable to free professionals
Main benefits and impacts for administrations	- Increased efficiency of administrative workflow - Increased effectiveness of citizens services
Measurement and sizing indicators	Demand calculation - Statistics on passport renewals on a yearly basis - Statistics on migrants Frequency - Once every 5 years, once every 10 years

6.3.4.3 Enrol as a student

Thanks to mobility programs, many students in Europe are spending a year in another country. Statistics from Eurobarometer and Eurostat confirm the high potential for cross-border e-government services for students. Every year 180,000 European students move to another Member State for the Erasmus programme or to attend a post graduate degree. Often, they remain and seek employment.

Description	An online service allowing the access to the enrolment as a student in a university or other education establishment - The ID card - The residence card - The passport
ID	Mandatory, it is necessary to have certainty on the identity of the requester
Implications	The possible legal value of the issued document
Cross-border value of public service	Medium-high: many foreign residents might need to renew the ID card or the passport
Potential market	Medium. In the case of passports it can be estimated that one third of

volume	the 12.5 million intra EU emigrants will need a passport every ten years, creating a yearly volume of 400.000 requests
Main benefits and impacts for private citizens	- Cost savings due to the reduced need for mobility - Time savings due to the possibility to access the service remotely, avoiding travel and queues - Fast delivery
Main benefits and impacts for businesses	- Cost savings due to reduced employee leave (not applicable to free professionals
Main benefits and impacts for administrations	- Increased efficiency of administrative workflow - Increased effectiveness of citizens services
Measurement and sizing indicators	Demand calculation - There are 583.700 European students per year - There are 663.100 extraEuropean students per year Frequency - Once or twice a year

6.3.4.4 Vehicle taxes payment

United Nations data reveals that on average there are 519.8 vehicles per 1,000 of the population (over 15) in EU27 Member States. Assuming that vehicle ownership is the same amongst immigrants as the indigenous population of EU27 States we estimate that immigrants will register 622,000 vehicles per annum.

Description	Online service to pay car taxes from a foreing country. People temporarily living abroad need to pay their car tax without moving mack to the home country -
ID	Optional. Identification can be done through the online payment means
Implications	None
Cross-border value of public service	Medium Low, quite a few expatriates will have to pay their car taxes
Potential market volume	Share of car owners who have not re-registered their car when relocating
Main benefits and impacts for private citizens	- Cost savings due to the absence of mobility - Time savings due to the possibility to access the service remotely, avoiding travel and queues - Fast delivery
Main benefits and impacts for businesses	- None
Main benefits and impacts for administrations	- Increased efficiency of administrative workflow - Increased effectiveness of citizens services

Measurement and sizing indicators	Demand calculation - Number of foreign cars in Europe Frequency - Once a year

6.3.4.5 Applying for or transferring a driver's licence

Applying statistics of application for driver's licence to the EU27 immigrant population suggests that there will be 104,000 cross-border driving license applications a year.

Description	Online service to apply for a driving licence in the home country -
ID	Mandatory
Implications	Legal verification of ownership
Cross-border value of public service	Low, quite a few expatriates will have to apply for or renew their driving licence. A permanent expatriate will apply for a local driving licence using a local application.
Potential market volume	Share of expatriate drivers who apply for a DL or to transfer it. Driving licences can expire or last indefinitely. Number of yearly applications
Main benefits and impacts for private citizens	- Cost savings due to the absence of mobility - Time savings due to the possibility to access the service remotely, avoiding travel and queues - Fast delivery
Main benefits and impacts for businesses	- None
Main benefits and impacts for administrations	- Increased efficiency of administrative workflow - Increased effectiveness of citizens services
Measurement and sizing indicators	Demand calculation - Number of foreign citizens needing a birth certificate or needing to declare the birth of a child Frequency - 10 years, 5 years and yearly expiry

6.3.4.6 Order a birth certificate

It is reasonable to assume that some immigrants will also need to obtain copies of their birth certificates for administrative requirements. We have assumed that the level of these requests will be two per cent of the (five year stock) immigrant population. These requests would generate about 120,500 further orders for birth certificates. Thus in total cross-border birth certificates orders will be 137,000 per annum.

Description	Online service to request a birth certificate or declare a birth -
ID	Optional/Mandatory

Implications	Not in every country it is necessary to identify oneself to get a birth certificate. The online procedure might be different. In case of the declaration of birth of a child the identification is mandatory
Cross-border value of public service	Medium-Low, the request is related to the birth of children of expatriates
Potential market volume	Number of children of expatriates
Main benefits and impacts for private citizens	- Cost savings due to the absence of mobility - Time savings due to the possibility to access the service remotely, avoiding travel and queues - Absence of mistakes
Main benefits and impacts for businesses	- None
Main benefits and impacts for administrations	- Increased efficiency of administrative workflow - Increased effectiveness of citizens services
Measurement and sizing indicators	Demand calculation - Number of foreign citizens needing a birth certificate Frequency - uncertain

6.3.4.7 Register a death

Applying official statistics to the (five year stock) immigrant population reveals that there will be 22,500 deaths that will need to be registered each year.

Description	Online service to declare a death -
ID	Optional/Mandatory
Implications	In some countries the procedure might be automatic and guided by the physician declaring the death
Cross-border value of public service	Medium-Low, the request is related to the need of expatriates to declare a death and to the legal possibility to do this
Potential market volume	Uncertain
Main benefits and impacts for private citizens	- Cost savings due to the absence of mobility - Time savings due to the possibility to access the service remotely, avoiding travel and queues - Absence of mistakes
Main benefits and impacts for businesses	- None
Main benefits and impacts for	- Increased efficiency of administrative workflow - Increased effectiveness of citizens services

administrations	
Measurement and sizing indicators	Demand calculation - Number of foreign citizens needing to register a death Frequency - uncertain

6.3.4.8 Register real estate purchase

An increasing number of Europeans are acquiring real estate outside their home Member State. In 2007, the volume of cross-border sales and purchases of real estate was 10 times greater than the figure in 2002, rising to a value of €55 billion. The application of certain national taxation rules on these transactions may render cross-border acquisition of property, in particular of homes, more difficult than acquisitions confined in all respects to the national territory (European Commission, 2010). This study therefore assumed that house sales (and thus real estate purchase registration) would, on average, be 11 per 1,000 of the population. Assuming this level of real estate purchase is representative of EU27 immigrants we estimate that the (five year stock) immigrant population will purchase approximately 66,000 properties per annum.

Description	Online service to register a real estate purchase in the land register -
ID	Optional/Mandatory
Implications	In some countries the procedure might be guided by the notary
Cross-border value of public service	Low, the frequency is unlikely to be very high
Potential market volume	Uncertain
Main benefits and impacts for private citizens	- Cost savings due to the absence of mobility - Time savings due to the possibility to access the service remotely, avoiding travel and queues - Absence of mistakes
Main benefits and impacts for businesses	- Cost savings due to the absence of mobility - Time savings due to the possibility to access the service remotely, avoiding travel and queues - Absence of mistakes
Main benefits and impacts for administrations	- Increased efficiency of administrative workflow - Increased effectiveness of citizens services
Measurement and sizing indicators	Demand calculation - Number of foreign citizens needing to register the purchase of real estate Frequency - uncertain

6.3.4.9 Register for legal aid

Legal aid is an important cross-border service, since many citizens may need to consult about legal issues in a foreign country. During the early stage of immigration citizens have to deal with many administrative formalities.

Using these parameters the calculations suggest that there are 106 cases per 1,000 of the EU27 immigrant population less than 15 years old on average in Belgium and the UK. 35 cases per 1,000 of the EU27 immigrant population age 15 to 64 and 149 cases per 1,000 of the EU27 immigrant population over 64 years old.

Description	Register on-line for legal aid -
ID	Optional/Mandatory
Implications	In some countries the procedure might be guided by the lawyer
Cross-border value of public service	Low, the frequency is unlikely to be very high
Potential market volume	Uncertain
Main benefits and impacts for private citizens	- Cost savings due to the absence of mobility - Time savings due to the possibility to access the service remotely, avoiding travel and queues - Absence of mistakes
Main benefits and impacts for businesses	- Cost savings due to the absence of mobility - Time savings due to the possibility to access the service remotely, avoiding travel and queues - Absence of mistakes
Main benefits and impacts for administrations	- Increased efficiency of administrative workflow - Increased effectiveness of citizens services
Measurement and sizing indicators	Demand calculation - Number of foreign citizens needing to register for legal aid Frequency - uncertain

6.3.4.10 Electronic prescriptions

Prescriptions can only be issued by doctors. Cross-border prescriptions are therefore possible under two circumstances. Firstly, someone can receive a prescription at 'home' and then travels to another EU27 State before obtaining the prescribed items. Secondly, someone could be ill while abroad and return home to receive the prescription.

Description	Receive an electronic prescription to be used in the foreign country or receive a prescription to be used when returned home -
ID	Mandatory
Implications	Close relationship with the physician issuing the prescription and the connection with the patient.

Cross-border value of public service	Medium Low,
Potential market volume	2,5 to 4,3 million prescriptions a year
Main benefits and impacts for private citizens	- Health benefits - Absence of mistakes and clear information and liability - Time savings due to the possibility to access the service remotely, avoiding travel and queues - Absence of mistakes - Ease if use by the physician
Main benefits and impacts for businesses	- None
Main benefits and impacts for administrations	- Increased efficiency of administrative workflow - Increased effectiveness of citizens services
Measurement and sizing indicators	Demand calculation - Number of foreign citizens needing a prescriptions and frequency

6.3.4.11 Access to patient summary

Slightly more than half of EU citizens are open to travel to another EU country to seek medical treatment (54%) and 70% of the EU27 population believe that costs of healthcare treatment received elsewhere in the EU will be reimbursed for them by their health authority.

visits to doctors. Since this is the event that will trigger a cross-border request for a patient summary by a doctor this is a useful surrogate in calculating cross-border patient summary requests.

Description	A physician visiting a patient from a foreing country will request the patient summary to support the treatment with extended information. -
ID	Mandatory
Implications	Close relationship with the physician issuing the prescription and the connection with the patient, also for privacy reasons.
Cross-border value of public service	Medium Low,
Potential market volume	6.6 million prescriptions a year
Main benefits and impacts for private citizens	- Health benefits - Absence of mistakes and clear information and liability - Time savings due to the possibility to access the service remotely, avoiding travel and queues - Absence of mistakes - Ease if use by the physician

Main benefits and impacts for businesses	- None
Main benefits and impacts for administrations	- Increased efficiency of workflow - Increased effectiveness of citizens health security - Citizen protection
Measurement and sizing indicators	Demand calculation - Number of foreign citizens needing a visit and frequency

6.3.4.12 Work Permit Application

Citizens of Bulgaria and Romania still need a work permit in many member states. Despite the fact that restrictions on both countries will be removed eventually, countries like United Kingdom, The Netherlands, Austria and Germany do not plan to remove it in a close future (EC 2012). Moreover, the economic crisis has caused Spain to start to restrict Romanian citizens movement to country, which can also be expected in the other Member States like Greece, Italy and Portugal in the near future.

Description	An immigrant coming from another EU Member State, for which a working permit is requested to relocate in the EU. -
ID	Mandatory
Implications	Strong legal implications for the legality of immigration and work
Cross-border value of public service	Medium high,
Potential market volume	200.000 – 300.000 a year
Main benefits and impacts for private citizens	- Absence of mistakes and clear information and liability - Time savings due to the possibility to access the service remotely, avoiding travel and queues -
Main benefits and impacts for businesses	- Easier procedures for employing labourers from other EU Member State
Main benefits and impacts for administrations	- Increased efficiency of workflow - Imorived control over illegal immigration - Increased effectiveness of citizens health security - Citizen protection
Measurement and sizing indicators	Demand calculation - Number of foreign citizens applying for a work permit

6.3.4.13 Income tax declaration

An approximate estimate of cross-border tax declarations leads to approximately 235,000 cross-border income declarations per annum.

Description	Online cross-border tax declaration -
ID	Mandatory, in conjunction with an electronic signature
Implications	Strong legal implications for validity of the declaration
Cross-border value of public service	Medium high,
Potential market volume	200.000 – 300.000 a year
Main benefits and impacts for private citizens	- Absence of mistakes and clear information and liability - Time savings due to the possibility to access the service remotely, avoiding travel and queues -
Main benefits and impacts for businesses	- Easier procedures for paying taxes to EU Member State
Main benefits and impacts for administrations	- Increased efficiency of workflow - Improved control over immigrants' tax declaration
Measurement and sizing indicators	Demand calculation - Number of foreign citizens making a cross-border tax declaration

6.3.4.14 Registering for a pension

Eurostat has extensive data about the EU27 population at Member State level for annual age group cohorts (demo_pjan). This data suggests, on average 2.262 million men reach the age of 65 per annum and 3.111 million women reach the age of 60 per annum. Extrapolating these figures for the EU27 immigrant population suggests that 2,000 cross-border pension registrations will be made each year.

Description	Online cross-border pension registering -
ID	Mandatory, in conjunction with an electronic signature
Implications	Strong legal implications for validity of the application and high complexity due to the need to reconcile data and financial flows from other countries
Cross-border value of public service	Low
Potential market volume	2.000 a year

Main benefits and impacts for private citizens	- Absence of mistakes and clear information and liability - Time savings due to the possibility to access the service remotely, avoiding travel and queues - No need for mobility
Main benefits and impacts for businesses	- Easier procedures
Main benefits and impacts for administrations	- Increased efficiency of workflow - Improved control over immigrants' request
Measurement and sizing indicators	Demand calculation - Number of foreign citizens applying for a pension

6.3.5 Business services

6.3.5.1 Register a new legal entity

Businesses that establish a new legal entity in another member state may also need to 'to register for VAT', register a 'corporate/business tax declaration', register as an entrepreneur or apply for 'business licenses or permits'. Several studies have examined these business start-up procedures.

There are extra costs arising from cross-border deliveries for companies. The cost of ensuring an efficient cross-border after-sales service is 55 per cent more than in a company's home country.

Description	Cross-border company registration
ID	Mandatory
Implications	Service with a lot of legal implications
Cross-border value of public service	Medium-high
Potential market volume	15.000-25.000 per annum
Main benefits and impacts for private citizens	- Speed of procedure - Absence of mistakes - No need for mobility
Main benefits and impacts for businesses	- Speed of procedure - Absence of mistakes - No need for mobility
Main benefits and impacts for administrations	- Increased efficiency of workflow - Improved control over immigrants' request
Measurement and sizing indicators	Number of new enterprises cross-border establishment per year

6.3.5.2 Corporate/business tax declaration

It is reasonable to assume that each enterprise in the stock of cross-border businesses will make a business tax declaration once a year. The probable level of cross-border business tax declarations is 140,000 per annum.

Description	Corporate tax declaration
ID	Mandatory
Implications	ID joint with personal responsibility
Cross-border value of public service	Medium
Potential market volume	15.000-25.000 per annum
Main benefits and impacts for private citizens	- Speed of procedure - Absence of mistakes - No need for mobility
Main benefits and impacts for businesses	- Speed of procedure - Absence of mistakes - No need for mobility
Main benefits and impacts for administrations	- Increased efficiency of workflow - Improved control over immigrants' request
Measurement and sizing indicators	Number of cross-border tax declarations

6.3.5.3 Registering for VAT

It is reasonable to assume that each year all the newly created cross-border enterprises will register for VAT. The probable level of VAT registration is 18,000 per annum.

Description	Corporate VAT registration
ID	Mandatory
Implications	ID joint with personal responsibility
Cross-border value of public service	Medium
Potential market volume	15.000-25.000 per annum
Main benefits and impacts for private citizens	- Speed of procedure - Absence of mistakes - No need for mobility
Main benefits and impacts for businesses	- Speed of procedure - Absence of mistakes - No need for mobility
Main benefits and impacts for administrations	- Increased efficiency of workflow - Improved control over immigrants' request

Measurement and sizing indicators	Number of cross-border VAT registration

6.3.5.4 Submitting VAT declarations

It is reasonable to assume that each enterprise in the stock of cross-border businesses will make four VAT declarations a year. The stock of cross-border businesses likely to make a VAT declaration is 140,289. Each of these businesses will make four declarations a year. Thus the total number of declarations in a year will be approximately 561,000.

Description	Corporate VAT declaration
ID	Mandatory
Implications	ID joint with personal responsibility
Cross-border value of public service	Medium-high
Potential market volume	500.000 per annum
Main benefits and impacts for private citizens	- Speed of procedure - Absence of mistakes - No need for mobility
Main benefits and impacts for businesses	- Speed of procedure - Absence of mistakes - No need for mobility
Main benefits and impacts for administrations	- Increased efficiency of workflow - Improved control over immigrants' request
Measurement and sizing indicators	Number of cross-border VAT declarations

6.3.5.5 Registering a new employee

Eurostat data (bd_9b_sz_cl_r2) provides information about the average growth rates for EU27 new enterprises over a two, three, four and five year period. The average rate of growth across all EU27 new enterprises is 60.3 per cent. These growth rates for each Member State were used to calculate the proportion of businesses that would be growing. This calculation, obviously, assumes that the percentage growth in employees is the same as the proportion of businesses growing, it is evident that all the employment growth in a country could come from a single business. However, in the absence of data it does not seem unreasonable to assume a similarity in employment growth and the proportion of growing businesses.

The total number of growing businesses that will therefore need to register a new employee is 84,597.

Description	Registering a new employee
ID	Mandatory
Implications	ID joint with personal responsibility
Cross-border value of public service	Medium low

Potential market volume	15.000-25.000 per annum
Main benefits and impacts for private citizens	- Speed of procedure - Absence of mistakes - No need for mobility
Main benefits and impacts for businesses	- Speed of procedure - Absence of mistakes - No need for mobility
Main benefits and impacts for administrations	- Increased efficiency of workflow - Improved control over immigrants' request
Measurement and sizing indicators	Number of cross-border employee registrations

6.3.5.6 Pay social contributions for employees

Eurostat data (bd_9b_sz_cl_r2) provides information about the number of businesses that have zero employees. Where this data is available for Member States 42 per cent of enterprises had zero employees. Obviously these businesses will not pay social contributions because they have no employees.

It is therefore evident that 58 per cent of enterprises will have one or more employees. This figure was therefore used to estimate the number of new migrant businesses that will need to pay social contributions (21,800). We made the assumption that all cross-border branches would have employees. Thus the total number of cross-border businesses paying social contributions for employees is 124,000. Since these contributions are made every month we estimate that the number of payments made by cross-border businesses is 1,491,000.

Description	Cross border Payment of employee
ID	Optional
Implications	ID joint with personal responsibility
Cross-border value of public service	Medium low
Potential market volume	1.00.0 – 1.500.000 per annum
Main benefits and impacts for private citizens	- Speed of procedure - Absence of mistakes - No need for mobility
Main benefits and impacts for businesses	- Speed of procedure - Absence of mistakes - No need for mobility
Main benefits and impacts for administrations	- Increased efficiency of workflow - Improved control over immigrants' request
Measurement and sizing indicators	Number of cross-border employee registrations

6.3.5.7 Reporting termination of employee(s)

It is well known that even growing businesses have employees that retire or leave to take up other jobs. There is no data on Eurostat concerning this phenomenon. The estimate is therefore that the number of businesses reporting termination of employees will be approximately 55,000.

Description	Terminating a new employee
ID	Mandatory
Implications	ID joint with personal responsibility
Cross-border value of public service	Medium low
Potential market volume	55.000 per annum
Main benefits and impacts for private citizens	- Speed of procedure - Absence of mistakes - No need for mobility
Main benefits and impacts for businesses	- Speed of procedure - Absence of mistakes - No need for mobility
Main benefits and impacts for administrations	- Increased efficiency of workflow - Improved control over immigrants' request
Measurement and sizing indicators	Number of cross-border employee termination

6.3.5.8 Register a new vehicle

A European Commission (2012) report suggests that each year, EU citizens and companies have to move 3.5 million vehicles to another Member State. Eurostat data (bd_9b_sz_cl_r2) provides information about the proportion of businesses with more than ten employees (6.3 per cent for EU27). Using this percentage and the above assumptions the estimate that 3,400 cross-border businesses will register a new vehicle each year.

Description	Cross-border vehicle registration
ID	Mandatory
Implications	ID necessary for register
Cross-border value of public service	Low
Potential market volume	3.400 per annum
Main benefits and impacts for private citizens	- Speed of procedure - Absence of mistakes - No need for mobility

Main benefits and impacts for businesses	- Speed of procedure - Absence of mistakes - No need for mobility
Main benefits and impacts for administrations	- Increased efficiency of workflow - Improved control over immigrants' request
Measurement and sizing indicators	Number of cross-border vehicle registration

6.3.5.9 Registering real estate purchase

Nonetheless, the total number of registrations is so small, in comparison with other services that even if these calculations were in accurate by a factor of ten they would still be amongst the least used of business cross-border services.

Adopting the above assumptions we estimate that 1,000 cross-border businesses will register a real estate purchase each year.

Description	Cross-border vehicle registration
ID	Mandatory
Implications	ID necessary for register
Cross-border value of public service	Low
Potential market volume	1.000 per annum
Main benefits and impacts for private citizens	- Speed of procedure - Absence of mistakes - No need for mobility
Main benefits and impacts for businesses	- Speed of procedure - Absence of mistakes - No need for mobility
Main benefits and impacts for administrations	- Increased efficiency of workflow - Improved control over immigrants' request
Measurement and sizing indicators	Number of cross-border real estate registration

6.3.5.10 Consult the business register

Assuming that each Member State business register has the number of enterprises recorded by Eurostat for the Member State we calculate that 4.641 million cross-border enquiries would be made each year.

Description	Inquiries in the Business Register

ID	Mandatory
Implications	
Cross-border value of public service	Mediumm-high
Potential market volume	4.5 million
Main benefits and impacts for private citizens	- Speed of procedure - Absence of mistakes - No need for mobility
Main benefits and impacts for businesses	- Speed of procedure - Absence of mistakes - No need for mobility
Main benefits and impacts for administrations	- Increased efficiency of workflow - Improved control over immigrants' request
Measurement and sizing indicators	Number of cross-border business register consultations

6.3.5.11 Submit a tender for public procurement

This study made the assumption that each contract notice has one EU27 cross-border applicant. Thus we estimate that there are 177,000 cross-border submissions of a tender for public procurement a year.

Description	Online tendering
ID	Mandatory
Implications	Legally binding commitment
Cross-border value of public service	Medium
Potential market volume	200.000 per annum
Main benefits and impacts for private citizens	- Speed of procedure - Absence of mistakes - No need for mobility
Main benefits and impacts for businesses	- Speed of procedure - Absence of mistakes - No need for mobility
Main benefits and impacts for administrations	- Increased efficiency of workflow - Improved control over immigrants' request
Measurement and sizing indicators	Number of cross-border tender submissions

7 SECTION 6: COMPARING THE SHORTLISTED OPTIONS A AND B

Based on the evidence and the assessments made above the policy options A and B have been on the basis of different policy assumptions:

- Create a regulatory framework enabling the interoperability of the different technical eID-solutions used by Member States to allow their secure and trusted use in cross-border eServices
- Create a framework of reference to determine the reliability of the issuer of the eID and the legal certainty on the cross-border use of eIDs
- A clear liability for the security, correctness and unique correspondence to the physical person of the eID
- Measures against discrimination of non-nationals when they access online services, including citizens not provided with an eID in their country

The comparison of the different impact is made on the basis of the magnitude of the impact and its likelihood. The magnitude is scored as follows:

---- Very negative impact (-3)

-- negative impact (-2)

- slightly negative impact (-1)

0 no or minimal impact

+ slightly positive impact (1)

++ positive impact (2)

+++ very positive impact (3)

Next to the magnitude there was the assessment of the likelihood that the impact is made (high=3, medium = 2 and low =1).

