PBLQ

for a strong public sector

International Comparison eID Means

Report

International Comparison eID Means

Final report

DISCLAIMER
This study was commissioned by the Dutch Ministry of the Interior and Kingdom Relations. The authors are accountable for the content of this study. The content does not necessarily reflect the point of view of the Ministry of the Interior and Kingdom Relations.

project 004599
version 1.0
date 10 April 2015

Table of contents

Preface

Both in the European Union and in the Netherlands, electronic identification (eID) is a ‘hot topic’. Whether to support the European Digital Single Market or the Dutch policy ambitions for full electronic service delivery in 2017, eID is a key enabler. The ‘electronic identification and trust services for electronic transactions in the internal market’ (eIDAS) Regulation, adopted last year, underlines this importance.

This report is the result of a study to discover the policy considerations in the European Union Member States for shaping a national eID scheme for electronic government services through public, private or both of those means. The study was conducted for the Dutch Ministry of the Interior and Kingdom Relations, which holds the coordinating responsibility for eGovernment and citizen identification in the Netherlands.

During the process of identifying the best way to implement an eID means for citizens with a high level of assurance, the Dutch Ministry of the Interior and Kingdom Relations commissioned a number of studies. One of those is represented by this document. The report, in Dutch, is used to support the decision-making process.

For this study, a number of national experts from different EU Member States were interviewed. It became clear that the angle and scope of the research was of interest to them, and they requested to be informed about the findings. Following this interest in the study, the Dutch Ministry of the Interior and Kingdom Relations commissioned an English version of the report to share the findings with the European eID community.

Through this report, the Dutch Ministry of the Interior and Kingdom Relations wishes to contribute to a deeper understanding of the solutions implemented and to inspire new ways of thinking, guaranteeing the success of national eID schemes and their cross-border exchange.

PBLQ and the authors in particular are grateful for the opportunity to offer their work to a wider community.

Nathan Ducastel
PBLQ management team member

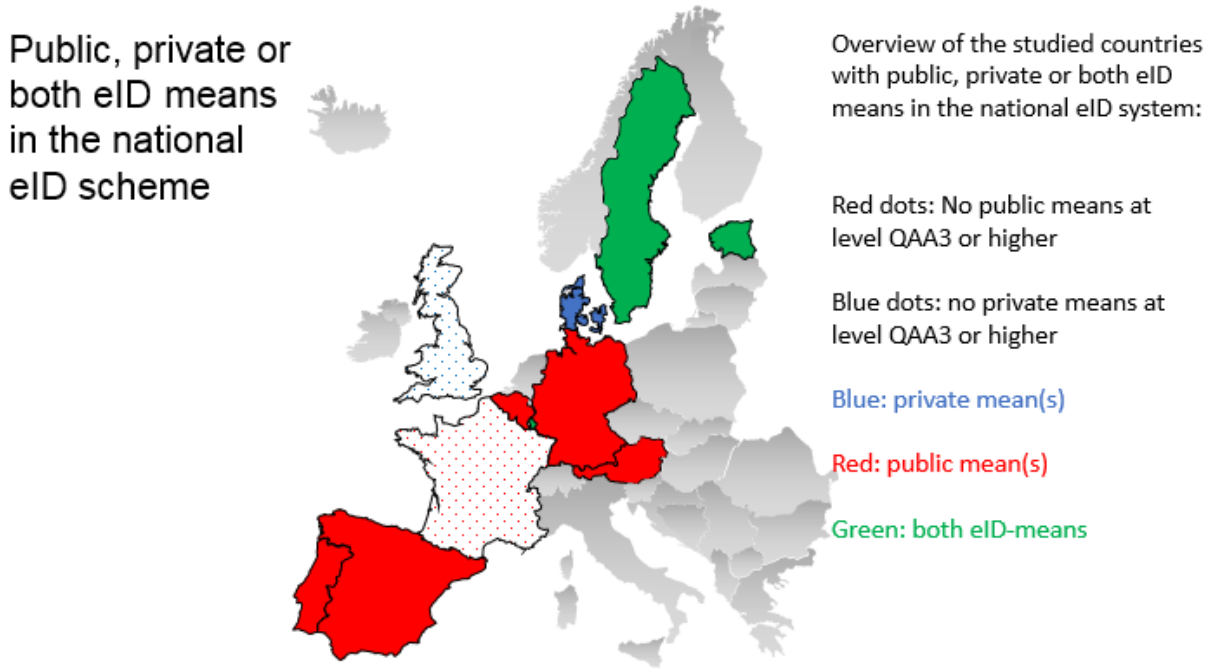
Executive summary

On behalf of the Dutch Ministry of the Interior and Kingdom Relations, an exploration regarding electronic identity (eID) means in other EU Member States has been conducted. During the production of this report, several of the international interviewees expressed their interest in the findings of the report. Hence, this edited English version to inform the eID community.

The report is part of the Dutch decision-making process regarding the possibilities for a public eID means with a high level of assurance for citizens in the Netherlands. As part of the decision-making process, the Ministry of the Interior and Kingdom Relations commissioned a study describing the situation regarding eID solutions and eID means in other Member States, and the policy arguments behind those solutions. This report therefore describes the factual situation in several countries and draws factual conclusions. The report does not provide recommendations for the Dutch situation.

The central question was: '*Describe whether public and/or private eID means are used in the different [EU] Member States for online access to at least government services. Elaborate the policy arguments on the basis of which this solution developed'.*

After a quick initial scan, eleven countries with a clear division in their choice of public and/or private eID means were selected and studied. The following figure shows the type of eID means used.



The range of eID means that are used in national eID schemes in different countries is broad: from private to public. It is difficult to classify the eID means in the category of private or public. This classification depends on national definitions and beliefs.

In fact, there appears to be a continuum. The continuum ranges from public coordination of *eID schemes* to private production of the actual *eID means*. All countries share these extremes: the eID scheme is set by the government and the actual production of the eID means is done by the private sector. However, countries differ in their precise location on this continuum.

The study shows that the cultural and historical contexts, as well as the administrative culture that is based on these contexts, are of great importance for the choice of public, private or both eID means in the national eID scheme. The eGovernment ambitions of the Member State and the moment that the eID means was introduced seem to be of importance. All countries consider similar policy-related aspects such as ‘availability’, ‘accessibility’, ‘privacy’, ‘security’ and ‘ease of use’, but they come to different conclusions on the basis of similar values to these aspects.

Public-private sector competition regarding eID means in the national eID scheme is not, or hardly, recognized. None of the countries have indicated serious discussions between the government and the private sector, or at the political level, regarding the choice of a public, e.g., private eID means in the national eID scheme.

With regard to the market for high-level reliable eID means for eGovernment use, the picture that emerges in a number of countries is that the market is not mature enough to support authentication to government services by itself. A stimulus from the government is needed.

Use of eID and ease of use of eID means are of major importance for all countries. This triggers the innovation of many eID means, e.g., contactless eID means or mobile ID. Other countries are investigating different levels of assurance, including username-password solutions with a lower assurance level, as compared to the eID card systems.

In some eID schemes where private eID means were used, such as Estonia, Luxembourg, Spain and Sweden, a public means was introduced later. This is often coupled with the renewal of the national (e)ID card. These decisions were made from the point of view of wide availability to and inclusion of all citizens.

Aspects such as the use of a national register or a national personal identification number (PIN) and the issue of a possible single point of failure (SPF) do not have a decisive influence on which eID means to introduce in the eID scheme.

1. Developing eID

Striving to continuously improve public service delivery and stimulate the digital economy, Europe and the Netherlands have put an emphasis on, and given priority to, realizing electronic identities for citizens and businesses alike. These developments form the context in which this study must be read and underline the importance of a successful eID scheme.

In the Netherlands, the question has arisen whether an eID means or solutions with high levels of assurance for citizens should be implemented through the private sector or the government. This study was conducted to provide input for this discussion.

1.1 eID in the Netherlands

The Netherlands is working on a national eID scheme[1] to realise its policy goal of full electronic public service delivery for citizens and businesses in 2017, as well as to support transactions in the private sector. This is part of the 'Digiprogramme', delivering on the generic base infrastructure needed for the effort to improve service delivery to citizens while at the same time making governmental operation more effective and efficient. The Digiprogramme is the result of a National Coordinator for Digital Government under the prime minister, appointed last year (2014).

One of the four cornerstones for this infrastructure is electronic identification. The current national eID means/scheme for citizens (DigiD[2]) and businesses (eRecognition[3]) will be brought together in one scheme, based on public-private partnerships. At the same time, a solution is sought to enable citizens to authenticate with a high assurance level/highly reliable eID[4], in addition to the current eID means for citizens, which operates at a lower level and which is highly successful in terms of use.

The Netherlands is considering not only the inclusion of eID means for citizens on existing carriers, such as the citizen card or driving licence, but also private means such as business means and the bank card. This study is part of a trajectory aimed at making an internationally inspired inventory of policy considerations to choose either public, private or both eID means with a high level of assurance, to be included in the national eID scheme, giving access to, at least, public services.