The score on each element is the product of the magnitude and the likelihood. The system thus gives a weighing to the different elements and a conclusive result.

The comparison shows clear preferences for policy option B, due to the very negative impacts of option A and the expected positive impacts of option B.

The strongest and most positive are impacts seen for the economic impacts for the objective to create a legal and regulatory framework enabling the interoperability of the different technical solutions used by Member States to allow their secure and trusted use in cross-border eServices. Overall the impacts in economic sense are stronger than the social and environmental impacts.

The strongest negative impact is related to the fragmentation of the market.

Impacts	**Option A** Keep the status quo			**Option B** Support the formulation and implementation of legislation		
Create a legal and regulatory framework enabling the interoperability of the different technical solutions used by Member States to allow their secure and trusted use in cross-border eServices						
	Magnitude	**Likelihood**		**Magnitude**	**Likelihood**	
Economic Impacts						
Risk of negative or low return on investment previously made in eID services	-	medium	-2	+	medium	2
Multiplied impact of ICT investment on productivity and competitiveness	---	medium	-6	++	medium	4

Reduction of administrative burden for service providers and users	--	medium	-4	++	medium	4
Increase economies of scale	--	medium	-4	+	medium	2
Social impacts						
Reduce barriers to mobility	-	medium	-2	+	high	3
Social exclusion	0	low	0	+	medium	0
Digital exclusion	-	low	-1	+	low	1
Environmental Impacts						
Reduced amount of paper used	0	low	0	+	low	0
Reduced amount of travel	--	high	-6	++	medium	4
Total score of Objective	-25			20		
Create a framework of reference to determine the reliability of the issuer of the eID, the legal certainty on the cross-border use of eIDs						
	Magnitude	**Likelihood**		**Magnitude**	**Likelihood**	
Economic Impacts						
Increase legal certainty, trust and security of cross-border eGovernment and administration services	--	medium	-4	+	medium	2
Reduce the fragmentation of the market	---	high	-9	++	medium	4
Socio-economic impacts						
Increase legal certainty of online IDs	--	Medium	-4	++	medium	4
Reduce identity theft	0	low	0	++	low	
Total score of Objective	-17			10		
A clear liability for the security, correctness and unique correspondence to the physical person of the eID once it is used in online transactions						
	Magnitude	**Likelihood**		**Magnitude**	**Likelihood**	
Economic Impacts						
Increase legal certainty	-	medium	-2	+	medium	2
Increased asset protection (institutional and monetary values)	-	medium	-2	+	low	1
Increased development of cross-border online services	0	low	0	0	low	0
Increased (cross-border) service interconnection	0	low	0	0	low	0
Total score of Objective	-4			3		
Measures against discrimination of non-nationals when they access online services, but also once some MSs do not issue eIDs to their citizens						
	Magnitude	**Likelihood**		**Magnitude**	**Likelihood**	
Economic Impacts						
Increased population using cross-border services	-	medium	-2	+	medium	2
Facilitated access to online services	-	medium	-2	+	medium	2
Social impacts						
Contrast of social exclusion	--	low	-2	0	low	0
Contrast of digital exclusion	-	low	-1	0	low	0

Total score of Objective	-5	4

8 SECTION 7: MONITORING AND EVALUATION

8.1 Introduction

Due to the rapid but somewhat unpredictable development of European cross-border online services, in particular of eID-enabled services as well as cross-border eID and eAuthentication services s, it is necessary to monitor and evaluate the whole scenario and the development of the single services, to:

- understand demand
- assess the benefits to users of alternative proposals, and
- evaluate the effectiveness of implementations in meeting their objectives.

Furthermore, monitoring and evaluation helps to discuss the case for new projects and expenditure, to justify the continued support to initiatives, to allocate additional funds to IT investment.
Two key policy-related features of Monitoring and Evaluation are

a) the assessment of progress towards the achievement of programme goals and to determine impacts;
b) the programme consolidation, feedback on European policy making, working out best practices, and selecting standards.

Monitoring and evaluation will build on a set of indicators measuring the development, effectiveness and take up of the progress towards cross-border European eGovernment services enabled by eID.

8.2 The feedback on policy making

One of the main uses of Monitoring and evaluation is on policy development, on the policy making process and on the relevant effects on the overall strategic-institutional dimension of the European development and of the digital single market.

The impact on policies shall be measured relating the dimensions of

- Input, i.e. the resources, incentives, funds made available for the policy process. These are the key elements for the determination of the comparison of costs and benefits;
- Output, i.e.: the internal and external results generated by the policy process and its internal implementation;
- Outcomes, i.e.: the effects generated by the policy intervention in terms of benefits, barriers created or lifted, service uptake and user satisfaction;
- Impacts at different levels, e.g.: on the situation of users, on the suppliers cooperating in the implementation of public or eGovernment cross-border services, on the economy and more in general on society.

The comparison of these dimensions and the feedback from the results of the monitoring and the different impacts on the overall policy process allows the assessment of policy making and its adjustment.

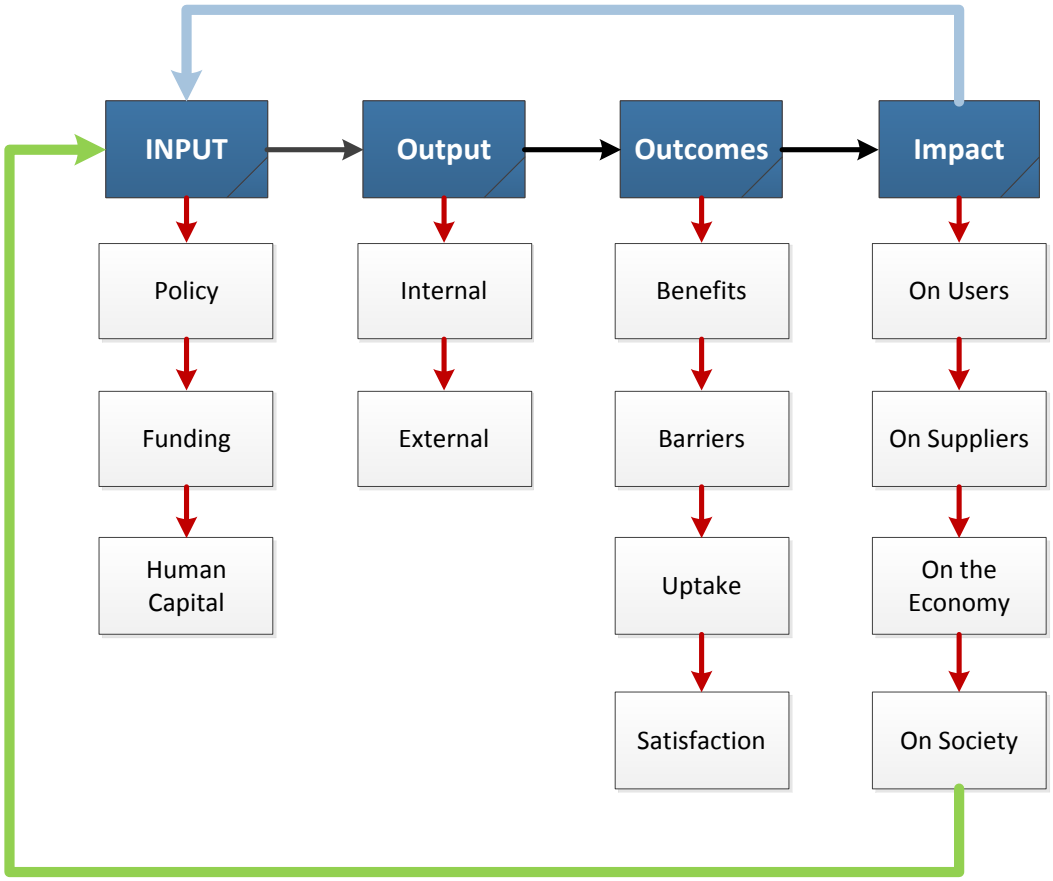


Figure 8-1: Monitoring and Evaluation Process

8.3 Monitoring and Evaluation

Monitoring and evaluation allows to collect evidence on the development of the eID and eAuthentication framework and to determine a number of effects and impacts on different domains of the services.
The observation concerns all the different aspects related to the EU cross-border services policy making, addressing different levels. Each monitoring observation uses different indicators, which will provide input to

1) Strategic and institutional objectives and policies of the EU
2) The way policies are designed and implemented
3) The benefits to citizens and businesses
4) More general societal, social and economic benefits.

The monitoring can be performed at different levels, involving the European Commission at the central EU level, the Member Stats and maybe the local authorities – in some specific application cases – in the collection and communication of relevant data. The Administration and the eGovernment developers and providers would contribute to the delivery of data and information.

8.3.1 The structuring of indicators

The following table provides a structure of the indicators to be monitored for the evaluation of the eID domain and the eID enabled services.

Monitoring area	Indicator
Development of the European Single Market and of the Digital Single Market	• eID and eAuthentication suppliers, Existence of eIAS suppliers that have activities in multiple EU member states • Number of formal eIDs notified to the EC
Regulatory integration	• legal interoperability • Data protection • Assess eID systems' security • Degree of harmonisation across members states when regulating eIAS (incl. ancillary trusted services) • Harmonised application and uniform implementation of eID-related legislation at EU level
Infrastructure, infrastructure interoperability, service integration and interoperability, Technological neutrality	• Degree to which devices become interoperational (e.g. eCard readers) between sectors, countries • operational interoperability • technological and security interoperability • Operational and service integration • Technical performance
Dimensional parameters of eID and eID-enabled services	• number of eID and eAuthentication transactions • Usage of eIAS services by eService providers in other sectors than the "traditional closed niche sectors" • Usage of eIAS by all categories of population (cf. via 'Household survey'-type questionnaires) • Extent to which eIAS are used by end-users for national transactions and international (cross-border) transactions • Official eIDs notified to the Commission • Services accessible with notified eIDs provided by central, regional, local authorities • Services accessible with notified eIDs provided by Points of Single Contact • number of interoperable eID services • number of mutually recognised formal eIDs • growth of interoperable eID services • growth of interoperable eID based cross-border services • business and company access to eID services and eID enabled services • Electronic delivery systems accessible with notified eIDs • Services accessible with notified eIDs in the private sector (online banking, eCommerce, eGambling, login to websites, safer internet services e.g. chatrooms for children)
Support competition in the Digital Single Market	• private and public development of cross-border services enabled by formal eIDs in Europe
Raise awareness	• Awareness raising actions • Effectiveness of awareness raising actions
Economic	• Investment and operational costs • Cost savings by individuals

Monitoring area	Indicator
	• Cost savings by businesses • Reductions of transaction costs • Reductions of need for mobility • Return on investment • Efficiency gains • Business user focus • Travel reduction • Reduction of the administrative burden • Personalisation • Simplification • Widening of markets and participation in cross-border competition (eProcurement) • Cost/benefit analysis
Non-economic	• Quality of life and living • Time saving • Travel reduction • Improvement of mobility • Increased efficiency of mobility • Individual user focus • User friendliness and usability • Personalisation • Reduction of the administrative burden
Accessibility	• Access, accessibility • User involvement in design/delivery
Citizen inclusion	• Number of citizens without access to interoperable eID services • Number of citizens suffering from the digital divide • Accessibility of cross-border services
User satisfaction	• Follow-up of reasons why consumers remain reluctant to use eIAS (cf. via 'Household survey'-type questionnaires) • User satisfaction surveys • Business user satisfaction surveys

Figure 8-2: Monitoring and Evaluation Indicators

8.3.2 Players in the monitoring and evaluation activity

The following table shows which player could provide which data on the overall scenario of eID-enabled service implementation and on eAuthentication.

	European Commission	Member States	Administrations	Service and technology providers	Businesses and Citizens
EU policy	☑				
Infrastructure development	☑	☑	☑	☑	
Service implementation		☑	☑	☑	

	European Commission	**Member States**	**Administrations**	**Service and technology providers**	**Businesses and Citizens**
Regulatory integration	☑	☑			
Economic benefits		☑	☑	☑	☑
Non-economic benefits		☑	☑		☑
Operational and service integration		☑	☑	☑	☑
Service structuring and implementation			☑	☑	☑
Reduction of administrative burden			☑	☑	☑
User satisfaction			☑		☑
Content	☑	☑	☑		☑

9 SECTION 8: CONCLUSIONS

The issues around cross border eID are complex and interwoven with public services, political interests, technical complexities and several types of (end) users.
The cross border use of eID affects more than 12,5 million EU citizens living in another EU Member State, 1,2 Million migrants per year (2009) and more than half a million daily cross border commuters. The further integration of the EU and the increased mobility of people and businesses will only increase this relevance over the coming period. To this ad hoc services can be added, which may require cross border use of eID (when on holiday or on a business trip) for instance using healthcare abroad. As such eID and its cross border use lies at the heart of the EU policy, in particular in terms of the single market and in terms of reduction of administrative burden.

The study has deployed several methodologies and approaches to reduce the complexity and to bring it down to the core elements on the basis of which policy decisions may be taken. The study then collected data and evidence (qualitative and quantitative) to analyse and assess the different options.
Since the actual cross border use of eID is still at the beginning, the study team has not had the possibility to base itself on actual cross border eID use, but instead had to primarily base itself on two basic pillars:

- National eID (use)
- Cross border online services

After extensive desk research the assumptions were assessed to find answers to several core elements of cross border eID use and the impact of EU-wide legislation on the Digital Single Market. The assumptions have been supported by data, studies and circumstantial evidence.

Using these data, together with the Commission policy documents, the options were assessed. Of the three proposed policy options (status quo, cease any action or take legislative/regulatory action), the potential impacts was analysed at two stages: the first stage included a policy impact assessment and an effectiveness/efficiency check. The purpose of this step was to eliminate options that would obviously not contribute to the EU policy in the field.

After the first stage assessment option C was eliminated, which would imply ceasing all EU activity and not aiming at regulation. The main reason for discarding this option is that it would destroy investments made (by the Commission and the Member States), would further fragment the field, and would slow down and hamper overall EU policies, in particular the DAE and the single market policies.
The two shortlisted options (baseline scenario and legislative measures) have subsequently been assessed (stage 2) using all available data.

Both maintaining the status quo and stopping all regulatory activities (option A and C) are not effective in overcoming the barriers to cross-border eID interoperability at the EU level. This option, new regulation on mutual recognition of eID, has a direct effect in overcoming certain legal barriers, and opens the way for overcoming technological incompatibilities at the EU level.

The key (economic, social, environmental) impacts were assessed against the different policy objectives. The result is a very clear recommendation towards the option supporting EU-legislation on eID. This recommendation is based both on the strong negative impacts of the status quo option (A), as well as on the anticipated positive effects of the regulation option (B).

The strongest and most positive impacts are related to economic impacts for the objective to create a legal and regulatory framework enabling the interoperability of the different technical eID-solutions used by Member States to allow their secure and trusted use in cross-border eServices. Overall the impacts in economic sense are stronger than the social and environmental impacts.

The strongest negative impact has to do with the fragmentation of the market.

The study has amongst others (in line with the opinion of the experts working in the field) revealed the need for better data and statistics. The initial monitoring approach was designed, which could be further elaborated or integrated in on going data collection activities. In addition the real effects of reduction of administrative burden at the administration and the 'user' side would deserve further measurements and analysis.

10 ANNEXES CONTAINING FACTUAL OR TECHNICAL MATERIAL

10.1 Untapped Demand

An important set of assumptions underlying the study are that there is an untapped demand for cross-border services, that missing interoperable eID is a barrier to cross-border services (and hence a cause for untapped demand), and additionally, that these two issues may be related in a "chicken and egg" fashion: which is causing which? To examine these assumptions, first the uptake of (cross-border) eID was considered, to find out if there is an untapped demand for cross-border services, and what role cross-border eID, or the lack thereof plays in this.

10.2 eID uptake

The uptake of eID within national borders appear to be relatively high. Since electronic identification is a key enabler for several other services such as electronic signatures, an indication can be obtained on the uptake of eID by looking at the uptake of eSignatures. 82% of respondents (from a total of 205 responses by organizations) in the Public Consultation[63] indicated that their organization uses eSignatures, eID and eAuthentication. The great majority of these (65%) uses these technologies on a daily basis. Nevertheless, respondents estimated that the uptake of electronic signatures was still low to moderate (78% of respondents estimated marginal or moderate).

Even if eSignatures and eIdentification and eAuthentication are comceptually and structurally different, eIdentification is strictly related to electronic signatures. The combination of eSignatures with eID in many cases will provide even stronger electronic signature, or make it easier to get one.

Compared to this, however, the uptake of cross-border eID appears to be limited. 11% (140 of 1251) of the respondents to the SME Panel[64] indicated that they used eID with partners or clients in more than one EU Member State, even though 61% of respondents answered positively to the question "Does your company use electronic signature or other services?"

"eID infrastructure technologies, embedded in operational applications and online services, will be critical to the development of broader eID applications, which are likely to emerge as a 'critical mass' of infrastructure becomes available. Increased portability of credentials and use of federated identification schemes would result in higher take-up and more extensive use of eID solutions, thus contributing to market growth."[65]. the JRC/IPTS has therefore provided indisputable arguments that

a) eIDs and eAuthentication are not a goal by themselves, but they represent a key enabling factor for online services and application;
b) these services and applications are currently hampered by the absence of eID interoperability and mutual recognition;
c) implementing (cross-border) eID infrastructure technologies will be a pre-requisite for the development of eID enabled public and private services.

10.2.1 The Study by Deutsche Bank Research: "eIDs in Europe" (2010)[66]:

[63] We refer to the Public Consultation on Electronic identification, authentication and signatures in the European digital single market, described in the methodology chapter

[64] We refer to the SME Panel on eSignature and eID described in the methodology chapter

[65] The state of the Electronic Identity market: technologies, infrastructure, services and policies, 2010, JRC/IPTS

[66] http://www.dbresearch.com/PROD/DBR_INTERNET_EN-PROD/PROD0000000000262236.pdf

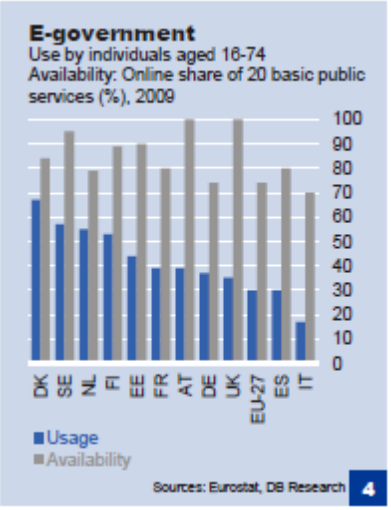


Figure 10-1: eGovernment. Online share of 20 public services

Twelve out of 30 countries in the EEA have already introduced an eID and nine more are planning its introduction. The QES has been introduced by 13 of the 30 countries to date. High eID penetration rates are to be found in Estonia, Spain, Belgium and Sweden. In Italy and Finland the share of eID holders among those people who carry ID is less than 10% (see chart 2).5 There are several reasons for this: firstly, the eID is not compulsory in most countries (e.g. AT, BE, FI, LU, SE and IT) and will therefore only slowly replace old ID documents, or in some countries there is no statutory obligation to carry an ID card. Secondly, the level of internet usage, which is a basic determinant of whether eID use makes sense, differs from country to country (for example, it is lower in Italy and Spain than elsewhere, see chart 3). A third reason could be that e-government or e-commerce services that require eID use are still under-developed and that therefore there is currently little incentive for people to use it.

Every version of the eID that has hitherto been introduced in any of the member states contains an electronic storage and processing medium that allows personal data to be stored so that the user can identify himself. The QES is in most cases an optional extra that can be installed on the eID card and is used to electronically submit a legally binding declaration of intent. On the basis of the signature laws in the respective member states the QES fulfils the requirement of a hand-written signature.

For eGovernment, the following two indicators are the basis for benchmarking: Percentage of basic public services available online, and use of online public services by the public.

To make these indicators operational, Member States have agreed to a common list of 20 basic public services[67], 12 for citizens and 8 for businesses. Progress in bringing these services online will be measured using a four stage framework: 1 posting of information online; 2 one-way interaction; 3 two-way interaction; and, 4 full online transactions including delivery and payment. Data will be collected in surveys twice a year.

The analysis of DB research on Eurostat Data shows that a high percentage of the 20 basic public services have a very high availability in most European Member States. In Sweden, Austria and UK it is higher than 90% and reaching 90%. The usage is less high. The European average is 30%.

The highest eGovernment use is in Denmark, Sweden, the Netherlands and Finland. The lowest is in Italy.

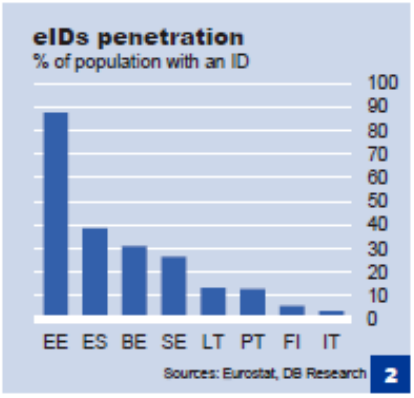


Figure 10-2: eIDs penetration % of population

It is significant that the eID penetration is maximum in Estonia, followed by Spain. In all other countries the share of citizens with an eID card is pretty low. This might represent a hampering factor for the development of cross-border public services. also the usage statistics in several countries are not very high.

[67] http://ec.europa.eu/information_society/eeurope/2002/action_plan/pdf/basicpublicservices.pdf

It should also be emphasised that based on the i2010 eGovernment Action Plan Progress Study[68], two thirds of Member States do not know what the take-up of their eID is, so it is hard to tell if and to what extent investment in eID systems have already paid off.

10.3 Demand for cross-border services[69]

One assumption behind the assumption that improving interoperability of national eIDs is necessary is that there is an untapped demand for cross-border online services. The assumption is examined verifying whether there is a difference in demand for services within borders, and cross-border. Among the manifold reasons why public services are not offered cross border is the lack of interoperable eIDs.

10.3.1 eGovernment

Respondents to the European Business Test Panel on "Business obstacles in the Internal Market" (359 respondents, 81% SME) indicated a number of different obstacles to doing cross-border business, including: taking action against piracy and counterfeiting of their products, applying for a patent in another EU country, using an eSignature in cross-border transactions, obtaining recognition of professional qualifications of staff from another EU country, reclaiming VAT from another country, obtaining licenses, participating in a public tender from another EU country, and getting information on business transfer possibilities.[70] eID may act in some situations as an enabler to reduce existing barriers.

The majority of "20 basic public services" (for which eID is horizontal enabler) is available online in the EU. 75% of EU countries have eID as enabler in place. Cross-border, these digitized public services will only be available when cross-border interoperable eID is available. In many countries, business services are equally supported by eID. VAT, Company registration and Corporate tax can be accessed with an eID in more than half of the benchmarked countries. (Cap Gemini 2010 - Digitizing Public Services in Europe - 9th Benchmark Measurement).

10.3.1.1 eGovernment availability and sophistication

eGovernment online availability, 2010, by country

The following table shows the maturity of eGovernment at Member State level in Europe. In most Member States the availability is above 85% and reaches 100% in Ireland, Italy, Malta, Austria, Portugal, Sweden.