---

[1] Stelsel eID - http://www.eid-stelsel.nl/snelbuttons/english/
[2] For more information, see: https://www.digid.nl/index.php?id=1&L=1
[3] For more information, see: https://www.eherkenning.nl/eRecognition
[4] At the time of the study this was defined as Quality Authentication Assurance (QAA) level 3 or 4 as adopted and further developed in the Secure Identities Across Borders Linked (STORK) large-scale pilot. Currently, in the discussions for the implementing act(s) of the eIDAS Regulation (EU) N° 910/2014, three levels are discussed: high, substantial and low, based on ISO 29115 and STORK. In this study, the STORK QAA levels are still referred to.

In the Netherlands, the issue of implementing a public or private eID means for citizens at STORK QAA level 3 or 4 in the eID scheme is particularly relevant. The Netherlands has legislation (Law Market and Government) regulating the relationship between the private sector and the government for the delivery of products and services.

The general gist of the legislation is that the government does not compete on an unequal footing with the private sector when offering services and products to the market. At the core are four rules for the government: (1) base the pricing policy on integral costs; (2) create a level playing field (no preferred suppliers); (3) do not use data unavailable to competitors; and (4) ensure the separation of positions. This law appears to be unique in Europe, but presents important points for discussion in the Netherlands.

1.2 eID in Europe

The Digital Single Market is one of the main priorities of the European Commission. It contributes considerably to economic resilience and growth. For the Digital Single Market (including commercial and administrative free space for services) to be successful, electronic identification and guarantees regarding privacy are essential. Citizens and businesses need to trust that their data are treated in full respect of existing data protection legislation. Secure electronic identification (eID) is an important enabler of service delivery, data protection and the prevention of online fraud.

Electronic identification has to enable secure cross-border electronic transactions. A strategy has been chosen to ensure the possible use of national eID schemes across borders. However, there is a lack of interoperability and common legal basis engaging each Member State to recognise and accept eIDs issued in other Member States. The insufficient cross-border interoperability of national eIDs prevents citizens and businesses from benefitting fully from the Digital Single Market. This situation is rapidly changing.

The STORK large-scale pilot project was introduced in 2008 and was succeeded by the STORK 2.0 project (running until 2015), which further develops the work, expanding towards legal identities and attributes. STORK is a programme of the Member States, co-funded by the EU. STORK developed a system for an EU-wide interoperable system for mutual recognition of national eIDs that enables businesses, citizens and government employees to use their national electronic identities in any EU Member State.

The eIDAS Regulation on electronic identification and trust services for electronic transactions in the internal market (adopted on 23 July 2014) guarantees the legal basis for cross-border mutual recognition of eIDs. The eIDAS Regulation strives to increase the effectiveness of public and private online services and of eBusiness and eCommerce in the EU. Currently, the EU and the Member States are working on the implementation. While the implementing acts consider three levels of assurance, in this study the STORK QAA levels are still referred to.

2. Researching eID means

This chapter describes the research question and methodology. It also gives a rough outline of aspects of eID means that are relevant for the study.

2.1 Research question: Public or private eID means?

'Describe whether public and/or private eID means are used in the different [EU] Member States for online access to at least government services. Elaborate the policy arguments on the basis of which this solution developed'.

The document 'Afwegingskader publieke diensten in het eID-stelsel NL' (Consideration framework for public services in the Dutch eID scheme) provided guidance for policy arguments. It lists accessibility, availability, competition sensitivity, efficiency and safety as aspects to be reckoned with. The judicial aspects are legal identification duty, personal data protection, personal identification number (PIN) and competition.

In order to have a common understanding of the content of this report, it is important to set definitions and make a distinction between the national eID scheme and the eID means.

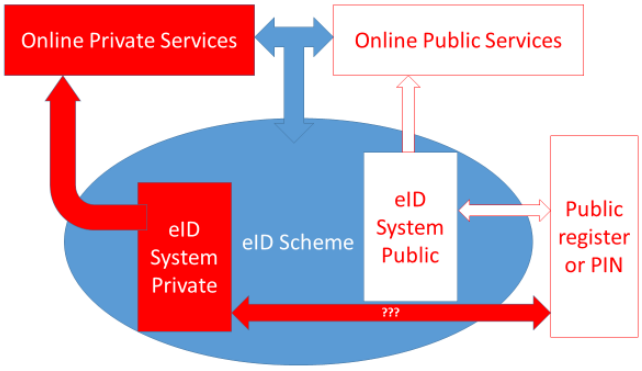
The national eID scheme is defined as the set of laws, standards, supervision and facilities that can contain one or more eID means (and their systems) and are acknowledged as a national facility by the corresponding country.