Only Greece, Cyprus, Romania, Slovakia and Iceland are lagging behind.

[68] http://ec.europa.eu/information_society/activities/egovernment/studies/completed_studies/index_en.htm

[69] This section will use more evidence on different types of services, which we are investigating in various sources.

[70] "Business obstacles in the Internal Market", 2011, European Business Test Panel

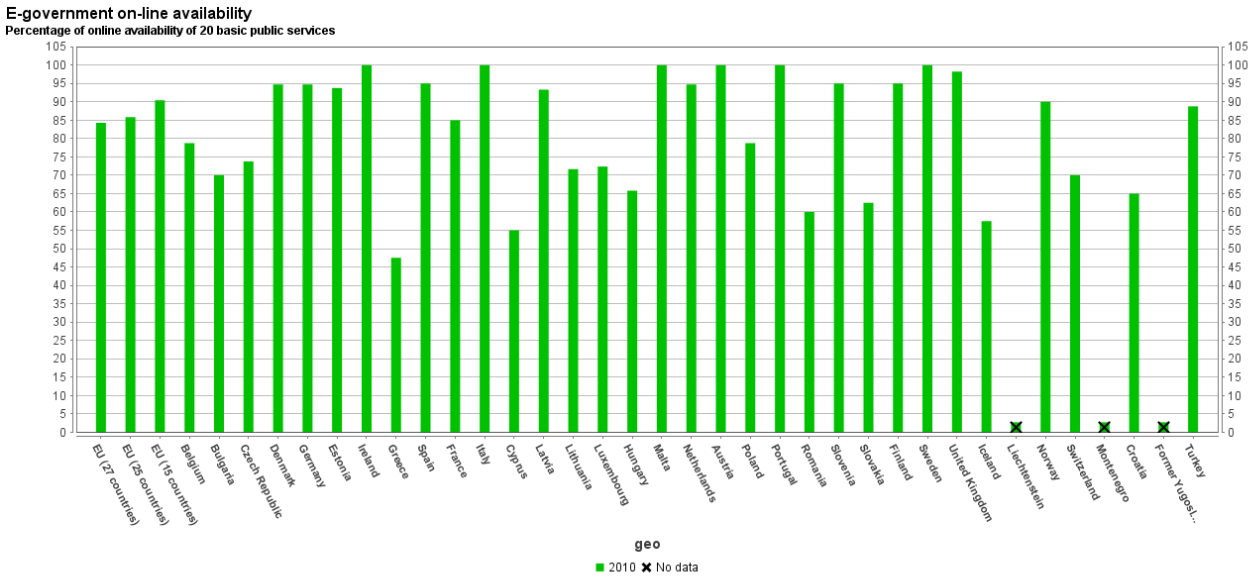


Figure 10-3: eGovernment online availability, 2010, by country

Source: Eurostat[71],

eGovernment online availability, all EU27+, by year (2001-2010)[72]

the following chart shows the trends of online availability in the EU from 2002 to 2010. Business services have an availability of about 30% in 2002 and have reached nearly 90% in 2010. Citizen services started at 18% in 2002 and nearly 80% in 2010.

[71] http://epp.eurostat.ec.europa.eu/tgm/table.do?tab=table&init=1&language=en&pcode=tsiir120&plugin=1

[72] Digitizing Public Services in Europe: Putting ambition into action 9th Benchmark Measurement | December 2010. Capgemini, IDC, Rand Europe, Sogeti and DTi

Figure 3.1: Full online availability trend 2001-2010 timeline for EU27+

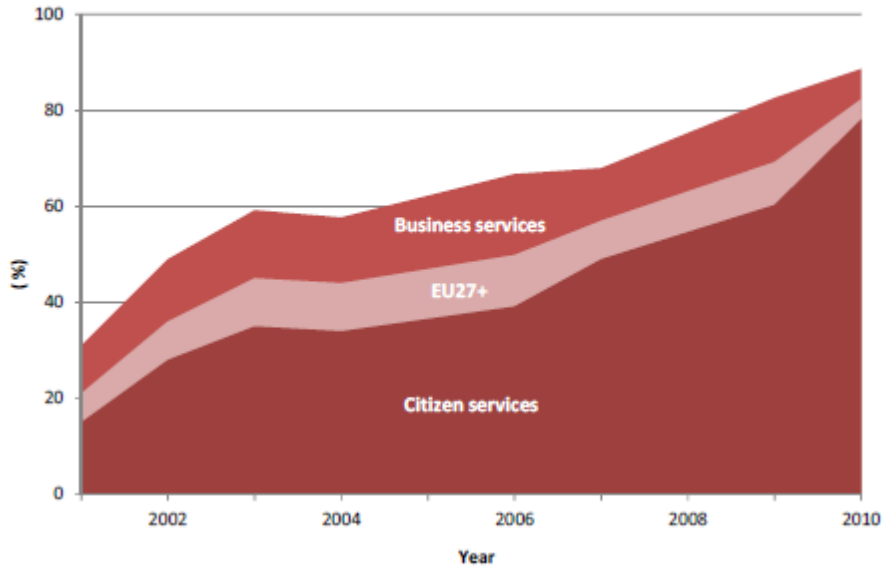
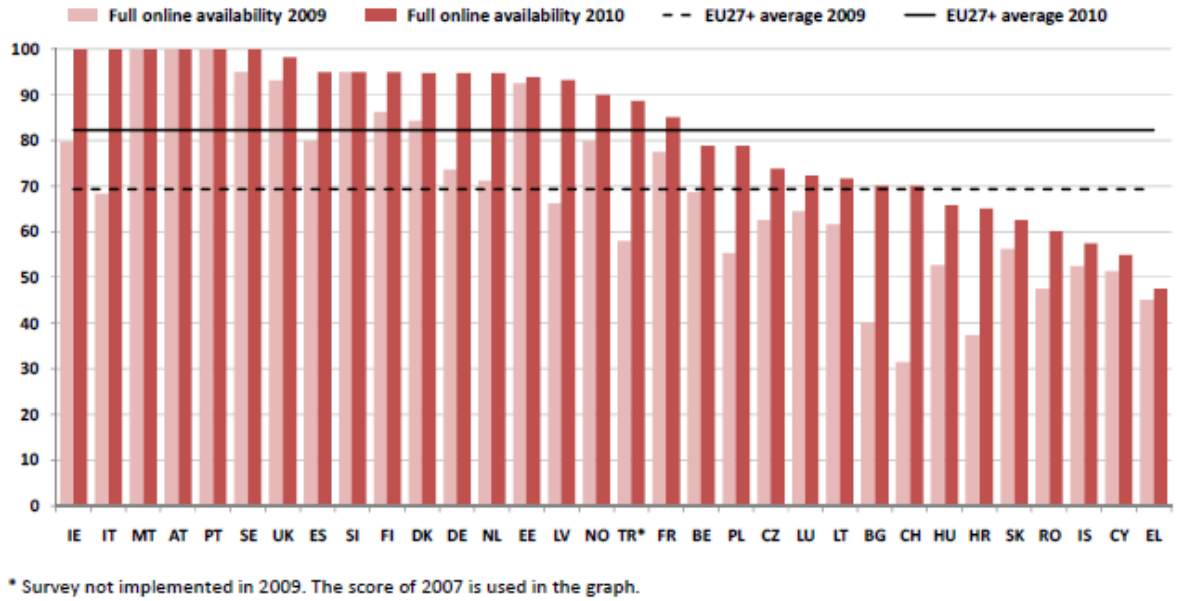


Figure 10-4: Full online avaialbility trend 2001-2010

The following chart makes a comparison across services between Member States. The benchmark shows that in Ireland, Italy, Malta, Austria, Portugal and Sweden all 20 services are now 100% e-enabled. Switzerland, Italy, Bulgaria, Croatia and Latvia have shown marked improvement (more than 25 percent) over the past year.

Figure 3.4: Full Online Availability, 2009-2010 (in %)



* Survey not implemented in 2009. The score of 2007 is used in the graph.

Figure 10-5: Full Online Availability, By Member State

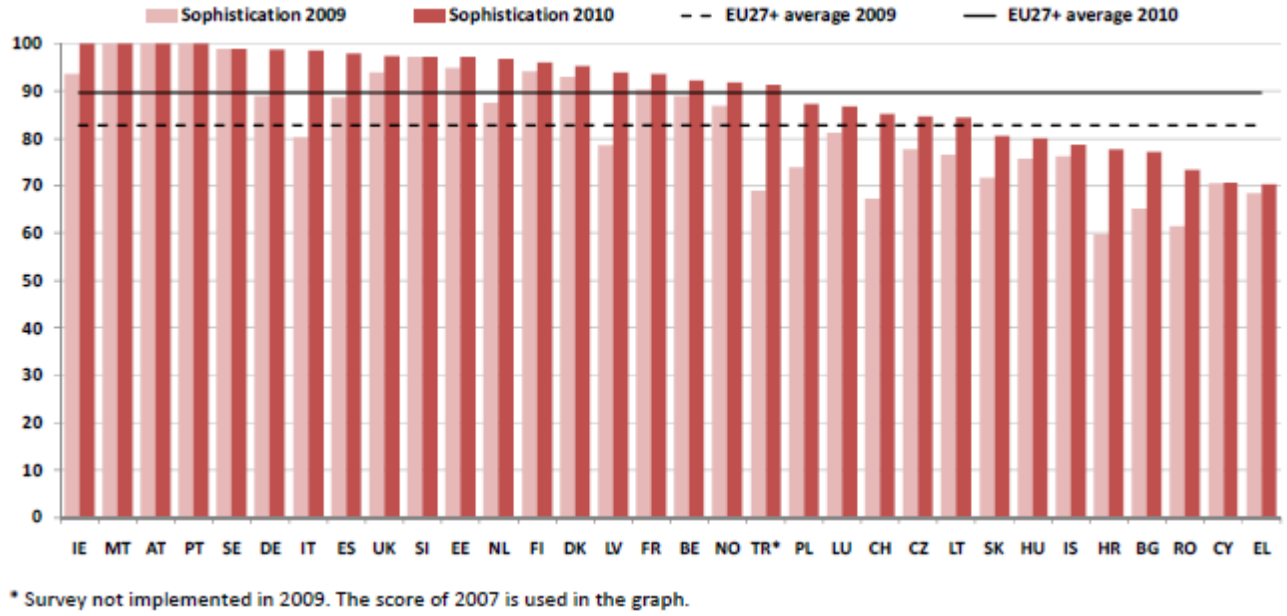
eGovernment sophistication, 2009-2010, by country[73]

The Online Sophistication assesses service delivery against a 5-stage maturity model: (i) information, (ii) one-way interaction, (iii) two-way interaction, (iv) transaction, and (v) targetisation/automation. The EU27+ score for this indicator now stands at 90% (an increase of 7% since 2009). In this comparison, the top performers are Ireland, Malta, Austria and Portugal (all at 100%), followed closely by Sweden, Germany and Italy (all at 99%)

Europe's eGovernment performance has greatly converged in geographic terms since the expansion of the EU in 2004 – both "old" and "new" Member States populate the leading eGovernment nations. When differentiating the results of full online availability between the EU15 and the "new" EU Member States, the

gap has narrowed further and this distinction hardly seems relevant anymore.

Figure 3.6: Services sophistication, 2009-2010 (in %)



* Survey not implemented in 2009. The score of 2007 is used in the graph.

Figure 10-6: Service Sophistication

The EU27+ score for the sophistication of services now stands at 90% (an increase of 7% since 2009) with there being little room for further overall growth. The difference between the overall sophistication of business and citizen services also seems to have become negligible.

[73] *Ditto*: Digitizing Public Services in Europe

eGovernment sophistication, all EU27+, by year (2007-2010)[74]

Figure 3.7: Sophistication, trend 2007-2010 for EU27+

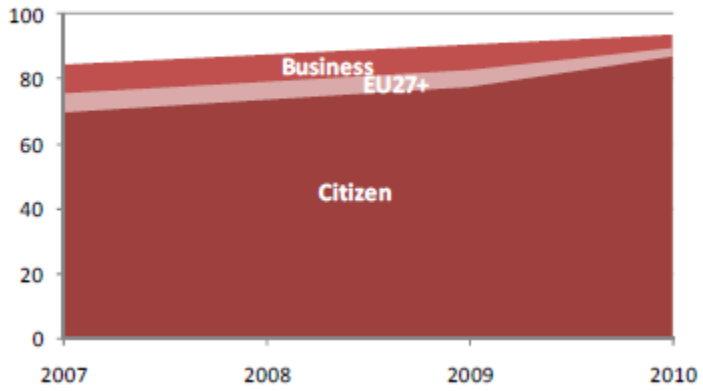


Figure 10-7: eGovernment Sophistication, trend 2007-2010

Looking more in-depth at the pro-active 5th level of sophistication, the differences between 2010 and 2007 are quite significant. Also, whereas in 2009 even, the ranking of the 5th level showed something of a "sliding scale", going all the way from 100% to 10%, this year the results are overall more homogeneous across countries.

Figure 3.8: Pro-active 5th sophistication level,2007 versus 2010

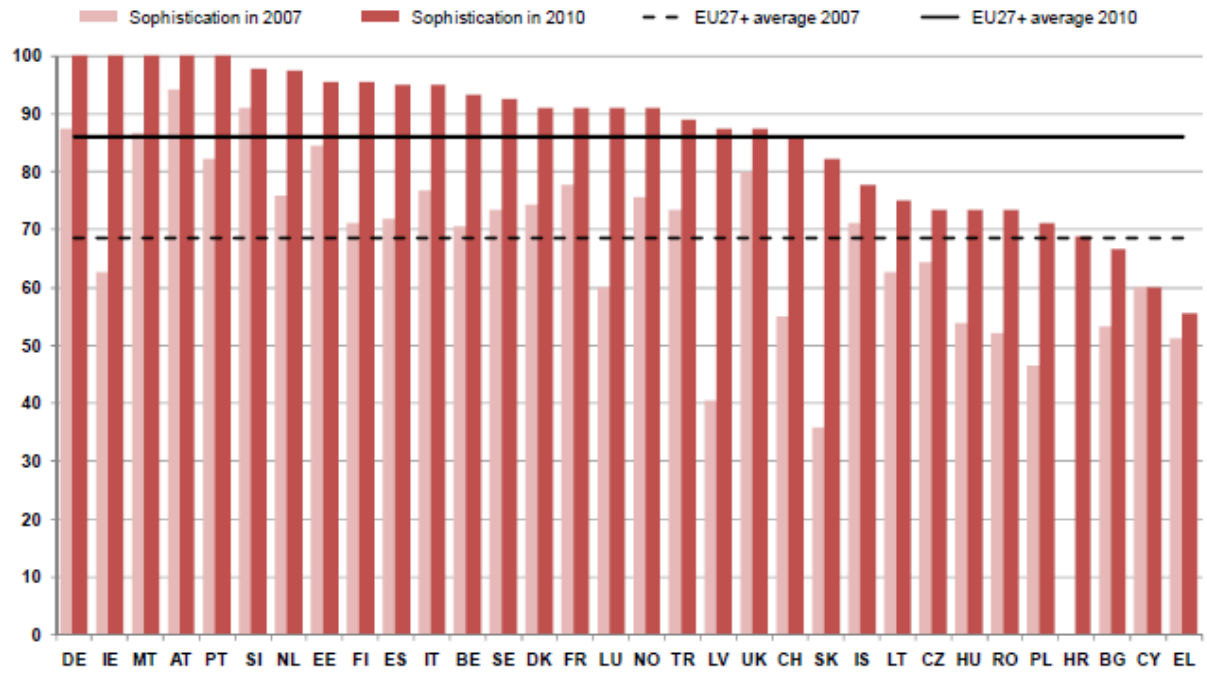


Figure 10-8: Pro-active eGovernment sophistication

[74] *Ditto*: Digitizing Public Services in Europe

eGovernment sophistication, all EU27+, 2009-2010, citizen vs. business services[75]

Figure 3.9: Sophistication in the EU27+ : citizen versus business services, 2009 and 2010 (in %)

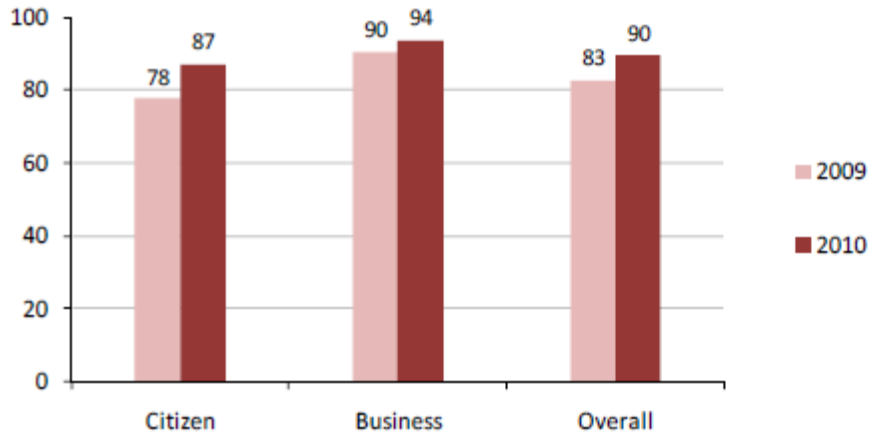


Figure 10-9: Sophistication of eGovernment. Citizen vs. business services

[75] Ditto: Digitizing Public Services in Europe

eGovernment aggregate country performance, 2010

Aggregate Country Performance									
	20 services		User experience		eProcurement		Life events		Key enablers
	Full online availability 2010	Sophistication 2010	User experience (average on all services)	User experience (national portal)	eProcurement pre-award 2010	eProcurement visibility in 2010	Business Life Event (automated + service available thr. portal)	Citizen Life Event (automated + service available thr. portal)	Availability (# enablers)
AT	100	100	50	90	84	72	100	65	9
BE	79	92	65	93	78	38	67	62	7
BG	70	77	74	79	52	89	0	47	2
CH	70	85	68	88	44	64	55	29	8
CY	55	71	53	80	100	94	20	36	5
CZ	74	85	43	76	84	96	57	35	4
DE	95	99	83	68	67	79	92	42	9
DK	95	95	92	90	90	81	100	45	9
EE	94	97	94	80	52	100	100	40	9
EL	48	70	91	91	.	36	14	56	4
ES	95	98	91	95	83	85	80	74	7
FI	95	96	86	88	48	38	11	96	6
FR	85	94	89	100	90	75	67	44	9
HR	65	78	90	73	36	40	64	23	4
HU	66	80	70	90	28	46	55	22	9
IE	100	100	87	50	100	100	100	75	5
IS	58	79	72	77	44	37	20	38	6
IT	100	99	79	23	87	72	83	42	7
LT	72	84	76	65	88	100	56	29	5
LU	72	87	66	69	36	71	53	11	6
LV	93	94	72	85	38	30	88	33	8
MT	100	100	100	100	76	100	30	70	7
NL	95	97	91	96	80	62	14	63	8
NO	90	92	67	86	92	84	100	52	6
PL	79	87	91	85	68	75	20	8	3
PT	100	100	91	94	84	82	78	70	7
RO	60	73	62	32	92	75	0	30	5
SE	100	99	99	68	94	90	100	46	7
SI	95	97	85	80	56	100	92	46	6
SK	63	81	85	93	76	47	29	23	7
TR	89	91	80	90	32	24	46	52	6
UK	98	97	99	83	96	87	100	58	4

Figure 10-10: Aggregate eGovernment Country Performance Source: eGovernment Benchmark 2010

10.3.1.2 eGovernment take-up

Individuals: Percentage of interaction with public authorities (in general), 2010, by country

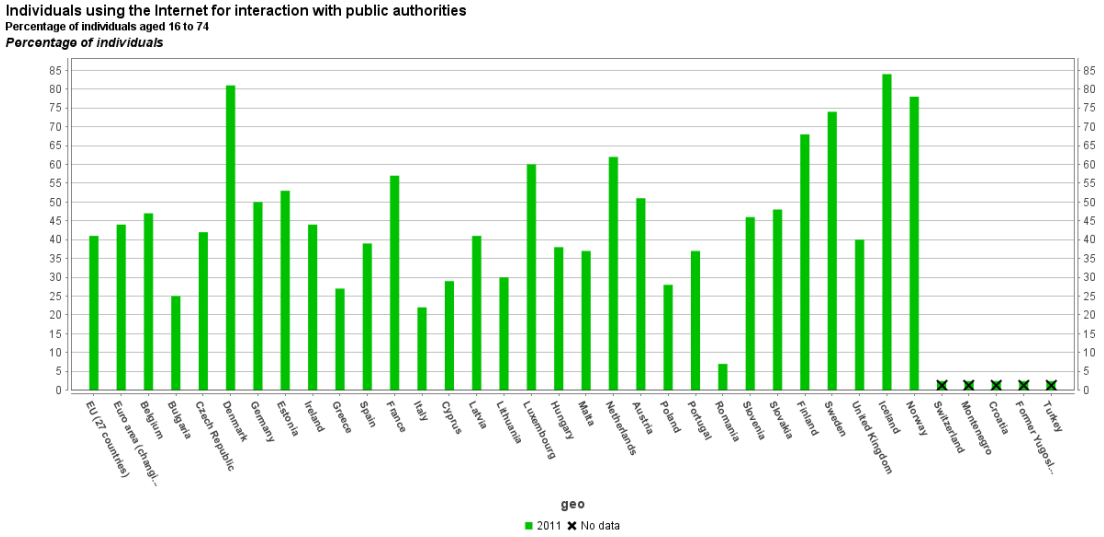


Figure 10-11: Percentage of Interaction with public authorities

Source: Eurostat website, s. http://epp.eurostat.ec.europa.eu/tgm/table.do?tab=table&init=1&language=en&pcode=tin00012&plugin=1

Individuals: Percentage of interaction with public authorities (in general), all EU27, by year (2008-2011)

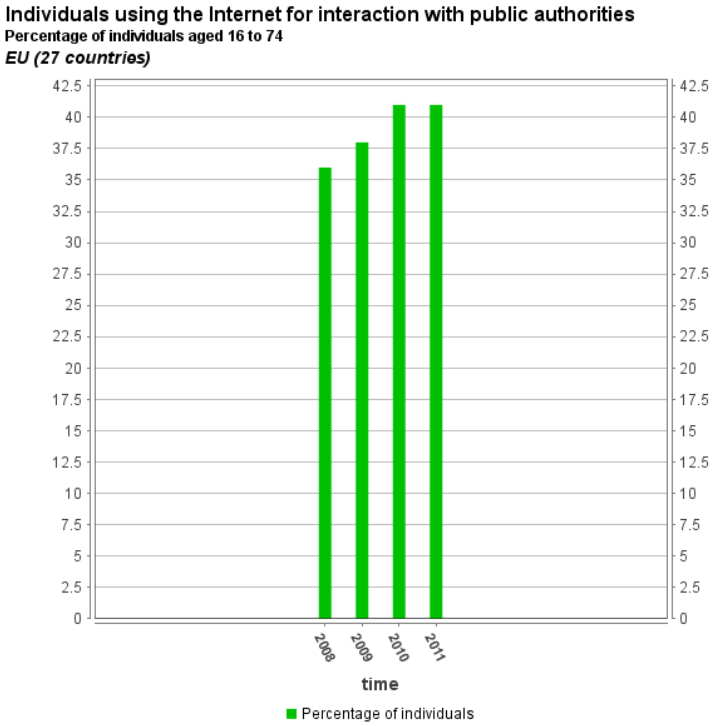


Figure 10-12: Increase of online interaction with public authorities

Source: Eurostat website, s. http://epp.eurostat.ec.europa.eu/tgm/table.do?tab=table&init=1&language=en&pcode=tin00012&plugin=1

Individuals: Percentage of interactions with the purpose of sending filled forms, 2010, by country

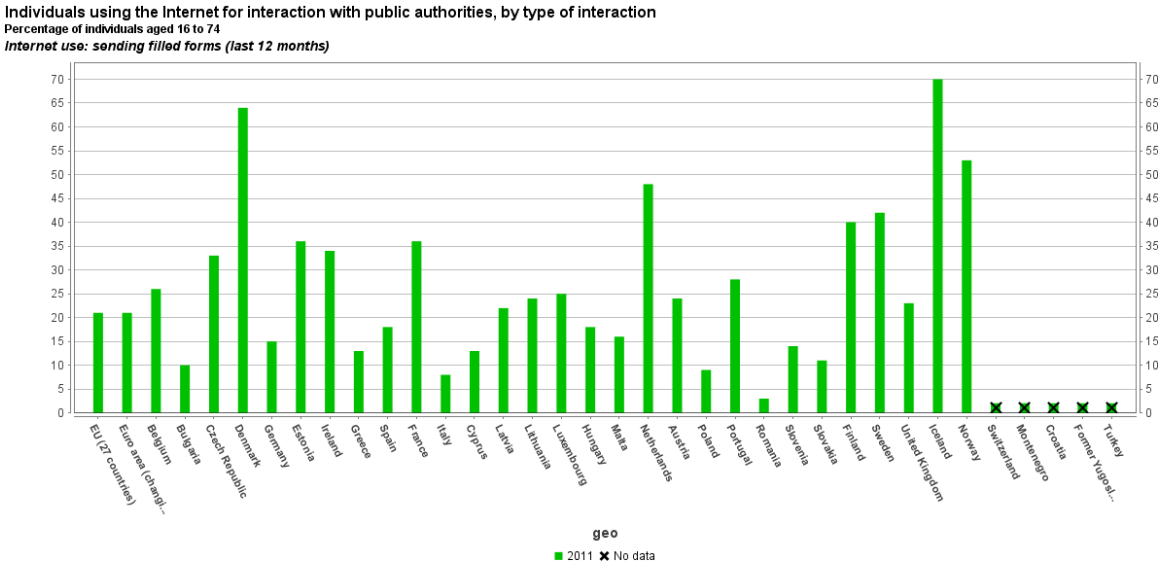


Figure 10-13: Percentage of interaction with the purpose od sending filled forms

Source: Eurostat website, s.

http://epp.eurostat.ec.europa.eu/tgm/table.do?tab=table&init=1&language=en&pcode=tin00013&plugin=1

Individuals: Percentage of interactions with the purpose of sending filled forms, all EU27, by year (2008-2011)

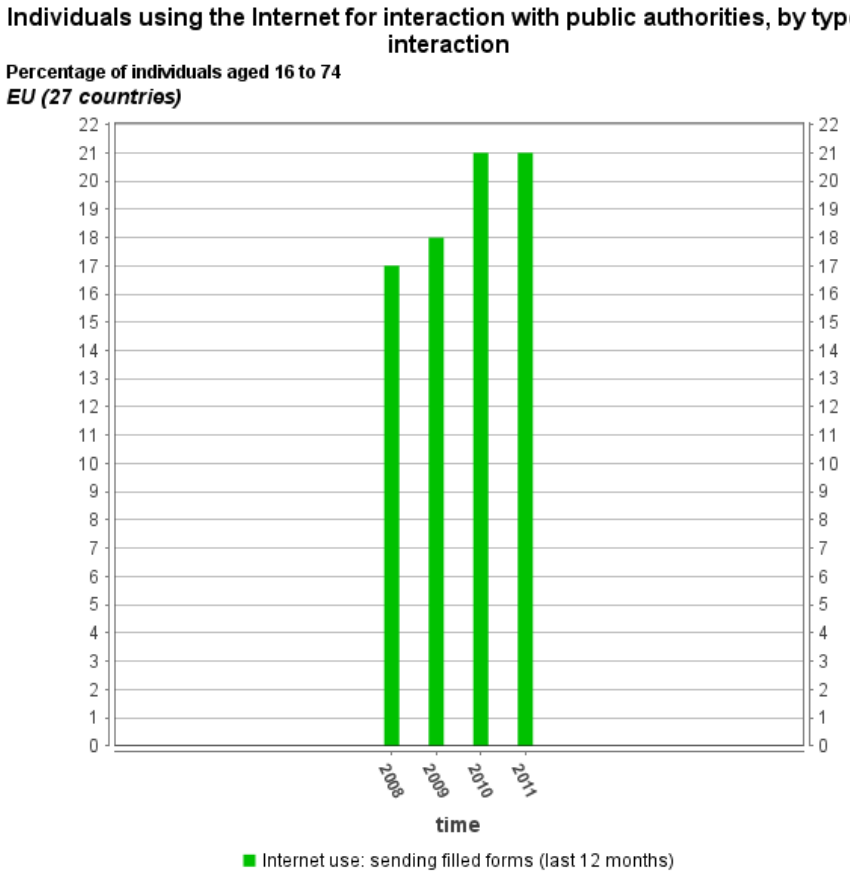


Figure 10-14: Increase of interaction for sending filled forms

Source: Eurostat website, s. http://epp.eurostat.ec.europa.eu/tgm/table.do?tab=table&init=1&language=en&pcode=tin00013&plugin=1

Individuals: take-up gap, 2010, by country

Figure 4.15: eGovernment take-up gap for citizens services, by gap-size (in %)

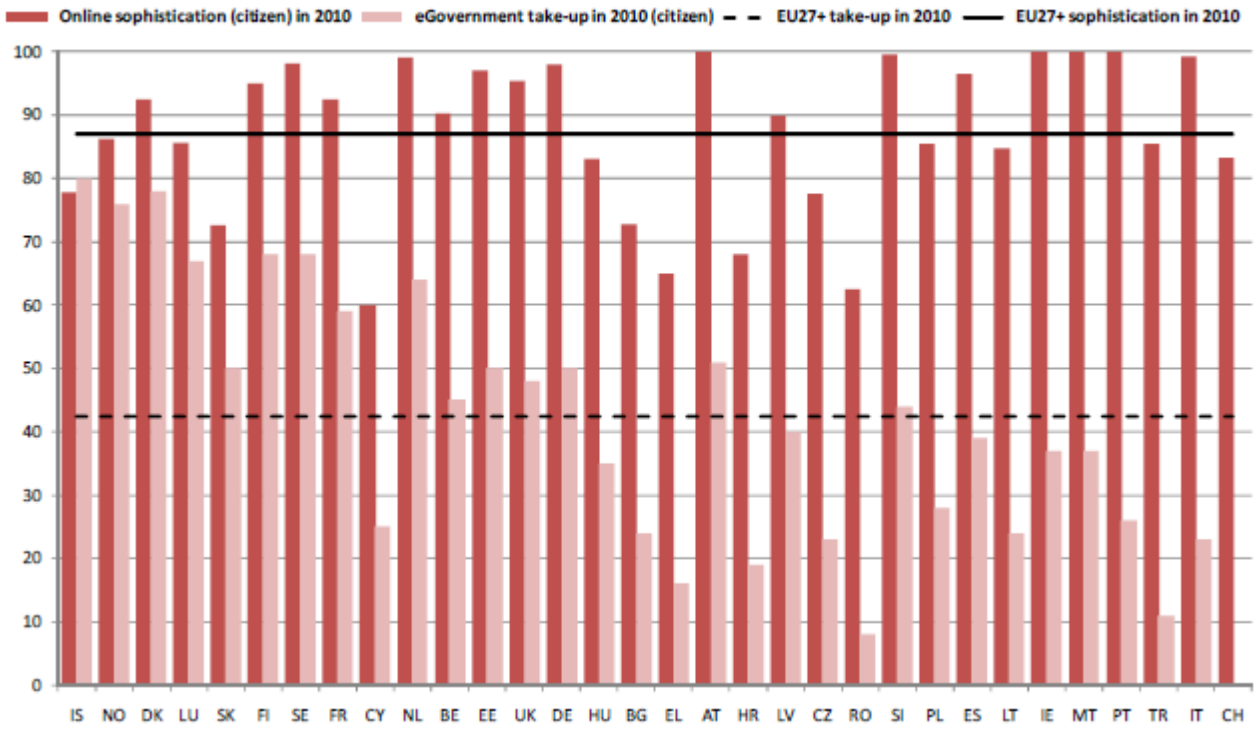


Figure 10-15: eGovernment take up gap for citizen services

Source: eGovernment Benchmark 2010

Enterprises: Percentage of interaction with public authorities (in general), 2010, by country

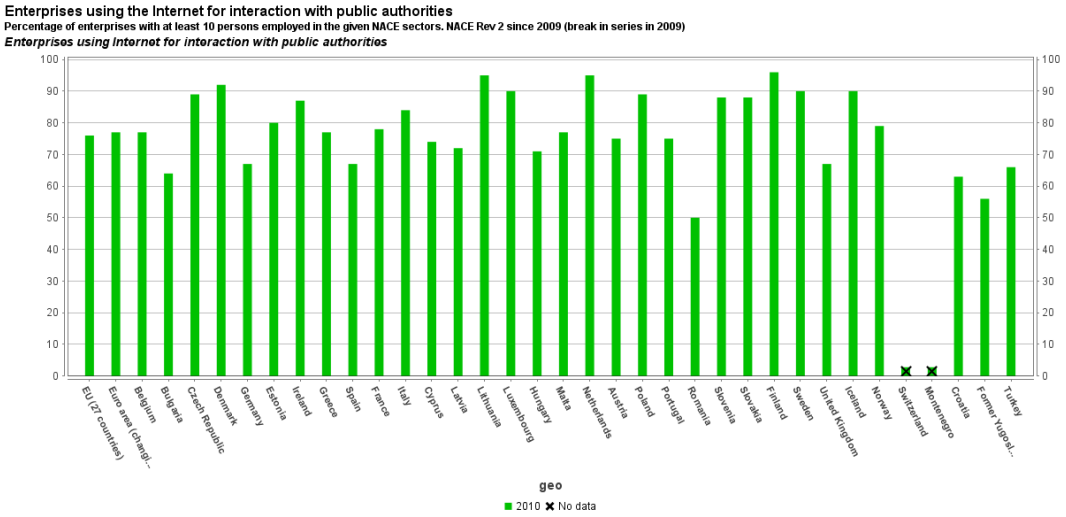


Figure 10-16: Percentage of Interaction with public authorities, by country

Source: Eurostat website, s.

http://epp.eurostat.ec.europa.eu/tgm/table.do?tab=table&init=1&language=en&pcode=tin00107&plugin=1

Enterprises: Percentage of interaction with public authorities (in general), all EU27, by year (2004-2010)

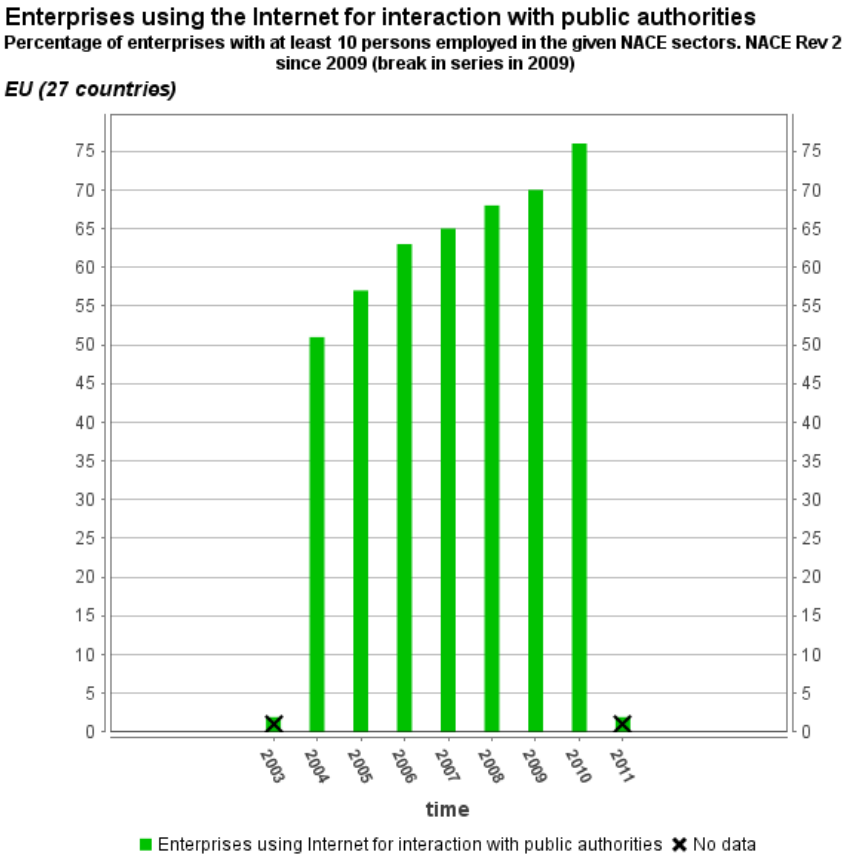


Figure 10-17: Increase of enterprise interaction with public authorities

Source: Eurostat website, s.

http://epp.eurostat.ec.europa.eu/tgm/table.do?tab=table&init=1&language=en&pcode=tin00107&plugin=1

Enterprises: Percentage of interactions with the purpose of sending filled forms, 2010, by country

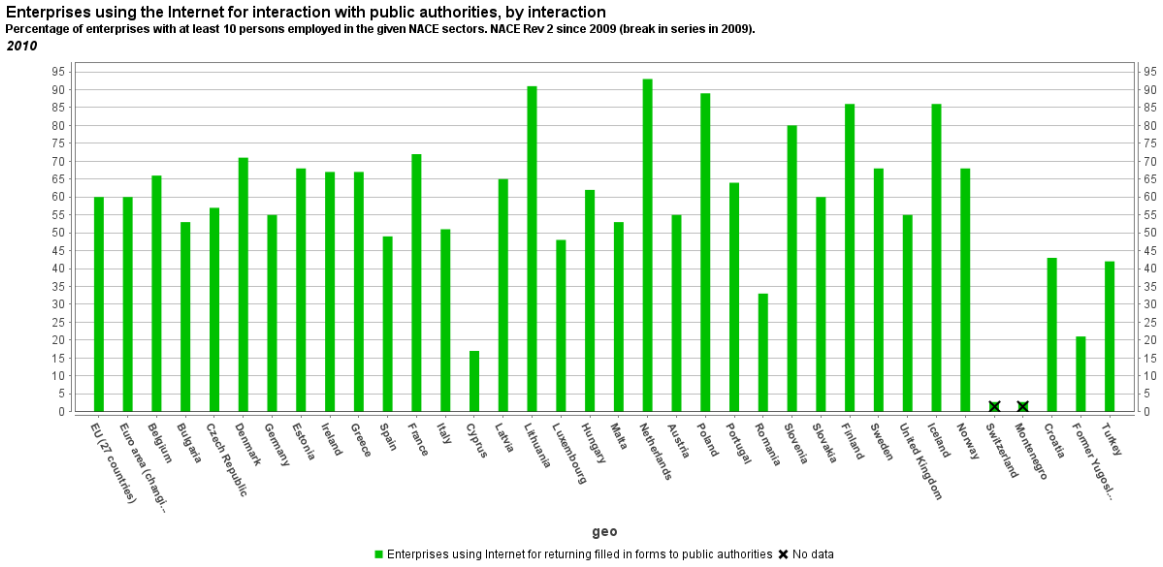


Figure 10-18: Percentage of interactions by enterprises to send filled in forms

Source: Eurostat website, s. http://epp.eurostat.ec.europa.eu/tgm/table.do?tab=table&init=1&language=en&pcode=tin00108&plugin=1

Enterprises: Percentage of interactions with the purpose of sending filled forms, all EU27, by year (2004-2010)

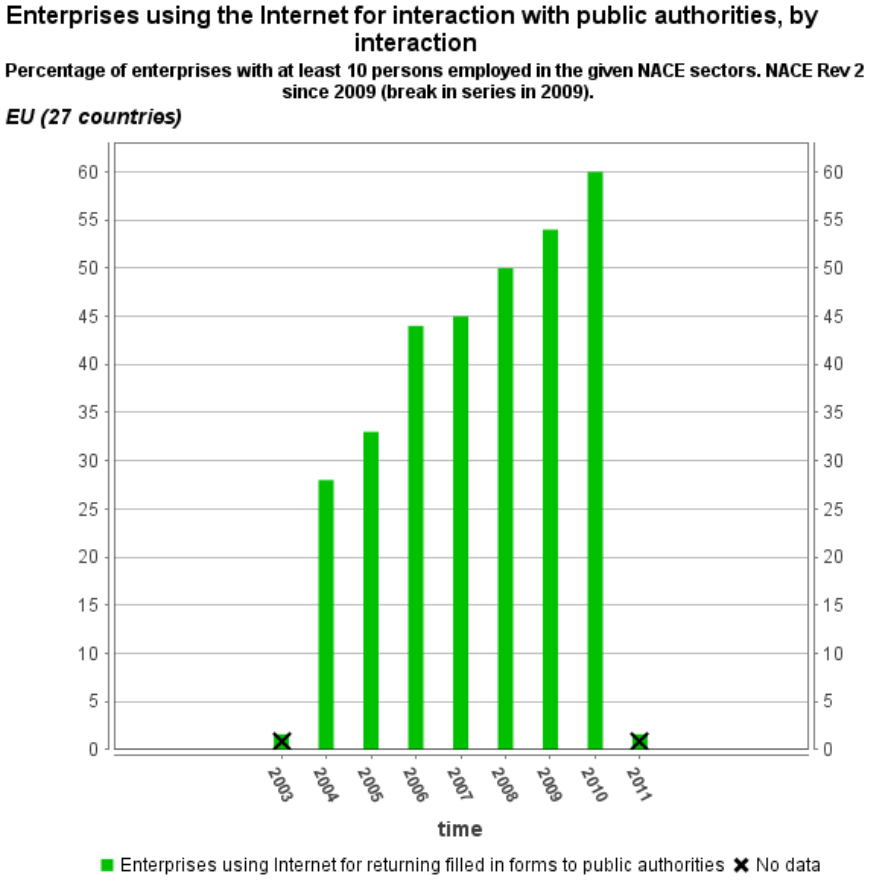


Figure 10-19 Increase of enterpise Interactions with the purpose of sending filled forms

Source: Eurostat website, s.

http://epp.eurostat.ec.europa.eu/tgm/table.do?tab=table&init=1&language=en&pcode=tin00108&plugin=1

Enterprises: Percentage of interactions with the purpose of electronic tender submission, 2010, by country

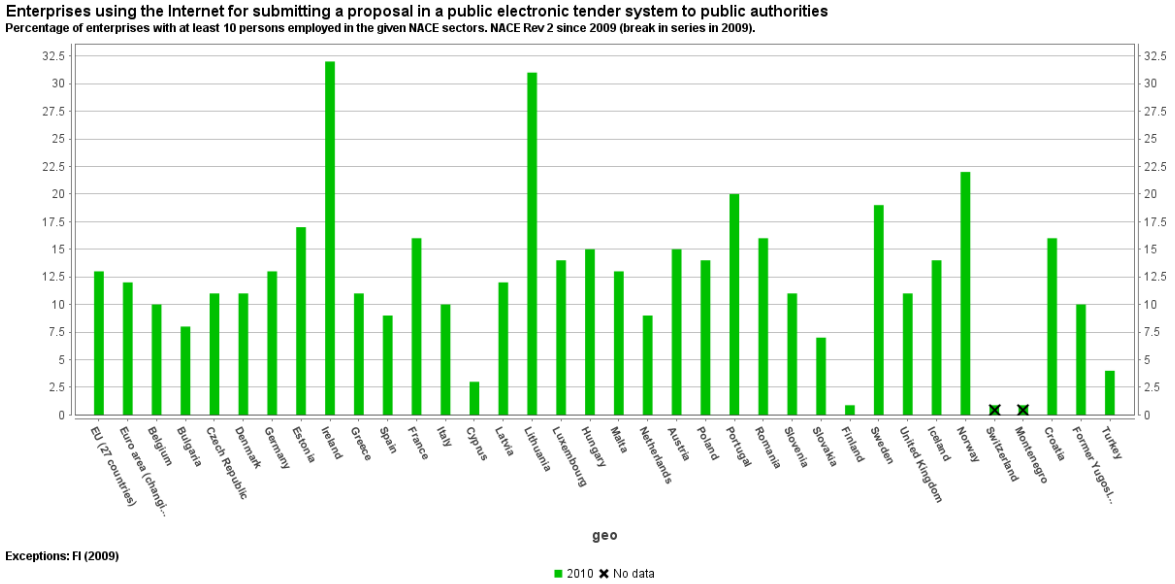


Figure 10-20: Percentage of enterprise interactions for electronic tender submission

Source: Eurostat website, s. http://epp.eurostat.ec.europa.eu/tgm/table.do?tab=table&init=1&language=en&pcode=tin00109&plugin=1

Enterprises: Percentage of interactions with the purpose of electronic tender submission, all EU27, by year (2005-2010)

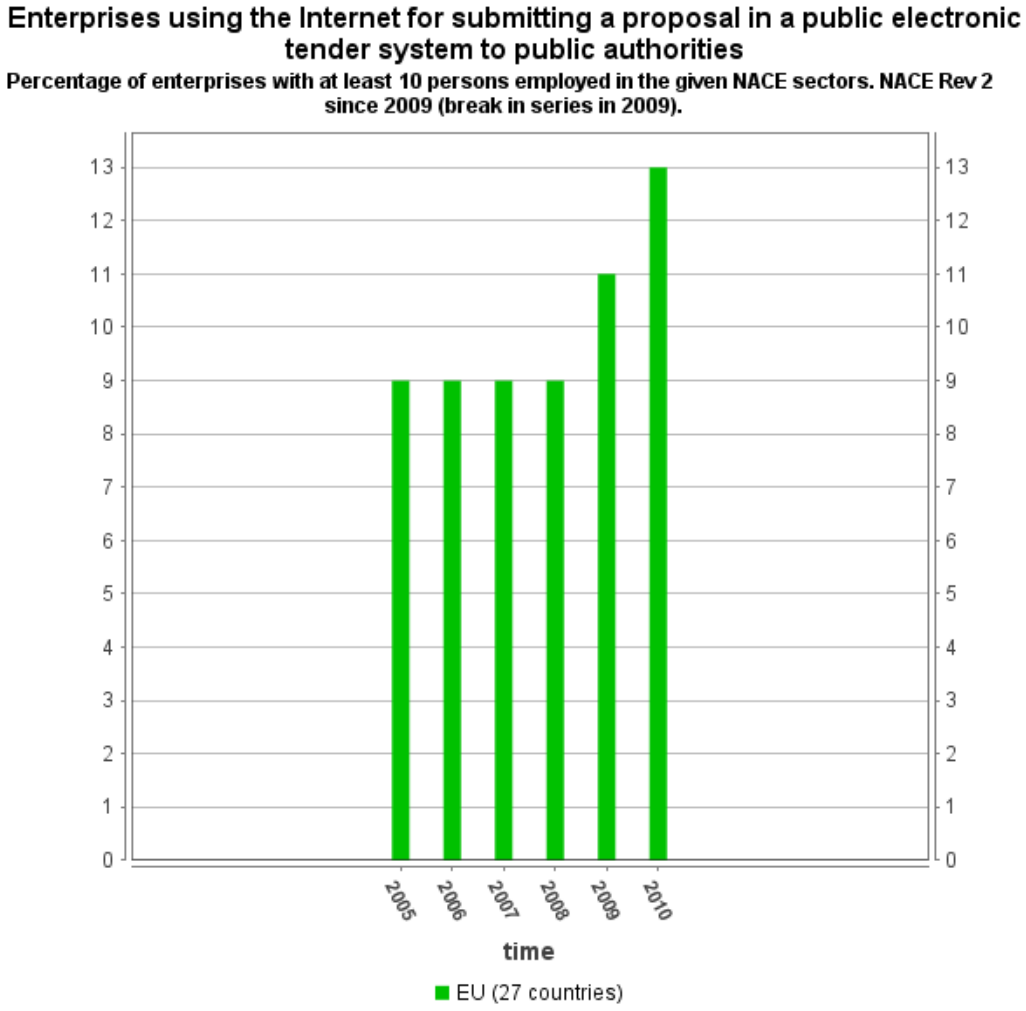


Figure 10-21: Increase of enterprises submitting tenders electronically

Source: Eurostat website, s. http://epp.eurostat.ec.europa.eu/tgm/table.do?tab=table&init=1&language=en&pcode=tin00109&plugin=1