An eID means is a system that is necessary to offer validated access to an electronic service. This means can either be public or private and can function within or outside an eID scheme. The study limits itself to eID means recognized in the national eID schemes, unless mentioned differently.

Public eID means are means that are produced, implemented and maintained under the direct supervision of the government and for which the responsible political minister is held accountable.

Private eID means are those that are produced, implemented and maintained under the direct supervision of the private sector. When these means are used to access public services, political responsibility is still in place. But when private eID means provide access to only private services, this is not the case.

The following figure provides a schematic visualization of the different, essential elements of this study. The study included the extent to which the use of national public numbers and records is permitted for private eID means and whether this has an effect on the choice of 'architecture'.



The study considers that different countries choose a different architecture for their eID schemes. Some countries choose public eID means; others, private eID means; and some others, a mixed system that hosts both. The figure above should be seen as hosting authentications via the eID scheme (blue), as well as direct services, via the red or white arrows.

To investigate the research question, generation of basic data, if available, regarding several important aspects of the national eID means and schemes took place. These data include:

Aspect	**Explanation**
Use	If available, this is about the level of penetration (use of means) and the real level of use (number of transactions).
Financial arrangements	Which financing constructions have been observed and how much money was spent on the eID means?
Private actors in the realization of an eID means	Were there any private actors involved in the realization, even if the solution is designated as a public eID means?
Private use of citizen registration/PIN	Are parties that are realizing a private eID means allowed to make use of the national citizen registration and/or the PIN?
Incidents	Have any incidents taken place that led to discussion in national parliament?
Mandatory open source software	Are there any open source software criteria used by private suppliers of the means?
Single point of failure	Has there been any discussion regarding ‘single point of failure’ problems and did it have any consequences for the design of, and the means in, the eID scheme?

2.2 Approach and scope

The research includes a desk study and semi-structured interviews with eID experts from selected EU Member States (MS). Attachment B holds the questionnaire that was shared with the experts before the meetings, and was the guideline for the semi-structured interviews. For meeting the experts and holding the interviews, grateful use has been made of an eIDAS meeting in Brussels, September 2014, bringing together many of the MS experts.

Starting from a quick scan of all Member States, a selection of Member States was made, aiming at maximizing diversity in the different varieties of public and/or private eID means in the national eID scheme, and including both smaller and larger Member States. See attachment C for more details.
The research and report does not include policy recommendations (for the Netherlands or the EU). It strives to describe the factual situation regarding eID means in national eID schemes for citizens and considerations in EU Member States, and comes to factual observations and conclusions.

Many studies regarding eID in Europe are already available. These studies describe the functioning and dependencies of national eID schemes in-depth. Many of these studies have been gratefully used for this report (see attachment A). The report wishes to be brief and concise within the available time frame. The research scope therefore explicitly focuses on the policy arguments and excludes, amongst others:

- A (technical) description of national eID schemes and eID means;
- A detailed description of the valid legal provisions in each country;
- Authentication of companies; and
- Electronic signatures.

2.3 On electronic identification means

Without moving into a technical description of eID means, it is important to outline and describe several important aspects of eID means to support and understand the conclusions of this research. In the following order, this paragraph discusses: a rough classification of different eID means, assurance of eID means and several aspects of the production of eID means.

2.3.1 Different types of eID

Electronic identification means come in different shapes. Roughly, the following types of eID means, relevant to this study, are available:

- Username-password;
- Username-password with text message verification;
- Software-based (public key infrastructure (PKI)) certificates;
- Smartcards with contact (card reader is necessary) or contactless chips (the card is equipped with a transmitter that makes the chip readable at a distance) on which a certificate is placed; or
- Mobile ID (by which the mobile phone or a combination of mobile phone and contactless smartcard is used for a higher level of authentication).

The concept eID card is mentioned frequently in the study. It refers to a national identity card, either mandatory or non-mandatory, that is used to add an eID functionality (by means of a certificate). Whenever the concept ‘(e)ID card’ is mentioned in this study, it refers to a public national identity card that also offers an eID functionality.

2.3.2 Assurance

The assurance of eID means depends not only on the means itself but also on the issuing process. The STORK project created Quality Authentication Assurance (QAA) levels. These QAA levels offer the possibility

of categorizing eID means based on assurance; the levels indicate the assurance by which someone's identity is determined and attach a value to the authentication. Level 4 is most reliable, and level 1 is least reliable. A high-level eID refers to a means that guarantees assurance at QAA levels 3 and 4.

Currently, in the discussions for the implementing act(s) of the eIDAS Regulation (EU) N° 910/2014, three levels of assurance are discussed: high, substantial and low, based on ISO 29115 and STORK. In this study, the STORK QAA levels are still referred to.

Regarding assurance
'For the architecture of the levels, we will look at organisational as well as technical factors. For organisational factors, we look at the identification procedure, the issuing process of identity tokens (e.g., with passwords, but also cards that include chips) and the quality of the certified authority. For the technical aspects, we mainly look at the type and the robustness of the identity token and the quality of the mechanism that is used for user authentication. Each of these factors will be valued and the weakest factor will decide the level of the authentication means.'[5]

2.3.3 Process

The process for production and use of a high-level means, assuming a certificate on a smartcard, roughly contains the following steps:

- Production of the card and chip;
- Production of the certificate;
- Personalization of the chip on the card with a certificate;
- Issuance of the smartcard;
- Activation and reactivation of the certificate (in case the card is valid longer than the certificate);
- Validation of the card against a validation register;
- Renewal of certificates (in case the card is valid longer than the certificate); and
- Supervision of the eID scheme and eID means.

It is important to recognize that production, implementation and use processes can be implemented by different public and private actors.

[5] Memo Forum Standardization FS22-10-07, concerning: 'Indeling van authenticatiemiddelen' (categorization of eID means), 25 September 2009.

3. Sketching the eID-means landscape

Following the central research question and the additional questions introduced in chapter two, this chapter describes the country selection (par 3.1), the state of affairs regarding private and/or public eID means and the policy arguments leading to these realities (par 3.2), and finally an overview of the state of affairs regarding a number of aspects that were discussed to assess policy arguments (par 3.3), the aim being to give indications, not precise figures or arguments.

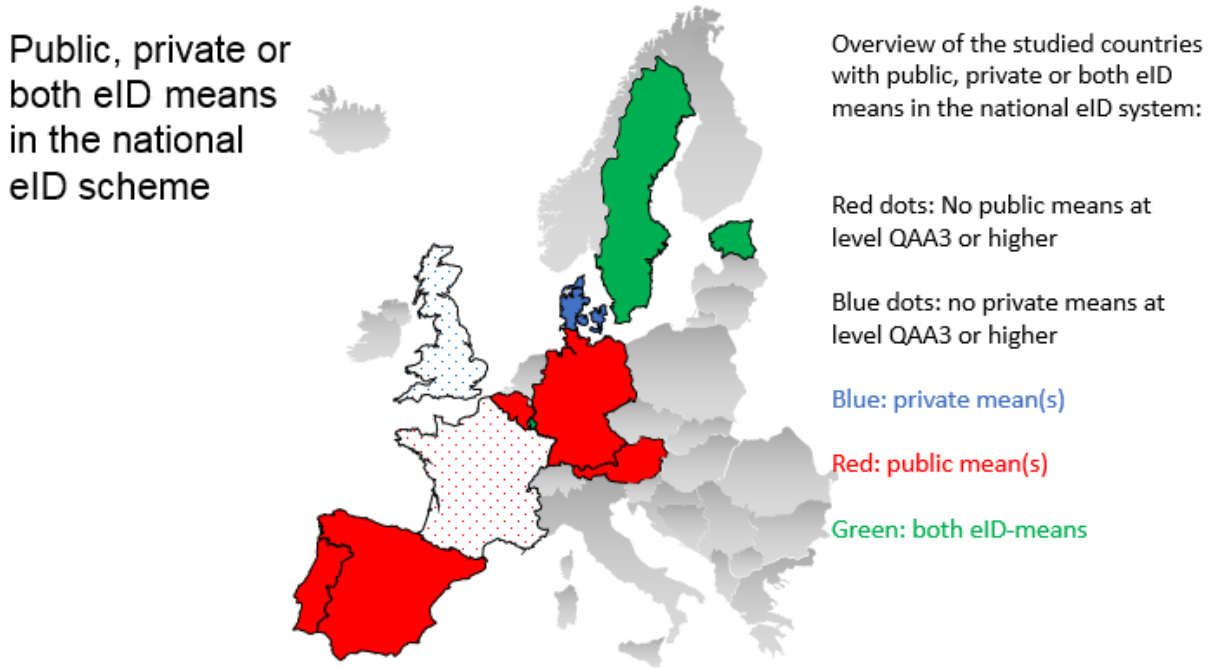
Attachment 4 gives an overview of some facts regarding the eID in the selected countries. The essential elements are presented in the following paragraphs.