10.3.1.3 eGovernment services for which eID is optional or mandatory

Citizens' services for which eID is optional or mandatory, 2010, by service

Figure 6.4: Citizens' services for which the usage of eID is optional or mandatory

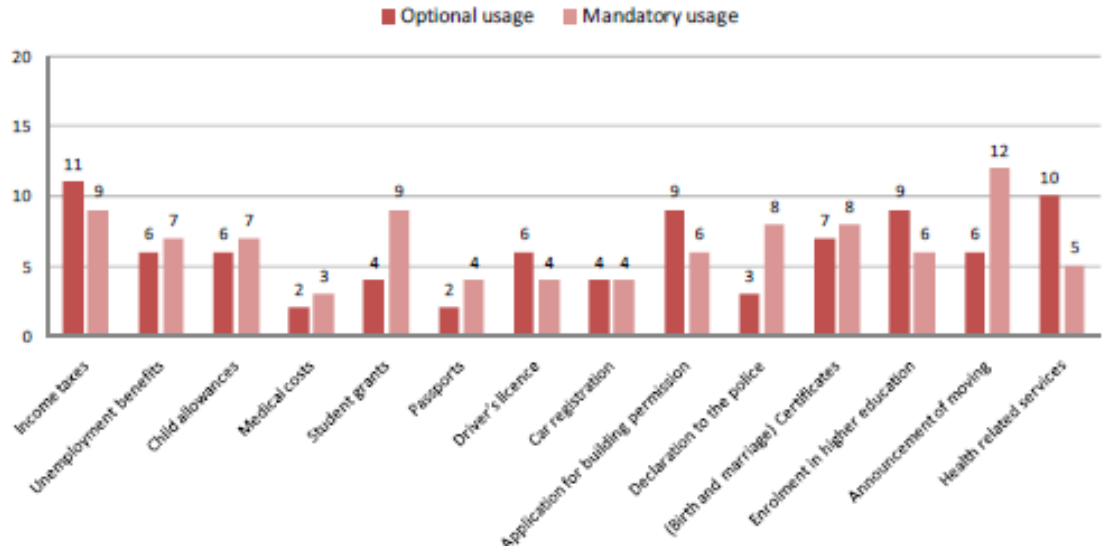


Figure 10-22: Citizen's services for which eID is optional or mandatory

Source: eGovernment Benchmark 2010

Businesses' services for which eID is optional or mandatory, 2010, by service

Figure 6.5: Businesses' services for which the usage of eID is optional or mandatory

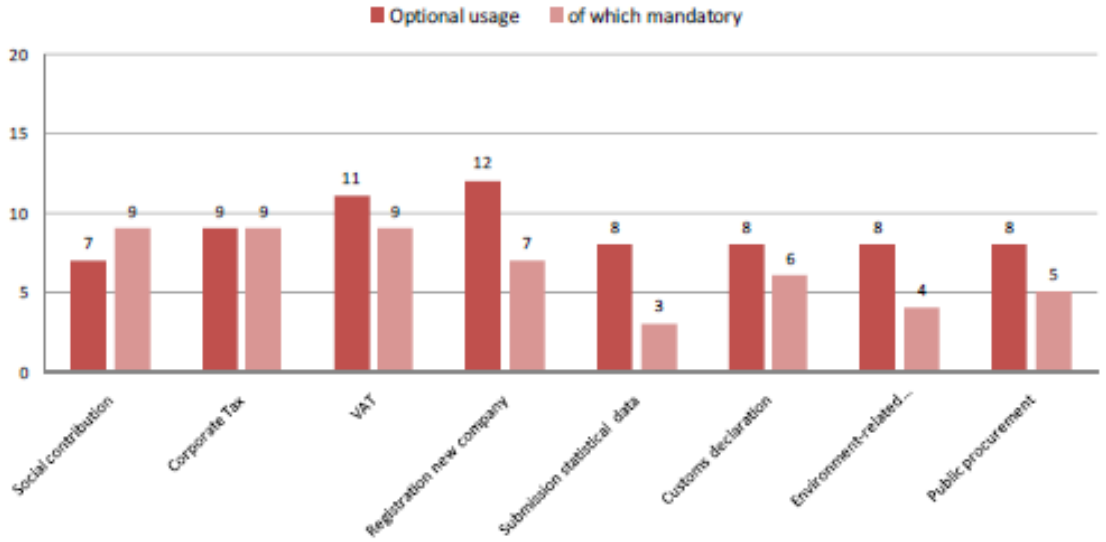


Figure 10-23: Businesses' services for which eID is optional or mandatory, 2010, by service

Source: eGovernment Benchmark 2010

10.3.2 eProcurement

According to the report on Digitizing Public Services in Europe: Putting ambition into action 9th Benchmark Measurement | December 2010 Prepared by Capgemini, IDC, Rand Europe, Sogeti and DTi, eID is mandatory for public procurement in 8 out of 13 countries surveyed.

Businesses' services for which eID is optional or mandatory, 2010, by service

Figure 6.5: Businesses' services for which the usage of eID is optional or mandatory

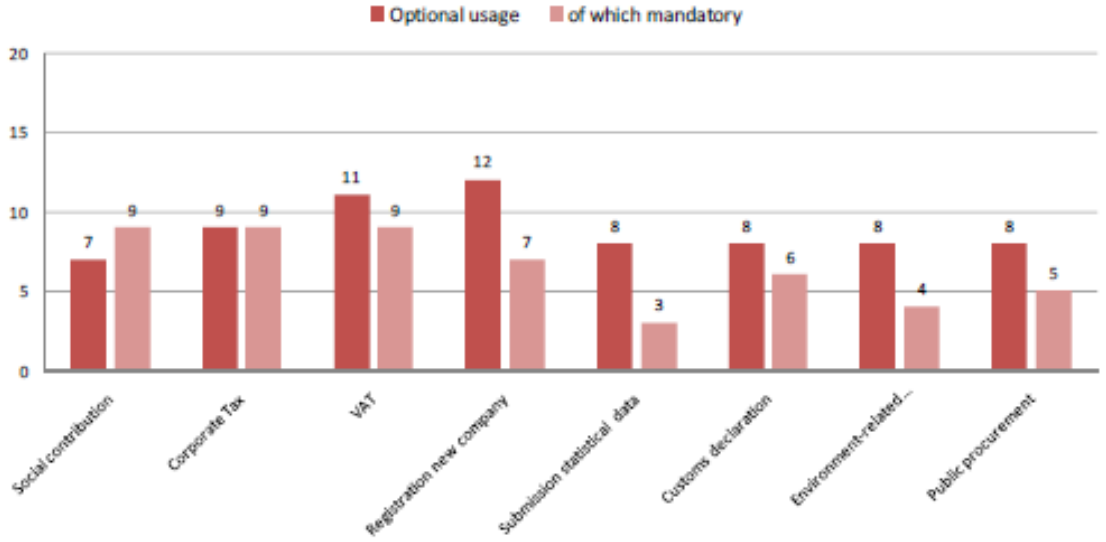


Figure 10-23: Businesses' services for which eID is optional or mandatory, 2010, by service

Source: eGovernment Benchmark 2010

10.3.2.1 ePROCUREMENT

Geographical scope of eProcurement platforms, 2010

Figure 3.16: Geographical scope of eProcurement platforms (% on total)

Figure 10-24: Geographical Scope of eProcurement

Source: eGovernment Benchmark 2010

Sectoral scope of eProcurement platforms, 2010

Figure 3.17: Sectoral scope of eProcurement platforms (% on total)

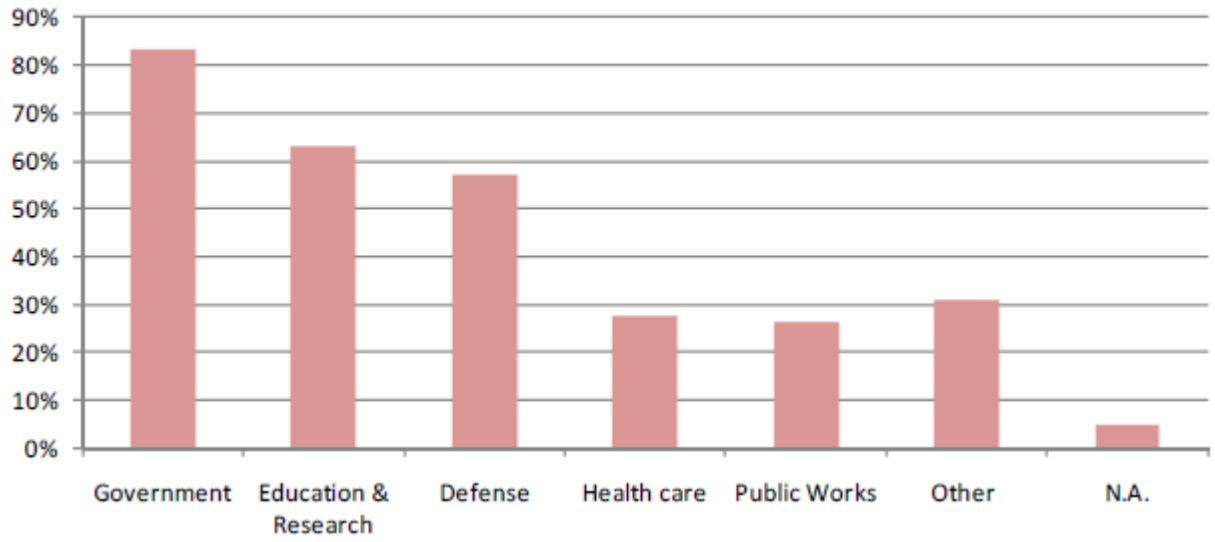


Figure 10-25: Sectoral Scope of eProcurement

Source: eGovernment Benchmark 2010

eProcurement visibility, 2010, by country

Figure 3.19: eProcurement visibility benchmark (in %)

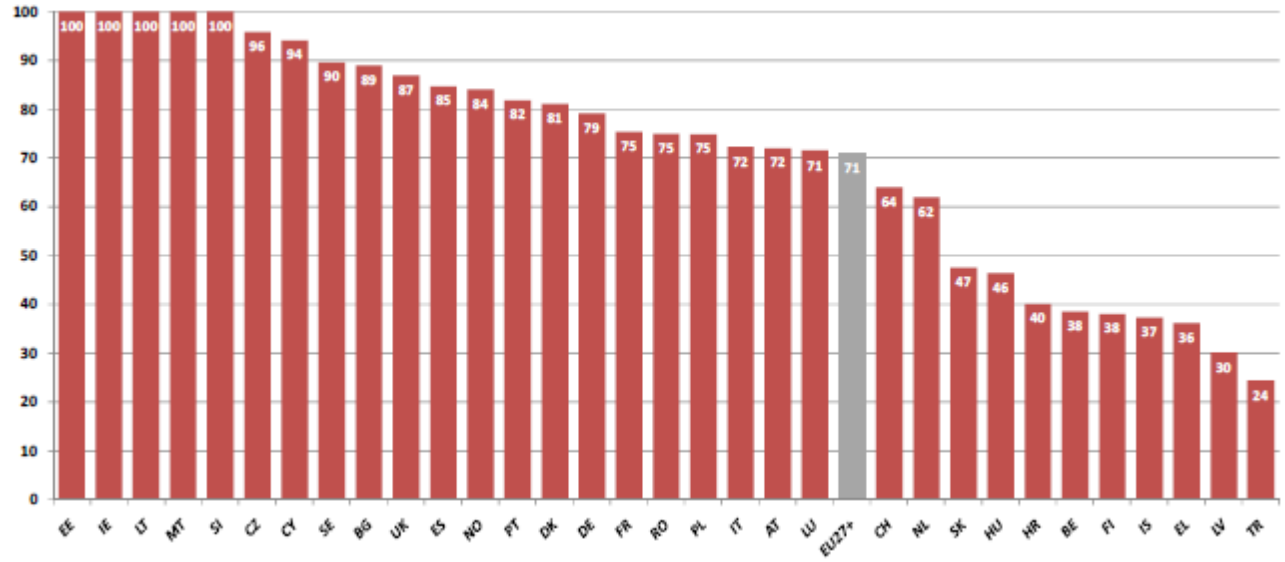
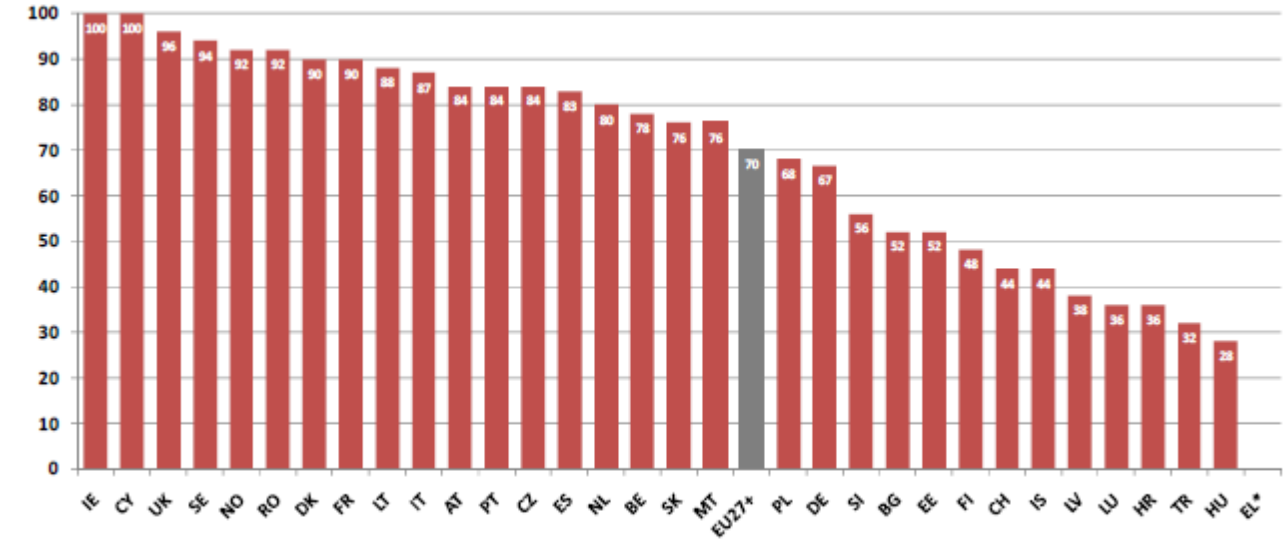


Figure 10-26: eProcurement visibility benchmark

Source: eGovernment Benchmark 2010

eProcurement pre-award process availability, 2010, by country

Figure 3.20: eProcurement pre-award process availability indicator (in %)



* Greece is not included in the benchmark because its platform is not operative yet.

Figure 10-27: eProcurement pre-award process availability indicator

Source: eGovernment Benchmark 2010

10.4 Barriers to the uptake of cross-border online services

10.4.1 Lack of cross-border eID as a barrier

The previously mentioned sources imply that the lack of interoperable national eID systems is a barrier to some extent.

As an enabler for many other services, the cross-border use of eID (or the lack thereof) may affect for example online services such as reclaiming VAT

However, for the present impact assessment the key question is: how big is the part which eID plays in this?

Nearly half (47% or 584 of 1251) of respondents to the SME Panel indicated that they use eID to complete procedures with public authorities, but internal procedures (25%), interactions with other companies (24%), and consumer relations (18%) were also indicated. This suggests that for these respondents, eID is an enabler for these activities.

The organizations responding in the Public Consultation indicated they expected a number of benefits for users from mutual recognition and acceptance of electronic identification and authentication across Europe, including: simplification of access to online services (76%), the reduction of numerous UID/passwords (64%), increase of user convenience (64%), and reduced exposure to ID theft (48%). Here, the respondents suggest that eID harmonization may assist in reducing the described barriers to accessing services.

In the PROCURE project it is argued that while eProcurement is considered one of the most promising services within e-government in terms of time and efficiency, this does not work at the moment for cross-border eProcurement.[76]

Respondents to the European Business Test Panel on "Cross border public procurement" (237 respondents, 82% SME) indicated that 23% of the respondents had participated in cross-border public procurement. Non-participating businesses found administrative obstacles as the most important obstacle (45%). The main reasons that are listed by the PROCURE project for the low uptake are lacking technical interoperability and legal harmonization, including the problem of identification of the signatory in form of unique national specific person identifiers. This is confirmed by respondents to the Public Consultation, of which 46% listed limited EU cross-border interoperability as an issue having a negative impact on the uptake of eSignature, in which eID plays a role.[77]

10.5 eID and the private sector

In most Member States national eIDs are used to, at least, access public online services, some of which are issued by the private sector. The cross-sector use of eID can include both: the private sector can potentially use national eID and governments can recognize eIDs issued by private entities. The relation of "national" eID to the private sector is important because it may have a big impact on the uptake of eID.

Different forms of regulation may impact the way in which private and national eID work together. Three of the assumptions elaborated by the study team relate to private sector eID, namely that the private sector plays a role in generating a critical mass for eID uptake (12), that privately-issued eIDs can be used

[76] "Electronic Signatures as Obstacle for Cross-Border E-Procurement in Europe: Lessons from the PROCURE-project" (https://www.eid-stork.eu/dmdocuments/public/ElectronicSignaturesAsObstaclesForCross-BorderEProcurementInEurope_LessonsFromThePROCUREProject.pdf)

[77] "Cross border public procurement", 2011, European Business Test Panel

in interactions with Member States public authorities (11), and that the private sector is willing to use government-issued or approved ("formal") eID's for their services (11b).

The need for a "critical" mass is confirmed by a 2009 report by the OECD on the role of digital identity management in the internet economy. It states that identity management initiatives are unlikely to pay off unless embraced by a critical mass of participants in the internet economy. The promise of these technologies depends not just on their technological development, but also on the actual uptake in the context of different value transactions. For private eID systems, an issue is that consumers do not seem to be willing to pay for eID systems.[78]

This is also argued by IPTS in a 2010 report on the State of the eID market, and the conclusion is drawn that "in order to fight market fragmentation as a result of the private sector creating piecemeal schemes rather than generic, interoperable infrastructure, governments should provide those components of trusted infrastructures that are too risky or costly for private sector organizations to develop." Provisioning clear standards for government adoption of eID technologies will support greater private-sector investment in eID.[79]

In the same report, IPTS concludes that "commercial credentials as sole identifiers when authenticating individuals and instead rely on proprietary sources, while a range of commercial breeder documents are used to make a risk judgment on identity, they are not used as the sole credential. Conversely, commercial providers will generally trust government-issued credentials even if these are used out of context – a passport is not designed for opening a bank account, but will be accepted for doing so." The same may be assumed for eID.

These sources indicate that the uptake of national and private-sector-issued (cross-border) eID are related, and should not be viewed in isolation. Government investment in eID may help in creating components of trusted infrastructures that are too risky or costly for private sector organizations to develop, while private sector uptake of eID is an important factor in creating a "critical mass" for the uptake of eID.

10.6 Involvement of stakeholders

10.6.1 Introduction

The two important and recent sources of evidence for the present study are the Public Consultation (2011) on electronic identification, authentication and signatures and the SME Panel survey (2011), the latter of which gave enterprises the opportunity to give their opinion on how new legislation on eIdentification and eSignatures could meet their needs. Both of them were launched by the European Commission[80].

10.6.2 Public Consultation

The Public Consultation on Electronic identification, authentication and signatures in the European digital single market was held from February-April 2011, and received a total of 434 contributions Of these, 417 respondents contributed via the online tool and 17 respondents contributed via email; only the respondents that used the online tool were used for statistical analysis. Little less than half of these responses were on behalf or an organization such as a large or small private company, a public authority or an industry association.

[78] "The Role of Digital Identity Management in the Internet Economy", 2009, OECD

[79] "The State of the Electronic Identity Market", 2010, IPTS

[80] A list of contributors and the results of the consultation are publicly available online at: http://ec.europa.eu/information_society/policy/esignature/eu_legislation/revision/pub_cons/ .

The analysis of the consultation was based on the responses from both individuals (51,07%) and organizations (48,93%).

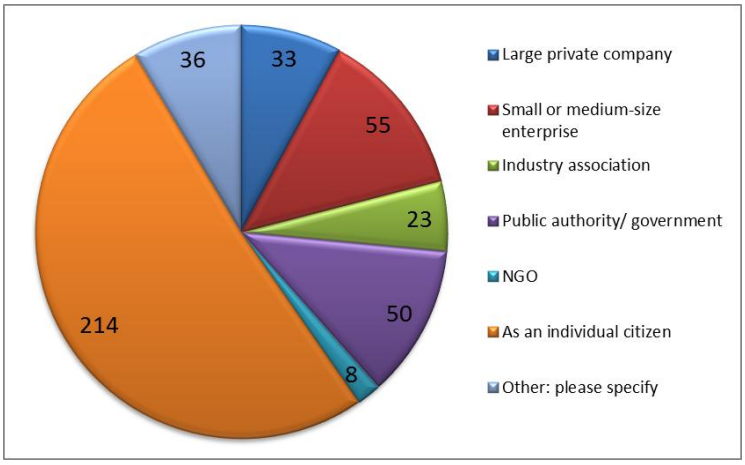


Chart: respondents to the Public Consultation

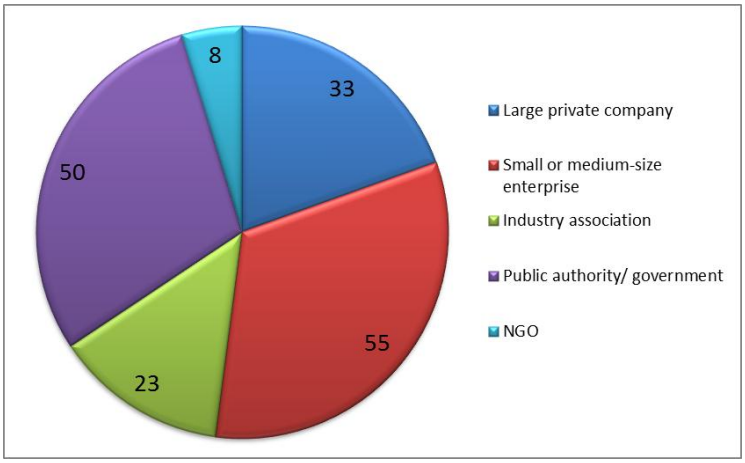


Chart: respondents to the Public Consultation, excluding individuals

10.6.3 The results of the Public Consultation

The public consultation clearly shows that the major part of the panel, nearly 80% uses eIdentification, eAuthentication and eSignatures. When focusing on the specific application fields, the data show a strong priority on secure transactions (60,62%), integrity of electronic documents (56,56%) and on the legal effect (42,24%). It is remarkable that nearly 75% of the respondents use eIdentification, eAuthentication and eSignatures either daily or weekly.

Question 2.2 For what online transactions do you consider electronic identification, authentication and signatures useful in coming years?

This question looks into the main area of application of eSIGs, eIDS and eAUTH. Remarkably a vast majority (84,96%) mentions eGovernment services, online banking and financial transactions (80,91%) and issuance of authentic electronic documents (72,08%). eCommerce and eBusiness are rated about the same (around 65%). Electronic Public Procurement, though high, is mentioned by 57,28% of the respondents.

Question 2.4 Would a stronger involvement of financial institutions in the provision of trusted e-signature and e-identification services have an impact on the take-up of e-signature and e-identification in other sectors?

The fact that 82,34% of the respondents agrees with a stronger involvement of financial institutions in the provision of trusted e-signature and e-identification services will have an impact on the take-up of e-signature and e-identification in other sectors. Stakeholders have the clear perception that the private sector which has developed significant experience in implementing and operating eID and eSIG applications shows a high level of trust in these types of organisations. This trust should be leveraged to increase the diffusion of eID based application and to enlarge the user base.

Question 2.5 Do you think that there are specific interoperability or security aspects that should be taken into account to foster the use of electronic signatures, identification and authentication through mobile devices (e.g. requirements on the SIM cards, on the handset, on the mobile operator)?

This question addresses the specific interoperability or security aspects that should be taken into account to foster the use of electronic signatures, identification and authentication through mobile devices. Indirectly, the majority of responses (82,34%) indicate that there is a role for mobile telecommunications providers in eIAS.

The main problems indicated were legal aspects including liability (63,48%) and standardisation (64,92%). There are no particular problems related to business for over 70% of the respondents.

Question 4.18 Do you see a need for additional legal or regulatory measures on electronic identification at EU-level?

64,92% of the participants in the consultations agree that there is a need for additional legal or regulatory measures on electronic identification at EU-level. The most important reasons for a EU-level regulation are Transparency, Liability, Personal data protection (64,44%, 59.56%, and 77,94% respectively).

Question 4.19 What effects for the digital single market do you expect from legal provisions on an EU-wide mutual recognition and acceptance of eID issued in the Member States?

The high percentages of participants in the consultation indicate that a EU-level regulation of mutual recognition and acceptance would be beneficial for

- Legal certainty
- Reduction of administrative burden
- Increase of cross-border digital mobility.

Question 4.20 How could users provided with electronic identification and authentication means benefit from their mutual recognition and acceptance across Europe and in which sectors?

63% of the respondents are of the opinion that the widespread diffusion of eID and eAUTH means would increase user convenience, simplify access to online services, reduce the number of user IDs required. Less participants in the consultation believe that eIDs would reduce exposure to ID theft.

Question 4.21 What are the specific aspects that should be taken into account to achieve cross-sector interoperability of electronic identities?

According to 59,27% respondents EU-wide legislative measures on eID should cater for a common legal basis, for common specifications for eIDs, and for personal data protection. Identity portability and the use of multiple identities issued by different providers were indicated by 27% respondents as less important .

Question 5.23 What European Union legislative measures on e-signatures, e-identification, and e-authentication of natural and legal person claims, would be appropriate in your opinion to best meet the challenges of the digital single market?

Nearly 50% of the participants have indicated that legislative measures on e-identification, e-authentication and e-signatures should address the revision of the legal framework embracing all requirements concerning e-identification, e-authentication and e-signatures, including related issues, to best meet the challenges of the digital single market.

Questions 3.17.A and 3.17.B Are there specific aspects that should be taken into account to address electronic archiving?

Nearly 80% of the respondents use eIdentification. 44,60% of which in form of a basic user ID and password, 22,86% a medium level smart card and 12,55% electronic ID cards. 22% indicated not to use eID at all.

The majority of the participants uses eID to complete procedures of public authorities (46,68%), almost 24% of whom for internal procedures and interactions with other companies and 17,67% for customer relations.

Question 3.18.A and 3.18.B Do you see a need for additional legal or regulatory measures on electronic identification at EU-level?

As main reason for non-using eIDs was indicated that it is not needed for business (62,61%). 20,68% were not aware at all what eID means.

Those not using eIDs indicate that they would use it in case it was mandatory (35,37%) and more widespread (25,58% if used in the specific business sector and 25,61 if used in all sectors).

10.6.3.1 Expectations with regard to cross-border recognition of eID

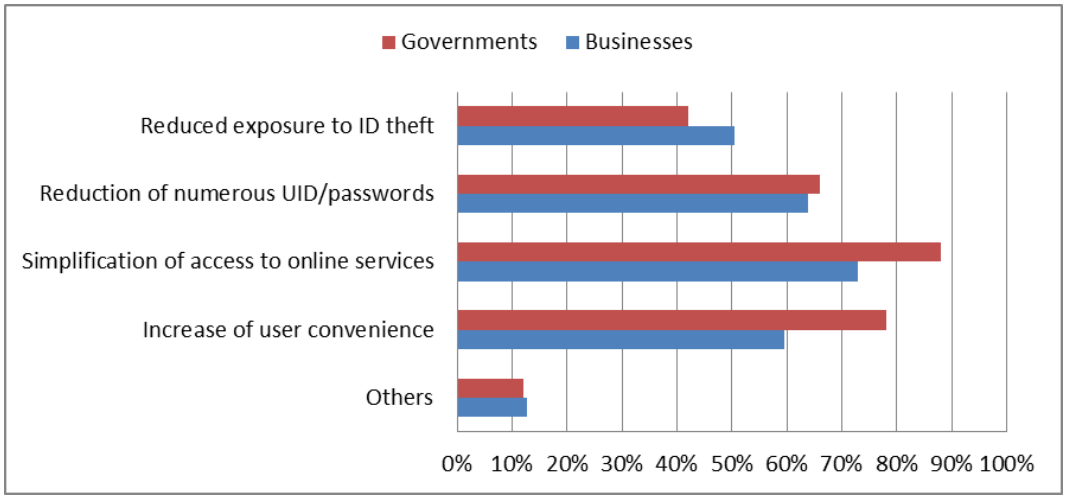


Figure 10-28: expectations with regard to cross-border recognition of eID (Public Consultation)

10.6.3.2 Need for regulation

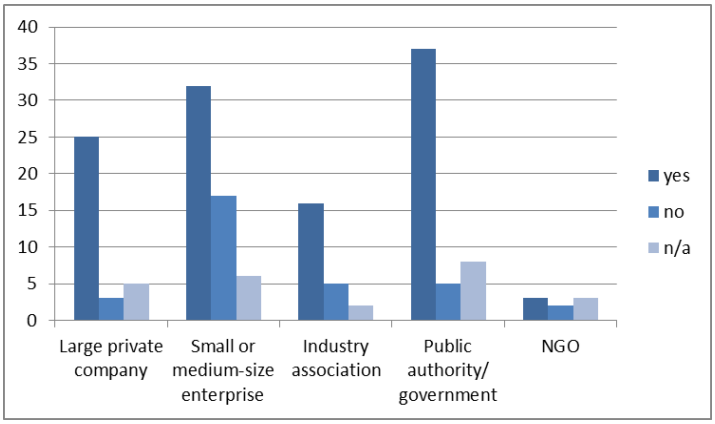


Figure 10-29:perceived need for additional regulation on eID at the EU-level (Public Consultation)

10.6.3.3 Desired legislative measures

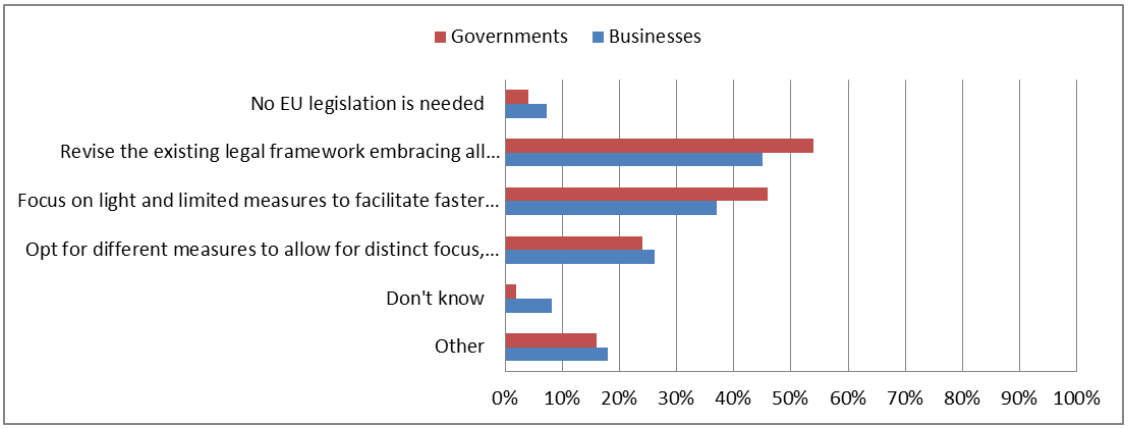


Figure 10-30:opinions on appropriate kind of legislative measures to be taken on eID (Public Consultation)

10.6.3.4 Preferences: centralized vs. federated approach

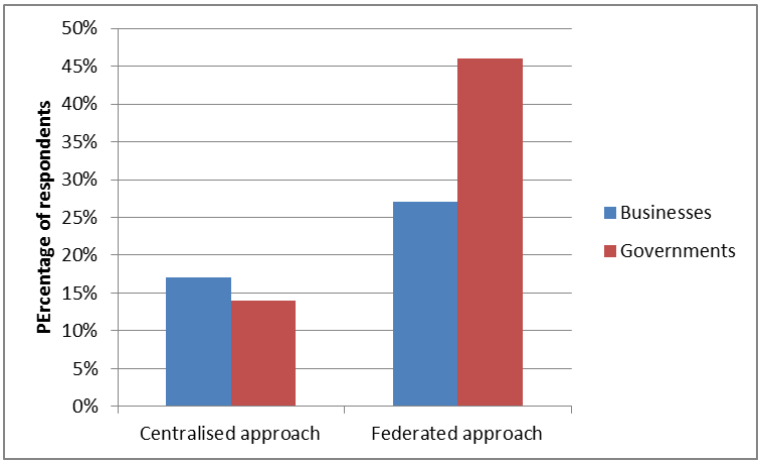


Figure 10-31: preferences of respondents for a centralized versus federated approach (Public Consultation)

The majority of the government respondents to the public consultation declare a preference for a federated approach which would give the Member States administrations the main responsibility over the management of the eID systems and only a defined level of coordination to the European Commission. Businesses are less concerned with their role and only about 25% prefer a federated approach. On the other hand, only about 15% of the businesses and administrations would prefer a centrailised approach to the management of the interoperability and mutual recognition of corss-border eIDs.

10.6.4 SME Panel on eSignature and eID

The SME Panel was held from October-December 2011. The consultation of the SME Panel on eSignature and eID received 1251 responses, the majority from micro-enterprises (39,97%) and from Small and Medium-sized enterprises (42,93% in total). Concerning the sector in which the respondents are active, the largest concentrations were manufacturing (17,99), ICT (14,31%) and professional, scientific and technical activities (12,71%). The share of public Administration was considerably low (0,48%) which could eventually be explained by the fact that they already participated in the Public Consultation.

1.A. Please specify the size of your company	# of responses	% of total (1251)
Individual (1 person)	139	11,11%
Micro (less than 10 employees)	500	39,97%
Small (less than 50 employees)	364	29,10%
Medium-sized (less than 250 employees)	173	13,83%
Large (more than 250 employees)	75	6,00%

Response to question 1.A. of the SME Panel on e-signature and e-id (2011)

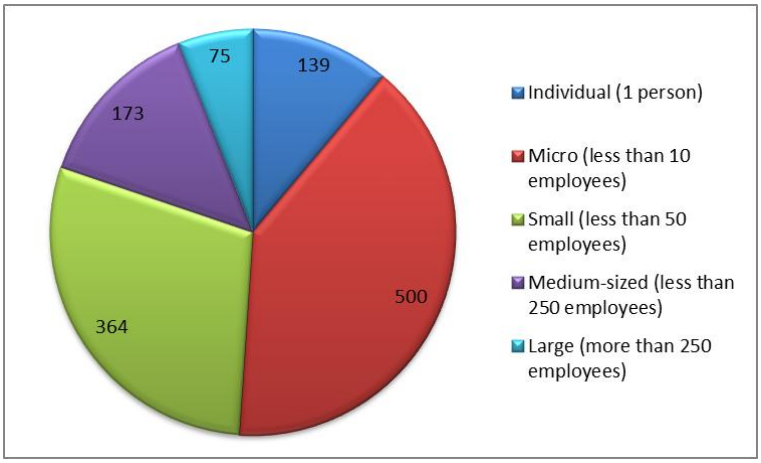


Chart: respondents to the SME Panel

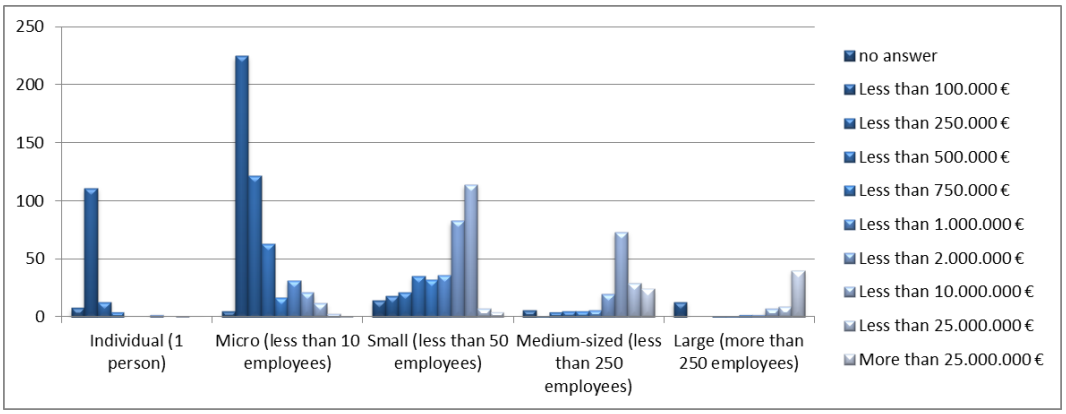


Chart: respondent company turnover and size

10.6.5 The result of the SME Panel

Questions 1.C, 1.D Please indicate the annual turnover of your company; Please indicate which of the following information and communications technologies (Infrastructure and connectivity) are used or implemented in your company

Over 70% use business accounting software, while other software is very much dependent on the business setup (production management, stock management, distribution management).

It is peculiar that CRM software is not mentioned, neither ERP applications.

A vast majority of participating enterprises uses online payments (67,95%), around 30% uses eID, eInvoicing, and electronic documents archiving.

Less than 20% have an electronic catalogue and electronic commerce systems.

It would be useful to have an indication of the share of cross-border transactions in respect to the national/local ones.

Question 2.6, 2.7 How frequently does your enterprise carry out electronic secure transactions (ie. online banking, electronic invoicing, …)? ; What solution for electronic signature means do you use in your enterprise?

The majority of the respondents (over 45%) carries out electronic secure transactions (ie. online banking, electronic invoicing, …) daily or weekly. 23,42% use smart cards, 25,90 USB tokens, and 22,14% software-only based solutions.

Question 2.8 How many of members of your staff (including you) have electronic signature means?

Over half of the respondents (52,20%) report that 1-5 members of staff have an electronic signature, probably business-related, i.e.: disregarding the personal ones. 38,53% do not provide any response.

44,60% confirms that electronic signature means are never shared. This happens in 15% of the cases, while 37,49% does not provide any answer.

Questions 3.17.A and 3.17.B For which purposes do you use electronic identification?

Nearly 80% of the panel members use eIdentification. 44,60% a basic user ID and password, 22,86% a medium level smart card and 12,55% and electronic ID card.

22% does not use eID at all.

The majority of the respondent uses eID to complete electronic procedures of public authorities (46,68%),.

Question 3.18.A and 3.18.B My company does not use electronic identification because ; I would use electronic identification if

10.6.5.1 Usage of eID

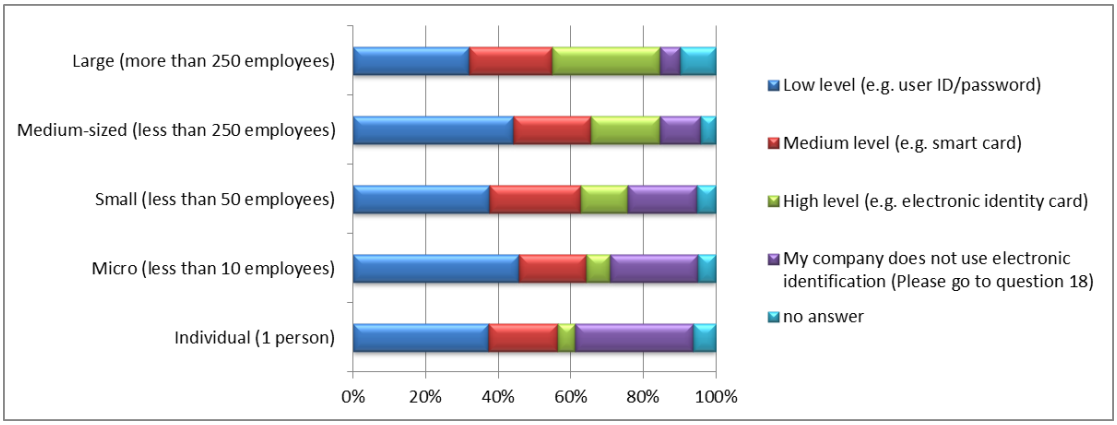


Figure 10-32: usage of eID by companies (SME Panel)

10.6.5.2 Purpose of eID usage

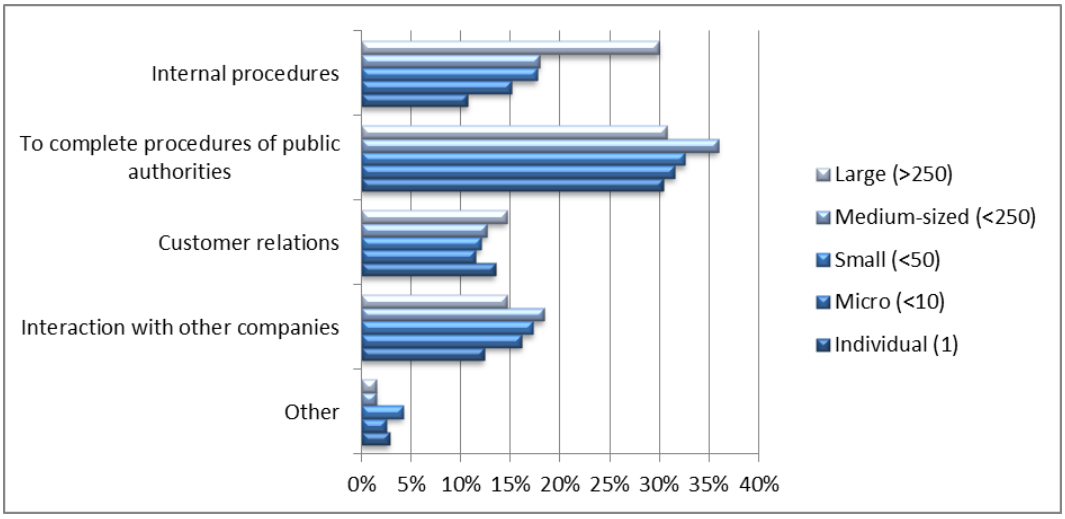


Figure 10-33: Purpose of eID use by companies (SME Panel)

10.6.5.3 Reasons for not using eID

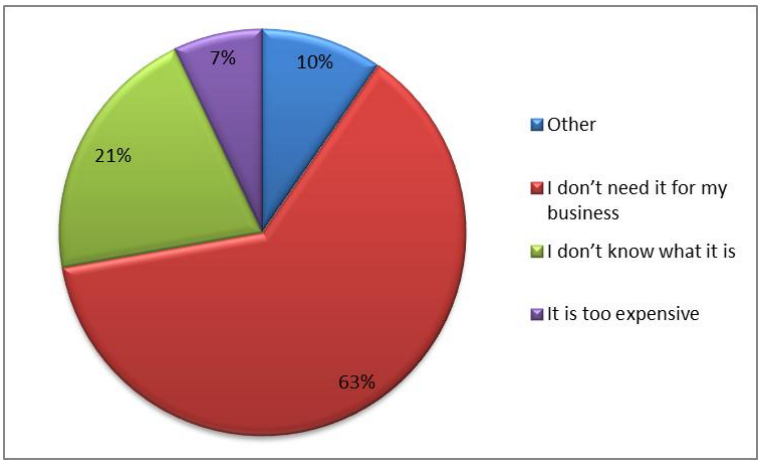


Figure 10-34: Reasons for not using eID (SME Panel)

10.6.5.4 Potential reasons for companies to use eID

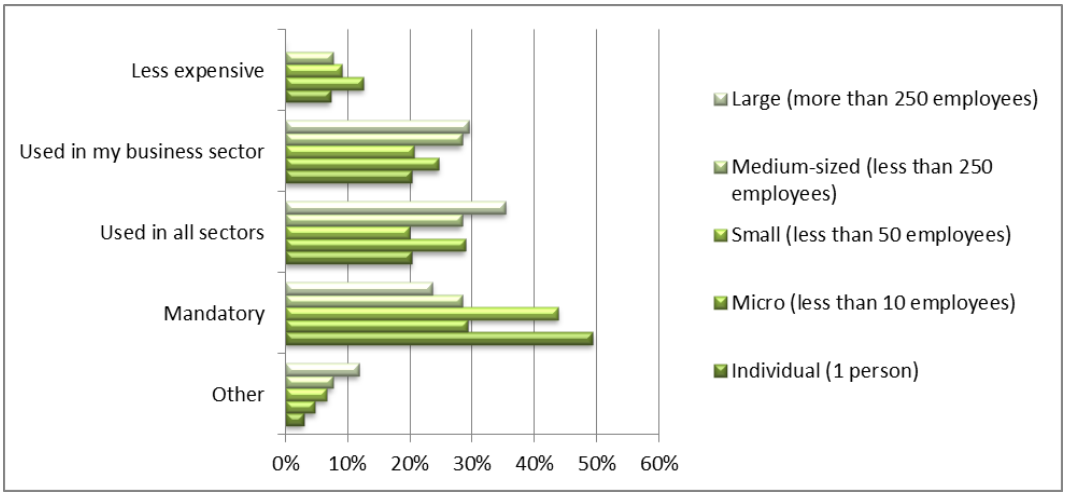


Figure 10-35: Potential reasons for companies to use eID (SME Panel)

10.7 Statistics and data

10.7.1 Cross-border services, demographics and business demographics

10.7.1.1 Immigrants and Commuters in the EU

	2009
Immigrants and commuters between EU Member States	1,790,000
Number of branches and immigrant business start-ups	140,000
Number of immigrants and commuters as potential users of cross-border eGovernment services and of cross-border eID	605,000
Number of "latent[81]" users among the immigrants and commuters	657,000
Total potential demand for online cross-border services	1,262,887

10.7.1.2 Number of commuters by country of destination 2006/7

Source: MKW. 2009. Scientific report on the mobility of cross-border workers within the EU-27/EEA/EFTA countries. *Estimate from EU average per 1,000 inhabitants.