3.1 Selection of countries

Starting from a quick scan of all Member States, a selection was made, aimed at maximizing diversity in the variety of public and or private eID means in national eID schemes, including both smaller and larger Member States, having a national eID means at QAA level 3 or 4.

At a later stage, France and the United Kingdom, albeit not having a QAA level 3 or 4 means, were included in the selected list because of the specific nature of their experiences in the area of eID and the value that may hold in discovering policy arguments.

The following figure shows the selected countries. The selection is further detailed in attachment C.



3.2 Findings on public and/or private eID means

Country	Classification	Policy considerations for the existing model
Austria	Public means, public-private use	The Austrian model makes use of a multi-means strategy of public and private cards as possible carriers of an eID means, and since 2009, it includes a mobile-ID solution (for improved convenience and usability). This model is monitored by the government. The Austrian government has decided to work with this strategy, because Austrian citizens will make use of the means that they already have 'in their pockets'. Availability and ease of use were therefore important considerations. The domain of issuing identity is seen as a (fundamental) government task. Therefore, the root identity (basic identity) is a government task. The market can subsequently fulfil different roles, if it meets the government's criteria. For this reason, the Austrian model has been made as open and technologically neutral as possible. Protection of identity is important. Therefore, the identifier has not been included on the certificate. The certificate comes from a private certificate authority (under supervision of the government).
Belgium	Public means, public-private use	With the introduction of the eID card, the Belgian government had a robust modernization agenda with strong political leadership. The rollout of an eID means belonged to this modernization agenda in which different actors, among which the Crossroads Bank for Social Security, played an important role. Belgium became a frontrunner in the area of eID, being one of the first countries to introduce an eID card. Now, mobile ID is also being considered. There is an active strategy to use the eID card and to phase out other cards, like the SIS card that is used in social security. The Belgian government consciously chose to keep identity and identification under its control. In this way, the government continues to have access to information about the most important actors in society: citizens and companies. In the Belgian context, this is an inalienable task of the government. This is why the Belgian government chose to work with a public means. Moreover, the market was not mature enough during the rollout, so there was no discussion about a public or private eID means. In the realization of the card and the accompanying infrastructure (e.g., card readers), different private parties were involved through tenders. Liability is an important issue and is maintained

Country	Classification	Policy considerations for the existing model
		with contracts and service level agreements (SLAs). The liability of the State is legally maximized to about EUR 2500.
Denmark	Private means, public-private use	In the area of eGovernment, Denmark is advanced and has high ambitions. Because several government services are mandatorily digital, it was and is essential to widely spread an accessible eID means. Denmark does not work with an ID card. Therefore, introducing an eID card was not among the options available to the Danish government. The Danish government furthermore assessed that it lacked the relevant knowledge to implement an eID solution itself. The government therefore called for tenders from the private sector, which would be valid for five years, and has done so twice so far. The current tender will end in 2017, and a new one is being prepared. According to the Danish, the high-level eID market for eGovernment services is insufficiently mature and cannot do without government stimulation, given the eGovernment ambitions.
Estonia	Public and private means coexist, public-private use	Under the supervision of the prime minister, the Estonian government introduced an active eGovernment policy called 'Digital Estonia'. Before the rollout of the eID, Estonia started with banking means for eGovernment. After the introduction of these banking means, Estonia rolled out a strong public eID card solution, which provides access to, amongst others, banking services. The eID card provides a higher possibility for financial transactions than the banking eID means, because of a higher assurance level. No discussion has taken place on this issue. The cooperation between banks and the government was and is very good. This fits with the culture and history of the country. The government did not pay for access to eGovernment services when only the banking eID means were used. A pragmatic solution-centred mentality contributes to a cooperative attitude between governments and between the public and private sector. There is no wish to compete on infrastructure since it offers very limited competitive advantage in the current scenario. Banks want to make the shift to the safer public eID card (including mobile ID). Considerations with regard