	Number of commuters to the Member State	**Commuters per 1,000 inhabitants**
Austria	48,142	5.2
Belgium	38,699	3.7
Bulgaria	300	0.1
Cyprus	820*	1.0
Czech Republic	20,747	2.2
Denmark	15,333	2.8
Estonia	1,000	0.8
Finland	22,360	4.2
France	10,653	0.2
Germany	86,334	1.0
Greece	5,600	0.5
Hungary	14,089	1.3
Ireland	17,000	4.0

[81] Immigrants and commuters having indicated an "interest" in cross-border online services

	Number of commuters to the Member State	Commuters per 1,000 inhabitants
Italy	11,116	0.2
Latvia	1,000	0.4
Lithuania	700	0.2
Luxembourg	127,533	255.1
Malta	425*	1.0
Netherlands	58,115	3.5
Poland	750	0.0
Portugal	4,000	0.4
Romania	1,250	0.1
Slovakia	795	0.1
Slovenia	1,100	0.6
Spain	6,000	0.1
Sweden	6,388	0.7
UK	14,700	0.2
Total	514,949	1.02 (average)

10.7.1.3 Cross-border business

Cross-border branches and immigrant business start-ups

Source: European Commission staff working document. 2010. Brussels, SEC(2010)

	Number of branches in the Member State 2009	Branches as a percentage of total enterprises 2009	Annual births from immigrants 2007
Austria	2,429	0.75%	741
Belgium	2,186	0.44%	1,370
Bulgaria	386	0.15%	12
Cyprus	223	0.44%	89
Czech Republic	3,042	0.35%	1,288
Denmark	771	0.36%	852
Estonia	477	0.93%	76
Finland	976	0.36%	390
France	6,734	0.26%	2,522

Germany	30,461	1.09%	3,386
Hungary	576	0.10%	443
Ireland	1,771	0.85%	440
Italy	6,463	0.16%	5,561
Latvia	342	0.46%	29
Lithuania	341	0.23%	252
Luxembourg	1,249	5.08%	438
Netherlands	19,067	2.73%	2,396
Poland	7,817	0.44%	1,252
Portugal	2,025	0.23%	1,191
Romania	768	0.16%	62
Slovakia	1,806	0.53%	380
Slovenia	336	0.32%	96
Spain	1,124	0.03%	5,203
Sweden	2,160	0.35%	1,081
United Kingdom	8,938	0.43%	6,668
Total	**102,470**	**0.44%**	**37,819**

10.7.1.4 The population of potential citizen and business cross-border service users

An estimate of the number of immigrants and commuters to EU Member States

Source: Immigration data from Eurostat; Commuters estimated from MKW. 2009. Scientific report. Growth between 2006/7 and 2009/10 was 13.6 per cent

	Immigration from EU Member States	Estimated commuters between EU27 Member States	EU27 Immigrants and commuters total	Cross-border total per 1,000 population
Austria	42,265	54,702	96,967	11.6
Belgium	65,611	43,972	109,583	10.2
Bulgaria	380	341	721	0.1
Cyprus	6,911	932	7,843	9.8
Czech Republic	24,477	23,574	48,051	4.6
Denmark	25,642	17,422	43,064	7.8
Estonia	2,338	1,136	3,474	2.6

	Immigration from EU Member States	Estimated commuters between EU27 Member States	EU27 Immigrants and commuters total	Cross-border total per 1,000 population
Finland	12,637	25,407	38,044	7.1
France	94,482	12,105	106,587	1.7
Germany	167,642	98,098	265,740	3.2
Greece	53,754	6,363	60,117	5.3
Hungary	15,932	16,009	31,941	3.2
Ireland	23,211	19,316	42,527	9.6
Italy	152,962	12,631	165,593	2.8
Latvia	1,476	1,136	2,612	1.2
Lithuania	3,845	795	4,640	1.4
Luxembourg	14,537	144,911	159,448	323.1
Malta	4,032	483	4,515	10.9
Netherlands	65,800	66,034	131,834	8.0
Poland	33,675	852	34,527	0.9
Portugal	17,866	4,545	22,411	2.1
Romania	2,896	1,420	4,316	0.2
Slovakia	7,552	903	8,455	1.6
Slovenia	3,201	1,250	4,451	2.2
Spain	128,246	6,818	135,064	2.9
Sweden	35,233	7,258	42,491	4.6
UK	198,624	16,703	215,327	3.5
Total	**1,205,226**	**585,115**	**1,790,341**	**3.6**

An estimate of number of EU27 branches and immigrant business start-ups in EU Member States

	Immigrant business start-ups	Number of Branches	Start-up and branches total	Cross-border business per 1,000 enterprises
Austria	741	2,429	3,171	9.8
Belgium	1,370	2,186	3,555	7.2
Bulgaria	12	386	398	1.5
Cyprus	89	223	313	6.2
Czech Republic	1,288	3,042	4,330	4.9

Denmark	852	771	1,623	7.5
Estonia	76	477	553	10.8
Finland	390	976	1,366	5.1
France	2,522	6,734	9,256	3.6
Germany	3,386	30,461	33,847	12.1
Hungary	443	576	1,019	1.8
Ireland	440	1,771	2,211	10.6
Italy	5,561	6,463	12,024	3.0
Latvia	29	342	371	5.0
Lithuania	252	341	593	4.0
Luxembourg	438	1,249	1,687	68.6
Netherlands	2,396	19,067	21,464	30.7
Poland	1,252	7,817	9,068	5.1
Portugal	1,191	2,025	3,216	3.6
Romania	62	768	830	1.7
Slovakia	380	1,806	2,186	6.4
Slovenia	96	336	432	4.1
Spain	5,203	1,124	6,328	1.9
Sweden	1,081	2,160	3,241	5.3
United Kingdom	6,668	8,938	15,606	7.5
EU MS Total	**37,819**	**102,470**	**140,288**	**6.0**

10.7.2 Uptake of online cross-border services

10.7.2.1 25 cross-border services shortlisted for further study

Citizen Services (14)

Moving and residence

Code	Service
M1	Register as domicile
M2	Request ID documents
M3	Enrol as a student
M4	Vehicle taxes payment (special declaration)
M5	Applying for a driver's licence
M6	Order a birth certificate
M7	Register a death
M8	Register real estate purchase
M9	Register for Legal Aid

Health

H1	Electronic prescriptions
H2	Access to patient summary

Employment

E1	Work permit Application
E2	Income Tax Declaration
E3	Register for a pension

Business Services (11)

Procurement

P1	Submitting a tender for public procurement

Business and start-up

B1	Register a new legal entity
B2	Corporate/business tax declaration
B3	Register for VAT
B4	Submit VAT declarations
B5	Register a new employee
B6	Pay social contributions for employees
B7	Report termination of employee(s)
B8	Register a new vehicle
B9	Register a real estate purchase
B10	Consult the business register

10.7.2.2 Ranking of the importance of services by citizens

Source: RAND, United Nations University, Maastricht University (2009) "Innovative and adaptive PEGS for citizens in 2010 and beyond: Evolution of PEGS: Impact Assessment for cross-border and Pan-European service.

Service or concern	Ranking
EU electronic identity card	1
EU standard for digital signatures	2
EU registry of available jobs and job seekers	3
EU index of health care providers	4
Services supporting portability of pensions etc:	5
eVoting, ePolling and participation services:	6
EU electronic patient record:	7
Pan-European emergency services:	8

Service or concern	Ranking
Online registration of EU wide work permits:	9
EU land and real estate registry:	10

EU's SOLVIT network: Relative importance of enquiries about citizen services

Solving 1,800 real-life problems encountered by people living, working, studying or doing business in another EU country as a result of misapplication of EU law, since 2002.

Source: RAND, United Nations University, Maastricht University (2009) "Innovative and adaptive PEGS for citizens in 2010 and beyond: Evolution of PEGS: Impact Assessment for cross-border and Pan-European service.

Service or concern	Percentage of requests
Recognition of qualifications	21
Market access for products	16
Social security	14
Taxation	11
Motor vehicle registration	7
Market access for services	6
Residence permits	5
Employment rights	4

Other general observations about the extent of cross-border matters

Source: Eurostat 2011

Gender	Cross border life choices (studying, working, living with a foreign-born spouse or purchasing a property abroad)
Female	10%
Male	16%

Source: TNS opinion

Share of EU citizens and cross-border professional or personal dimensions (studying, working, living, foregn-born spouse, abroad property)	20%

10.7.3 Uptake of online cross-border services

10.7.3.1 Use of eGovernment services

On average, 35 per cent of the European citizens were eGovernment users in 2009. Only 13 per cent of European citizens sent information electronically within 3 months prior to the survey in 2009.

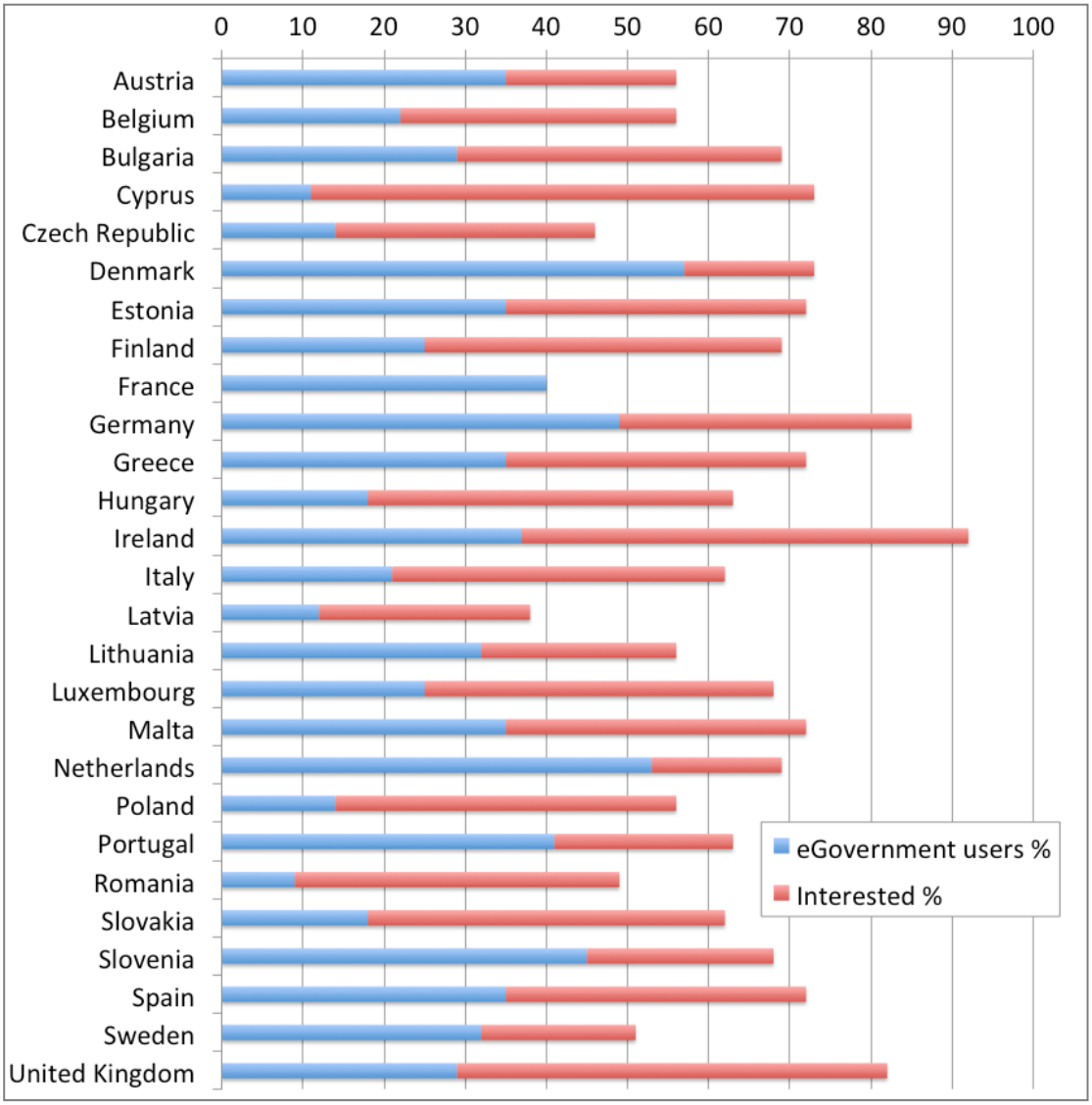


Figure 10-36: Use of Government Services

Source: Eurostat: http://epp.eurostat.ec.europa.eu/statistics_explained/index.php /E-government _statistics#Use_of_online_services_by_the_citizens

Figure 10-37: Use and interest in using eGovernment services in 2009

11 GLOSSARY

CEF	Connecting Europe Facility
CIP ICT-PSP	Community Innovation Programme, ICT Policy support Programme
DAE	Digital Agenda for Europe
EHIC	European Health Insurance Cards
eIAS	Electronic identification, authentication and signature
eID	Electronic identification
epSOS	European Patients - Smart open Services.
EU	European Union
ICT	Information and Communication Technologies
IDP	Electronic Identity Provider
LSPs	Large Scale Pilot projects
PEPPOL	Pan-European Public Procurement Online
QAA	STORK Quality Authentication Assurance: common authentication assurance levels
SMA	Single Market Act
SMEs	Small and Medium Enterprises
SPOCS	Simple Procedures Online for Cross- Border Services
TSPs	Trust Service Providers
TTP	Trusted Third Party

Glossary

Advanced Electronic Signature	"advanced electronic signature" means an electronic signature which meets the following requirements: it is uniquely linked to the signatory; it is capable of identifying the signatory; it is created using signature means that the signatory can with high level of confidence maintain under his sole control; it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable. (art. 2.2, Directive 1999/93/EC)
Authentication	An adjunct step to identification that confirms an asserted identity with a specified, or understood, level of confidence. Authentication can be used to provide high assurance that the purported identity is, in fact, the correct identity associated with the entity that provides it. The authentication mechanism can be based on something that the entity knows, has, or is (e.g., a password, smart card that uses some encryption or random number for a challenge-response scheme, or a fingerprint).
Certification	the administrative act of approving a computer system or component for use in a particular application.
Certification Authority /Certificate Authority	a specially established trusted organisation or part of a larger organisation that accepts the responsibilities of managing the certificate process by issuing, distributing, and verifying certificates.
Certified e-document delivery	The reliable and verifiable electronic delivery of data; this can be thought of as the electronic equivalent to traditional registered mail
Conversion of paper to eDocuments	Ensuring that paper documents can be converted into electronic equivalents without losing their legal validity; this can be thought of as an electronic equivalent to the paper certified copy (*copie conforme*).
Cryptographic Algorithm	A mathematical procedure, used in conjunction with a closely guarded secret key, that transforms original input into a form that is unintelligible without special knowledge of the secret information and the algorithm. Such algorithms are also the basis for digital signatures and key exchange.
Cryptography	The science and technology of keeping information secret from unauthorised parties by using a code or a cipher. Cryptography can be used for many applications that do not involve confidentiality.
Digitalisation	The process of converting information in analogue form into digital form.
Digital Certificate	An electronic device which is issued by a third party to attest to the authenticity of the issuer of a document. The combination of encryption techniques and the use of an independent third party prevents fraudulent documents from being accepted as genuine facilities secure transactions between, for example, a government agency and citizens using its services or a bank and its costumers.

Digital Signature	A digitised analogy of a written signature, produced by a cryptographic procedure acting (commonly) on a digest of the message to be signed.
eCODEX	An e-justice project to improve the cross-border access of citizens and businesses to legal means in Europe as well as to improve the interoperability between legal authorities within the EU.
Electronic Transactions	Dealings between people and organisations (such as finding out a piece of information, filling out a form, or making a payment) that take place using electronic networks.
epSOS	The main European electronic Health (eHealth) interoperability project co-funded by the European Commission and the partners. It focuses on improving medical treatment of citizens while abroad by providing health professionals with the necessary patient data.
eSeals	The equivalent to the signature of a legal person[82]; in practical terms, this can be thought of as the electronic equivalent of stamps or seals on paper documents, which are tied to a legal entity rather than to a natural person.
e-Signature / electronic signature	Stands for "electronic signature" and it's a generic term to indicate any way to electronically implement authenticity mechanisms, many often also referred as "digital signature". Basically, a digital signature is a mathematical scheme for demonstrating the authenticity of a digital message or document. A valid digital signature gives a recipient reason to believe that the message was created by a known sender, and that it was not altered in transit
e-Signature product	Any product aimed to provide e-signatures solutions
e-Signature service	Any type of activity or set activities enabling processes involved in the e-Signature scenario, for example providing certificates, delivered by appropriate organizations
e-Signature Technology Providers	Companies that build and distribute materials to support hardware and software producers and solution integrators, for example electronic components (microchips, smartcards, tokens), but also firmware/software products
e-Signature Solutions Integrators	Companies that assemble, distribute and support what provided by technology providers to create new solutions for e-Signature scenario, also managing integration issues between different technologies
Hacking	The term used to describe gaining access to private data or systems, without permission from their owner, typically using the internet.
Interaction	A two-way exchange of information or transaction.
Key	A sequence of easily changed symbols that, used with a cryptographic algorithm, provides a cryptographic process.

[82] The important feature of some documents issued by an organisation is their authenticity, i.e. that the document was genuinely produced by the organisation (ex. a certificate). Authenticity can be proven by an electronic stamp which is to a certain extent.

Long-term preservation of e-signatures	To ensure the legal validity of electronic signature over extended periods of time, ensuring that e-signatures can be validated irrespective of future technological evolutions.
Non-Repudiation (of a signed digital message, data or software)	The status achieved by employing a digital-signature procedure to affirm the identity of the signer of a digital message with extreme high confidence and, hence, to protect against a subsequent attempt to deny authenticity, whether or not there had been an initial authentication.
PEPPOL	Pan-European Public Procurement OnLine project, which aims at expanding market connectivity and interoperability between eProcurement communities. PEPPOL enables access to its standards-based IT transport infrastructure through access points, and provides services for eProcurement with standardised electronic document formats
Public Key	The publicly-known key associated with a given person's use of a public-key cryptographic system.
Public Key Infrastructure (PKI)	PKI is a set of hardware, software, people, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates. In cryptography, a PKI is an arrangement that binds public keys with respective user identities by means of a certificate authority
Private Key	The private (secret) key associated with a given person's public key for a public-key cryptographic system.
Qualified Certificate	A certificate that identifies a signatory and meets a set of appropriate legal requirements. It is commonly used for verification of secure electronic signatures
Qualified Electronic Signature	A certain "type" of electronic signature that is automatically considered by law as equivalent the handwritten signature. It is a rather complex matter because it involves a mixture of legal, technological and political issues
Secure Signature Creation Device	According to Directive 1999/93/EC, it is any tool suitable and secure to ensure the functionality of Advanced Electronic Signatures
SPOCS	SPOCS (Simple Procedures Online for Cross- Border Services) is a large-scale pilot project launched in May 2009. SPOCS aims to build the next generation of online portals (Point of Single Contact or PSC), which every European country now has in place, through the availability of high impact cross- border electronic procedures.
STORK	A competitiveness and innovation framework programme, co-funded by EU. It aims at implementing an EU wide interoperable system for recognition of eID and authentication that will enable businesses, citizens and government employees to use their national electronic identities in any Member State. It will also pilot transborder eGovernment identity services and learn from practice on how to roll out such services, and to experience what benefits and challenges an EU wide interoperability system for recognition of eID will bring.

SWOT Analysis	SWOT analysis is a strategic planning method used to evaluate the Strengths, Weaknesses, Opportunities, and Threats involved in a project or in a business venture. It involves specifying the objective of the business venture or project and identifying the internal and external factors that are favorable and unfavorable to achieve that objective. • Strengths: characteristics of the business, or project team that give it an advantage over others • Weaknesses: are characteristics that place the team at a disadvantage relative to others • Opportunities: external chances to improve performance (e.g. make greater profits) in the environment • Threats: external elements in the environment that could cause trouble for the business or project Identification of SWOTs is essential because subsequent steps in the process of planning for achievement of the selected objective may be derived from the SWOTs
Time stamping	The application of a trustworthy time reference to electronic data, so that its existence at a given point in time can be determined with certainty.
Token	When used in the context of authentication, a (usually) physical device necessary for user identification.
Trustworthiness	Assurance that a system deserves to be trusted.

12 APPENDIX – ASSUMPTION MATRIX

	Assumption	Assessment dimension	Analytical question	Evidence required/potential indicators	Main analytical method	Main sources of information
1a	**Coordinating the harmonisation of minimum requirements for cross-border eID authentication is a task for the EC**	Subsidiarity: Role of the EC in the process of cross border recognition and acceptance of eIDs	How are the roles and responsibilities divided between EC and the MS's in the process of establishing the needed minimum requirements for implementing an operational cross border eID infrastructure **Using bilateral agreements for mutual recognition will constitute a hampering factor for the deployment of the cross-border use of eIDs in the EU**	Listing all elements of the process Identifying key tasks analysing the subsidiarity as well as the reality of achieving such a system	Desk research and interviews	Main policy documents, general legal base for action on the part of the EC and intervention on specific cross-border eID issues. Experts interviews (EC and stakeholders).