Country	Classification	Policy considerations for the existing model
		to availability were important to realize the strategy of a strong Digital Estonia. User comfort and use led to the mobile-ID strategy.
France	No means at a high level	France prepared an eID card solution to provide for a national eID scheme and eID means. This was rejected by the French Constitutional Council (Conseil Constitutionel). Privacy, possible accountability of the State towards the market (the card would also provide access to market services) and biometric data that would be placed on the card were points of issue. France does have a username and password system for certain sectors, including access to the national personalised government portal (mon.service-public.fr). A federation project is going on in order to realise generic access. This is based on a username and password system and does not provide a high level of assurance.
Germany	Public means, public-private use	Germany explicitly chose a public eID means in order to monitor privacy and safety. Identification is an important task of the government, and Germany seeks influence and control in the entire identity chain. Germany has a strong tradition with the ID card and it is widely accepted among the population. Therefore, the decision to work with a public eID card was a logical one, which was not challenged. In Germany, the provision of a means of identification, including electronic identification, is exclusively part of the public sector. That does not mean that no private parties are involved with the production; private parties are involved and they expect a certain amount of governmental control. Germany has a contactless card and has also developed a mobile ID whereby the mobile phone functions as a card reader for the eID card.
Luxembourg	Public and private means coexist (since 1-7-2014); private means gives access to public and private services; the public means gives access to public services	In Luxembourg, the eID scheme has long been managed by LuxTrust, with only private means. LuxTrust itself is a public-private partnership, with the government share being two-thirds. The choice of a private means was a pragmatic one; nothing else was available for a long time. Recently, Luxembourg started with the rollout of a public eID card that also offers functionality as a travel document. The card is significantly cheaper than the private solution, but offers less digital functionality. There has not been any resistance from

Country	Classification	Policy considerations for the existing model
		private partners to the introduction of the eID card. Broad availability and access to as many services as possible have been the main considerations for the introduction of the public means.
Portugal	Public means, public-private use	Portugal has provided its ID card with the eID functionality. This eID card replaces five other cards. Adding eID functionality was a logical step. Moreover, the Portuguese eID scheme offers mobile ID. Accessibility to services and the development of eGovernment and EU regulations are important considerations for the implementation.
Spain	Public means (and mixed), public-private use	In the Spanish context, the availability of an eID means is an important factor. The federal government has limited competences regarding the regions. Therefore, the national (e)ID card (DNIe) is the only option to guarantee universal coverage. DNIe is mandatory for every public administration. Activation and use by citizens can be further improved. For this reason, Spain is also considering the introduction of mobile ID. In Spain, the law allows multiple eID means. The national eID means is the eID card, but there is an alternative eID. This system is allowed by the law and is based on electronic certificates. It consists of a combination of public and private eID means and is used more often. There are regions that do not accept some of these eID means mainly because of the costing structure. Within this eID scheme, there is a discussion about the balance between public and private means, because the public eID certificate is issued for free and therefore competes with private eID means. Furthermore, Spain (just like France) is working on a federation project in order to combine the different username-password systems that are active for the supply of government services to one federative solution.
Sweden	Public and private means coexist, public-private use	In Sweden, the eID Scheme and eID means have been introduced in a very pragmatic way. The government has introduced standards and tests these standards, which include an open market for private (and public) suppliers of eID means. If a party meets the standards, it can join the system. De facto, it is

Country	Classification	Policy considerations for the existing model
		mostly the bank authentications that dominate the use. The government did not want to pull the 'technique' to itself and the market was prepared to supply authentications if the authentications were paid for. Experiencing privacy in Sweden is different than it is in the Netherlands. In Sweden it is normal for personal data and numbers to be used frequently by different government organizations as well as by the private sector. Moreover, the banks are very much trusted, even during the recent crisis. Although the banking solution did not completely cover the eID issue at the start, it was practical and offered a quick take-up. With the introduction of an eID function on the eID card, a solution was found for those unable to access an eID means earlier. Based on the argument of inclusion, it was decided to make it possible to also use the public ID card as an eID means. With that decision, a public carrier has been added to the eID scheme, which has become a mixed scheme de jure. In fact, the actual transactions are largely transactions that go through banks.
United Kingdom	Private means, public-private use *only up to QAA level 2 is currently available!*	Plans for a national eID card solution did not take-off in the UK, as public opinion was against it. Not expecting people to carry around a card and not creating a single database of all people are important underlying arguments in the UK. This is in line with the general opinion with regard to a central persons register and a PIN, both of which are not available in the UK. Privacy and trust levels are important factors in the UK. To enable eID in the UK, a new approach has been introduced, covering QAA levels 1 and 2. The approach includes a call for tenders to the private sector for authentications, not only dealing with the authentications themselves but also determining the identity of the user. To enable this system, the UK has defined outcome-based assurance levels. In a tender from the government, private sector actors have been selected. This approach has taken away worries of the citizens, enables innovation and safeguards privacy. Choosing a market-based solution fits well within the UK tradition, where private initiative plays an important role.