	Assumption	Assessment dimension	Analytical question	Evidence required/potential indicators	Main analytical method	Main sources of information
1b	**Enforcement is a task of the EC**	Subsidiarity: Role of the EC in the process of cross border recognition and acceptance of eIDs	How are the roles and responsibilities divided between EC and the MS's ? Can the EC supervise the processes (or be responsible for the supervision) of the MS (technically and legally Is it the preferred option? What liability for the EC will arise How can recommendations and changes be enforced? Should the EC limit its action to monitoring?	Listing all elements of the process of supervision and remedy; Identifying key tasks analysing the subsidiarity issues as well as the reality of achieving such a system; What should be the characteristics and elements of monitoring?	Desk research and interviews	Main policy documents, general legal base for action on the part of the EC and intervention on specific cross-border eID issues. Experts interviews (EC and stakeholders).
2	**There is an untapped demand for cross-border services**	Dimension of demand of organisations/businesses Dimension of demand by end-users	What is the current demand? What are factors for supplying cross border	#Cross-border requests in the 'analogue world' #Cross border requests per type in the	Descriptive and analytical statistics	Demand statistics SME Panel

	Assumption	Assessment dimension	Analytical question	Evidence required/potential indicators	Main analytical method	Main sources of information
			services? Are there distinct differences between sectors/type of services? Which is the scenario for the development of cross-border eServices in the public domain Which is the scenario of private cross-border eServices	'analogue world'		Consultation
3	**Missing cross-border eID schemes are a hampering factor to cross-border services**	Role of eID in enabling cross-border services Causal link between cross-border eID and demand Other explanations for untapped demand	What are the hampering and driving factors in general? Is the lack of cross border authentication a hampering factor? Is the existence of cross border eID a driver?	Listing of driving and hampering factors;	Desk research and interviews	SME Panel Consultation
4	**There is a "chicken and egg problem": demand**	Role of eID in enabling cross-border services	Will a functioning system of cross	Listing of driving and hampering factors;	Desk research and interviews	

	Assumption	Assessment dimension	Analytical question	Evidence required/potential indicators	Main analytical method	Main sources of information
	for cross-border services depends on the availability of cross-border eID authentication and acceptance, and vice versa	Causal link between cross-border eID and demand	border authentication and acceptance of eID stimulate the supply of cross border services? If so how far?			
5	**Trust is the main factor for the adoption of cross-border eID authentication and acceptance**	Perception of causal links between factors and trust	Is a functioning cross border eID authentication and acceptance approach enhancing a trusted system? Do all MS need to be included to create the trusted system?	Stakeholder opinion (legal expert) Assessment of coordination playing field and effort for harmonisation	User opinion survey, user interview, focus group	Qualitative analysis
6a	**There are substantive organizational and legal incompatibilities in national eID schemes**	The legal requirements for national and informal eIDs where already in existence in the MS's	Do legal requirements differ, what differs and how much do they differ. Are there particular impediments to a regulation not affecting national	National MS legislations	Desk research, interviews	STORK (pilots) National legislation researched by STORK

	Assumption	Assessment dimension	Analytical question	Evidence required/potential indicators	Main analytical method	Main sources of information
			eID schemes but simply providing cross border recognition modalities?			
6b	**There are substantial technical incompatibilities in national eID schemes**	The technical requirements for formal and informal eIDs where already in existence in the MS's	Are current eID systems interoperable? To which extent is interoperability and issue?	National eID infrastructures and processes	Desk research and interviews	STORK
7	**Issuance and validation liability for MS's is a major stumbling block**	Balance between liability and minimum requirements and supervision Direct liability relationships Third party involvement and liability	Do MS's appreciate their potential liabilities and are they prepared to take them? Can liability be contracted away (to the private sector implementer)? Is the liability relationship limited to the issuing and validating party and the challenging party	Listing of potential liabilities and their causes.	Desk research and interviews	

	Assumption	Assessment dimension	Analytical question	Evidence required/potential indicators	Main analytical method	Main sources of information
			Liability should be limited to issuance of a unique identifier and to the eID validation			
8	**Different eID classes (levels) will facilitate the harmonisation process and the acceptance by the MS's**	Definition of different classes	Can different classes be used for different levels of required trust/security? Will this help overcome the differences between the MS's? Will a flat regulation be the solution for the mutual recognition issues?	Listing of key elements of eIDs	Linking elements and requirements to levels of trust/security	
9	**There is a risk of exclusion from the single market of business and individuals because of selective acceptance of eID schemes by Member States**	Assessment of potential users against the supply of public online services	Number of potential users Number of excluded users depending on national policies	End-user statistics Business/administration user statistics Interviews of end users on exclusion	Demand statistics User opinion survey, user interview, focus group	Descriptive and analytical statistics Qualitative analysis
10	**Natural and legal**	Assessment of the	Is a unique identifier	Purpose and use of	Desk research	

	Assumption	Assessment dimension	Analytical question	Evidence required/potential indicators	Main analytical method	Main sources of information
	persons can have several eIDs, but only MS's can issue a (national) unique identifier	different eID provider types	needed, and who has to issue? Can the EU issue unique identifiers?	different types of eID		
11	**Privately issued eIDs can be used in interactions with MS's public authorities.**	Assessment of the different types of privately issues eIDs, their level of requirements and their use	Can privately issued eID partially replace certain needs for nationally issued eIDs in the interaction with public authorities? If so to what level?	Listing of privately issued eIDs, the minimum requirements and their use	Desk research interviews	
11b	**The private sector is willing to use "formal eIDs" for their services**	Compatibility of formal eIDs with private-sector eServices	Are private sector eServices operators willing to accept formal eIDs? Are formal eIDs easily integrated into private eServices?			
12	**There is a potential critical mass factor when extending the "formal" eID to market**	Assessment of the deployment potential of the formal eID in sectors other than the public	Are market players willing to take up formal eID schemes? Which are the core	Requirements for acceptance Requirements for trust from private users	User opinion survey, user interviews, focus groups	Qualitative analysis

	Assumption	Assessment dimension	Analytical question	Evidence required/potential indicators	Main analytical method	Main sources of information
	uses	services and the eGovernment sector Assessment of the acceptance of formal eID schemes by market players	specifications of an eID scheme which could be acceptable for the private sector?			
13	**There will be a large scale diffusion and take up of cross-border eID in the short- and medium term**	The general demand for eIDs as an enabler for cross-border electronic transactions is growing Several public sectors are likely to adopt cross-border eID schemes The private sector is likely to adopt EC recognized eID schemes The private sector is likely to accept the assurance processes of EC recognized eID schemes	Trends in demand Adoption of formal eID schemes Trust in formal eID assurance processes	Strategies, opinions Quantitative statement of potential demand Perception of trustworthiness by decision makers	Interviews Focus groups Document analysis Survey	Qualitative analysis Descriptive and analytical statistics
14	**Formal eID schemes can provide a favourable cost/benefit ratio**	The "weight" of eID as an e-Transaction enabler in public services The weight of eIDs as an	Cost/benefit ratio Weight of the public services sector Weight of the	Costs Benefits Supply weight for market and public	Statistical review Descriptive statistical analysis	Quantitative data sources A few interviews

Assumption	Assessment dimension	Analytical question	Evidence required/potential indicators	Main analytical method	Main sources of information
	enabler in market-related services Cost calculation of formal eID schemes Monetary benefit estimation	market eID sector Which are possible cost schemes for eIDs How can the benefits be expressed in monetary terms	sectors Benefit monetisation	Qualitative analysis	

13 APPENDIX – EXPLORATORY QUESTIONS

This is the full set of exploratory questions used in the different investigations.

Since several questions address the quantitative issue of the demand to eIDs and of services which relate to them, they will all be integrated to respond to Assumption 2 and Assumption 4.

Issue	Main exploratory question	Assumption	Policy option affected	analysis target
On-going actions on mutual recognition	Is there an autonomous regulation of mutual recognition between Member States (dynamic) - Which are the cross-border eID regulatory initiatives of MSs? - Are there any market-led initiatives? - Which is their sustainability? - Which number of MS is involved? - Which is the Pace of developments and likely breakthroughs - Which is the diffusion of autonomous mutual recognition - Which is the degree of dependence on EU policy (DAE, eGov action plan)? - Which is the degree of dependence on the evolution and support and results of large scale pilot projects? - Will initiatives on cross-border recognition stop	1a	Mainly "no action" or "status quo"	- Member States (STORK consortium)

Issue	Main exploratory question	Assumption	Policy option affected	analysis target
	should any EU initiative on eID be halted?			
Current mutual recognition agreements	Are there currently mutual recognition agreements in existence (static) - How many? - Which MS do they involve? - Are they sustainable?	1a	Mainly "no action" or "status quo"	- Member States (STORK consortium)
"Soft" measures	- How can "soft" instruments be used to support the autonomous action of MS? - Which are these "soft" instruments (T. Hooghiemstra)	1a, 1b	Mainly "no action" or "status quo"	- Experts in the team of IISA
Current national eID and eAUTH systems and the impact at EU level	- How do you rate the performance of current national eID systems, as designed or implemented in different Member States? - To what extent it is possible to infer conclusions on the establishment and operation of mutual recognition and acceptance of eIDs at EU level? - Which are the obstacles to the deployment of formal eID measures at national level? - Do the potentialities justify a major effort to overcome these obstacles?	4, 6a, 6b	Mainly "no action" or "status quo"	
Issues for cross-border mutual recognition and acceptance of formal eIDs	- Under which conditions would you (Member State, Private Institution, Stakeholder) be prepared to recognise formal eIDs issued in another Member State? - Do we need a supervisory body, in charge of: (a) setting minimum standards; (b) setting	1b, 5, 6a, 6b, 7, 10,	Option B (B1, B2, B3) Cross-border legislation	- Member States (STORK consortium)

Issue	Main exploratory question	Assumption	Policy option affected	analysis target
	interoperability rules; (c) intervening in dispute resolution? - **Shall Natural and legal persons have several eIDs, but only MS's be allowed to issue a (national) unique identifier?** - **Will different eID classes (levels) facilitate the harmonisation process and the acceptance by the MS's** - Are there substantive **organizational and legal incompatibilities in national eID implementations?** - **Are there substantive technical incompatibilities in national eID schemes**			
National regulations on the use of eIDs	- Do national eID regulations allow the use of formal eIDs in private sector transactions, opening up eAuthentication systems to non-governmental players?	6a, 6b	Option B (B1, B2, B3) Cross-border legislation	- Experts in the team of IISA - Member States (STORK consortium)
National rules on paper eIDs and for foreign citizens	- What are the rules which enable citizens of other Member States to receive your "national" ID card? - Which are the conditions for foreign citizens to obtain "national" eIDs? (the relevant regulatory provisions)	6a, 6b	Option B (B1, B2, B3) Cross-border legislation	- Experts in the team of IISA - Member States (STORK consortium)
Cross-border Interoperability	- Which are the EU-level interoperability requirements deemed necessary to ensure the	6a, 6b	Option B (B1, B2, B3) Cross-border	- Experts in the team of

Issue	Main exploratory question	Assumption	Policy option affected	analysis target
requirements	cross-border operations of eID? - What are the key elements of EU-level governance of eID systems? Is a EU-level governance body necessary? - Will encouraging standardization support cross-border eID schemes?		legislation	IISA - Member States (STORK consortium)
Liability Issues	- Which are the liability issues related to the delivery of cross-border public eServices in respect to the potential immaterial and monetary damage due to the breach of the concerned eID system? [here we might want to look at different services and assess the associated risks and liabilities. Then we can ask for an assessment of the risk/liability issue in each specific case]	7	Option B (B1, B2, B3) Cross-border legislation	- Experts in the team of IISA - Member States (STORK consortium)
Trust conditions in cross-border eID management	- Which are the conditions of trust in cross-border eID management? - How do you assess the different eID "classes" of eIDs and the associates levels of strength? - How do you assess the issue of the security of eAuthentication technological systems in other Member States? - Are you prepared to trust these systems? - Which are the conditions for trust? - Would you envisage a sort of security classification of "foreign" eAuthentication systems and should an independent party be involved?	8	Option B (B1, B2, B3) Cross-border legislation	- Experts in the team of IISA - Member States (STORK consortium)
	- Which are the minimum provisions for each MS to	5	Option B (B1, B2, B3)	- Experts in

Issue	Main exploratory question	Assumption	Policy option affected	analysis target
	recognise formal eIDs issues in another MS? [here we need to build a catalogue and ask for ranking and assessment, considering the "eID and eAuthentication systems" and their functional and security issues]		Cross-border legislation	the team of IISA - Member States (STORK consortium)
	- Is it realistic to "oblige" MSs to accept eIDs and eAuthentication from other Member States?	1a	Option B (B1, B2, B3) Cross-border legislation	- EC
Cost models of current national eIDs	- Which are the cost models of current national eID systems? Considering investment, update, interoperability, security and current operating costs? - How are the costs recovered (payment by citizens)? Which are the additional costs for the cross-border use of eIDs? - Shall there be a pay-per-use, or just issuance cost recovery?	12, 13, 14	Option B (B1, B2, B3) Cross-border legislation	- Experts in the team of IISA - Member States (STORK consortium)
EU-level adoption of national eID and eAUTH rules	- Which are the current legal provisions and existing agreements concerning eID and eAuthentication which can be taken up in a forthcoming cross-border legislation?	6a, 6b	Option B (B1, B2, B3) Cross-border legislation	- Experts in the team of IISA - EC

Issue	Main exploratory question	Assumption	Policy option affected	analysis target
The landscape of available cross-border services based on eID	- Which is the number and type of cross-border services available and potentially available (demand) [seek for some forecast scenario, trying to make out how eID-based services will evolve]? - Is an immediate necessary or would a gradual implementation be feasible? Would a gradual implementation lead to disparities among Member States and discriminate citizens? - To which extent will the development of cross-border eServices dependent on EU policies? - Are cross-border services dependent on mutually recognised eIDs? [is the absence a barrier?] - What are the likely trends in development of cross-border eServices dependent on eIDs (demand)? - Which eGovernment services are hampered by the absence of mutually recognised eIDs? - Which private-sector cross-border services are hampered by the absence of mutually recognised eIDs? - Do we need formal eIDs for the development of cross-border eGovernment services? - Do we need formal eIDs for the development of cross-border private eServices	2, 3, 4	Option B (B1, B2, B3) Cross-border legislation	- Experts in the team of IISA - Member States (STORK consortium)
The benefits of eIDs	- Which are the benefits for citizens and businesses deriving from the use of formal eIDs? - Immaterial benefits, monetary benefits?	12, 13, 14	Option B (B1, B2, B3) Cross-border legislation	- Experts in the team of IISA - Member States

Issue	Main exploratory question	Assumption	Policy option affected	analysis target
				(STORK consortium)
The private sector and formal eIDs	- Are private-sector entities inclined to use the formal eID? - Which are the trade-offs to use custom developed eID and eAuthentication systems rather than formal eIDs? - Which is the potential demand of private-sector entities for formal eIDs? [volume estimation and the associated cost] - Shall privately-issued eIDs be used in interactions with MS' public institutions? - Is there a potential critical mass factor when extending the formal eID to market uses?	11, 11b, 12	Option B (B1, B2, B3) Cross-border legislation	- Experts in the team of IISA - Private sector (STORK consortium)
Technical aspects	- Are technical aspects relevant for mutual recognition? Shall the interoperability issue be addressed? - Is the acceptance of cross-border eIDs dependent on any security assurance of eAuthentication systems?	6b, 7, 8,	Option B (B1, B2, B3) Cross-border legislation	- Private sector (STORK consortium)

14 APPENDIX – CROSS-BORDER USE OF EID: QUESTIONS FOR THE LSP'S

Pilot	Services	Initial demand & trends	Barriers	Potential uptake & benefits	General
STORK	SaferChat	*Does this service need cross-border formal eID?* *Who needs it, how many transactions?* *What are the trends in the use of eID to promote this service? Are you preparing to develop your own solution for the cross-border eID requirement if a general EU solution does not come available?* *Who will pay for the availability of cross-border eID?*	*Do you see legal/ organizational/* *technological issues relating to use of formal cross-border eID?* *What is the effect of non-regulation (no legal framework on cross-border eID) on the provision of this service? Will it be discontinued? STORK: What financing model for the interoperability infrastructure would be feasible (budget funding, end-user pays)?*	*How big do you think the potential uptake of formal cross-border eID for this service could become? (# of transactions, etc.)* *What would be the estimates on impact on the administrative burden: cost savings due to simplification, liability costs?*	*Discuss the different policy options: what do you think of it?* *STORK: How high do you estimate that the implementation costs (at the EU level and Member State level) of a mutually recognized eID framework would be?* *STORK: How high would the operational costs be (at the EU level and Member State level) compared to this?*
	Student mobility	,,	,,	,,	,,
	Change of address	,,	,,	,,	,,
	STORK-ECAS integration	,,	,,	,,	,,
	eDelivery	,,	,,	,,	,,
	Cross-border eGovernment services pilot	,,	,,	,,	,,
PEPPOL	eOrders	,,	,,	,,	,,
	eInvoices	,,	,,	,,	,,
SPOCS	points of single contact 2.0	,,	,,	,,	,,
	electronic documents	,,	,,	,,	,,
EPSOS	…	,,	,,	,,	,,
ECODEX	…	,,	,,	,,	,,

15 APPENDIX – REFERENCES

Studies

- "Digital Internal Market", by FPS Rechtsanwälte und Notare, for the European Parliament, IMCO Committee, 2011, www.europarl.europa.eu/document/activities/cont/201106/20110615ATT21451/20110615ATT21451EN.pdf, last accessed on 25/06/2012
- "Digitizing Public Services in Europe: Putting ambition into action" (9th eGovernment Benchmark Measurement), by Capgemini, IDC, Rand Europe, Sogeti and DTI, for the European Commission, DG InfSo, 2010, http://ec.europa.eu/information_society/newsroom/cf/document.cfm?action=display&doc_id=747, last accessed on 25/06/2012
- "European Cross-border E-commerce: The Challenge of Achieving Profitable Growth", by Accenture, 2012, www.accenture.com/SiteCollectionDocuments/PDF/Accenture-ERRT-Brochure.pdf#zoom=50, last accessed on 25/06/2012
- "Identification and analysis of 10 cross-border eID services, obstacles for further development, and assessment of their socio-economic and cross-sectoral impacts", Draft Final Report of 4 April 2011, European Commission, JRC-IPTS, 2011
- "Electronic Signatures as Obstacle for Cross-Border E-Procurement in Europe: Lessons from the PROCURE-project", by Institut für Informationsmanagement Bremen GmbH (ifib), 2009, www.ifib.de/publikationsdateien/2009-06-15_eSig_article_final_ePractice.pdf, last accessed on 25/06/2012
- "Smarter, Faster, Better eGovernment" (8th eGovernment Benchmark Measurement), by Capgemini, Rand Europe, IDC, Sogeti and DTI, for the European Commission, DG InfSo, 2009, http://ec.europa.eu/information_society/eeurope/i2010/docs/benchmarking/egov_benchmark_2009.pdf, last accessed on 25/06/2012
- "Study of Gambling Services in the Internal Market of the European Union", by Swiss Institute of Comparative Law, for the European Commission, 2006, http://ec.europa.eu/internal_market/services/docs/gambling/study1_en.pdf, last accessed on 25/06/2012
- "Study on Analysis of the Needs for Cross-Border Services and Assessment of the Organisational, Legal, Technical and Semantic Barriers" (SMART 2011/0074), Draft Final Report, by Capgemini, tech4i², time.lex, Universiteit Antwerpen, 2012
- "Study on cross-border Interoperability of eSignatures" (CROBIES), by SEALED, time.lex and Siemens, for the European Commission, DG InfSo, 2010, http://ec.europa.eu/information_society/policy/esignature/docs/crobies_deliverables/crobiesdo.pdf, last accessed on 25/06/2012
- "Study on eID Interoperability for PEGS", by time.lex and Siemens, for the IDABC programme, 2010, http://ec.europa.eu/idabc/servlets/Doc2ba1.pdf?id=32521, last accessed on 25/06/2012
- "The Impact of ICT on Employment", by Humboldt-Innovation GmbH, for the European Commission, DG InfSo, 2010, http://ec.europa.eu/information_society/eeurope/i2010/docs/benchmarking/impact_ict_on_employment.pdf, last accessed on 25/06/2012
- "The Role of Digital Identity Management in the Internet Economy: A Primer for Policy Makers", by Katarina de Brisis of Norway et al., for the OECD, 2009, www.oecd-ilibrary.org/the-role-of-digital-identity-management-in-the-internet-economy_5ksdxhgl22vk.pdf;jsessionid=18hlxtgxll042.delta?contentType=/ns/WorkingPaper&itemId=/content/workingpaper/222134375767&containerItemId=/content/workingpaperseries/20716826&accessItemIds=&mimeType=application/pdf, last accessed on 25/06/2012

- "The State of the Electronic Identity Market: Technologies, Infrastructure, Services and Policies", European Commission, JRC-IPTS, 2010, http://ftp.jrc.es/EURdoc/JRC60959.pdf, last accessed on 25/06/2012
- "The User Challenge: Benchmarking the Supply of Online Public Services" (7th eGovernment Benchmark Measurement), by Capgemini, for the European Commission, DG InfSo, 2007, http://ec.europa.eu/information_society/eeurope/i2010/docs/benchmarking/egov_benchmark_2007.pdf, last accessed on 25/06/2012
- "Towards a Trusted and Sustainable European Federated eID system", by Cristof Fleurus et al., for the European Commission, DG InfSo, 2011, http://ec.europa.eu/information_society/activities/egovernment/docs/studies/sustainabilitystudyeuropeaneidplatform-smart2010-0068.pdf, last accessed on 25/06/2012

Survey reports

- "Attitudes on Data Protection and Electronic Identity in the European Union", Special Eurobarometer 359 , 2010, http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf, last accessed on 25/06/2012
- "Attitudes towards cross-border trade and consumer protection", Flash Eurobarometer 299a, 2011, http://ec.europa.eu/public_opinion/flash/fl_299a_en.pdf, last accessed on 25/06/2012
- "Consumer attitudes towards cross-border trade and consumer protection", Flash Eurobarometer 299, 2010, http://ec.europa.eu/public_opinion/flash/fl_299_sum_en.pdf, last accessed on 25/06/2012
- "Consumer protection in the internal market", Special Eurobarometer 298, 2008, http://ec.europa.eu/public_opinion/archives/ebs/ebs_298_en.pdf, last accessed on 25/06/2012
- "Consumer protection in the internal market", Special Eurobarometer 252, 2006, http://ec.europa.eu/public_opinion/archives/ebs/ebs252_en.pdf, last accessed on 25/06/2012
- "Cross-border Public Procurement", European Business Test Panel, 2011, http://ec.europa.eu/yourvoice/ebtp/consultations/2011/cross-border-public-procurement/index_en.htm, last accessed on 25/06/2012
- "Digital Agenda Scoreboard", European Commission Staff Working Paper, 2011, http://ec.europa.eu/information_society/digital-agenda/scoreboard/docs/scoreboard.pdf, last accessed on 25/06/2012
- "Retailers' attitudes towards cross-border trade and consumer protection", Eurobarometer 300, 2010, http://ec.europa.eu/public_opinion/flash/fl_300_en.pdf, last accessed on 25/06/2012
- "SSEDIC Deliverable Report D.2.3.1: YEAR 1 eID adoption survey", by is-practice, 2011, http://www.eid-ssedic.eu/images/stories/pdf/SSEDIC%20D2.3.1%20eID%20Adoption%20Survey%20Y1%20v1.1.pdf, last accessed on 25/06/2012

Research briefings, press releases etc.

- "Computer skills in the EU27 in figures", Eurostat news release, 26/03/2012, http://epp.eurostat.ec.europa.eu/cache/ITY_PUBLIC/4-26032012-AP/EN/4-26032012-AP-EN.PDF, last accessed on 28/05/2012
- "eIDs in Europe: Not (yet) yielding profits for the cross-border financial services sector", 07/09/2010, http://www.dbresearch.com/PROD/DBR_INTERNET_EN-PROD/PROD0000000000262236.pdf, last accessed on 28/05/2012
- "E-Skills Week 2012: Computer skills in the EU27 in figures", Eurostat news release, 26/03/2012, http://europa.eu/rapid/pressReleasesAction.do?reference=STAT/12/47, last accessed on 28/05/2012

- "ICT usage in enterprises 2010", Eurostat *Data in focus*, no. 49/2010, http://epp.eurostat.ec.europa.eu/cache/ITY_OFFPUB/KS-QA-10-049/EN/KS-QA-10-049-EN.PDF, last accessed on 28/05/2012
- "Internet usage in 2010 – Households and Individuals", Eurostat *Data in focus*, no. 50/2010, http://epp.eurostat.ec.europa.eu/cache/ITY_OFFPUB/KS-QA-10-050/EN/KS-QA-10-050-EN.PDF, last accessed on 28/05/2012
- "OpenID 2009 Year in Review", OpenID, http://openid.net/2009/12/16/openid-2009-year-in-review, last accessed on 28/05/2012

Databases

- Eurostat data, http://epp.eurostat.ec.europa.eu