3.3 Findings en marge

Country	Use	Financing	Private actors in realizing an eID means	Private use of citizen registration/ PIN (citizen no.)	Incidents	Mandatory open source software	Single point of failure (SPF)
Austria	N/A. About 650,000 certificates are currently in active use by citizens.	The government purchases certificates through a tender; different ministries make a contribution. Mobile ID leads to questions about the costs of text messages.	Yes, tendered.	No. Identifier is part of the public sector and is not included in the eID means.	None.	Not applicable.	Validation service is possible SPF, but is not a point of discussion.
Belgium	Mandatory use of eID card leading to high level of penetration. The number of transactions is unknown.	The card is provided by municipalities; the citizen pays for the costs of the eID card. Other expenses (maintaining the necessary infrastructure) are financed from the central budget.	Yes, tendered.	Not applicable. (public means)	None.	Not applicable.	Not point of discussion.
Denmark	About 4.2 million NemIDs are activated. About 50 million transactions *per month* of which about 75–80% are from banks and 20–25% are from other transactions.	The government spends about DKR 200 million for a five-year period (standard amount). This is about one-third of the total costs. Other costs are paid by the respective market actors. The government budget need is supplied by the different levels of government, following a fixed calculating rule.	Yes, private means.	Encrypted use of national PIN.	No.	Yes, certificate policy that CA needs to comply.	Yes, SPF is a motivation to reconsider the model. The vulnerability does not go well with mandatory use.

Country	Use	Financing	Private actors in realizing an eID means	Private use of citizen registration/ PIN (citizen no.)	Incidents	Mandatory open source software	Single point of failure (SPF)
Estonia	About 200 million transactions in the past 10 years (only government).	Mobile ID is a service for which the citizen pays monthly. The eID card is paid for by the citizen. The production cost of the eID card is covered by the citizen. The citizen makes a one-time payment of EUR 25 when the application is submitted in Estonia and EUR 50 when it is submitted at the embassy.	Yes, tendered.	Yes.	None.	Recommen-dations are given.	Reason to roll out a distributed interoperable architecture.
France	Not applicable.	Not applicable.	Not applicable.	Not applicable.	N/A	Not applicable.	Not applicable.
Germany	The use is not measured or updated as a policy decision.	The citizen pays for the eID card. Other costs are covered by the federal budget. If a citizen forgets his or her PIN, re-activation is a paid service.	Yes, the German government has taken an interest in the fabrication of the eID card.	Not applicable. Germany does not work with a PIN. Connection with the register takes place at the municipal level.	None.	Not applicable.	Not point of discussion in Germany due to the chosen model.
Luxembourg	Unknown.	Information about the recurrent budget is unknown at present. The government-offered eID cards cost EUR 14, the private eID cards offer more functionality and cost EUR 85.	Yes.	No.	None.	No.	Not point of discussion.

Country	Use	Financing	Private actors in realizing an eID means	Private use of citizen registration/ PIN (citizen no.)	Incidents	Mandatory open source software	Single point of failure (SPF)
Portugal	In 2013, there were about 115,000 eID users and about 6 million transactions in Portugal.	The eID card is financed by the citizen; other costs are financed by the budget.	Yes, tendered.	Not applicable.	None.	Not available.	Not available.
Spain	In 2013, there were about 1.2 million validations of the national eID card (a very high level of penetration, no mandatory use of eID). Most probably, the use of other certificates is almost three times as high.	The eID card is financed by the citizen, regardless of whether it is activated (which is not mandatory). Other costs are financed by the general budget. Changes in the system have been agreed and will be implemented towards a fee per unique user validations per month.	Yes, tendered.	Private parties that issue a certificate are allowed to register the PIN.	None.	Not applicable.	The validation platform is not a strategic point of discussion.
Sweden	The level of penetration is high. More than 5 million eID carriers; about 300 million transactions per year of which about 80 million are eGovernment.	The government buys 'validation control' (pay per validation) of private actors. Any private actor that meets the criteria can offer eID services (predominantly banks).	Yes, private means.	Yes, private means.	None.	No, only the 'identity insertion' is a strict prescription.	The service discovery module, which is not critical.

Country	Use	Financing	Private actors in realizing an eID means	Private use of citizen registration/ PIN (citizen no.)	Incidents	Mandatory open source software	Single point of failure (SPF)
United Kingdom	The eID scheme has just started and uptake is starting to take shape, reaching almost 100,000 authentications in 2015 as of March 2015.	The identity assurance programme currently runs on a centralised funding model, with the central government department (the Cabinet Office) bringing together demand from all other departments to make one procurement. In December 2014, an OJEU notice estimated the value of the procurement as GBP 150 million.	Yes, private means.	Not applicable.	Not applicable.	The market is free to make its own design.	Discussed, but did not design the model.

4. Conclusions

The central question was: '*Describe whether public and/or private eID means are used in the different [EU] Member States for online access to at least government services. Elaborate the policy arguments on the basis of which this solution developed'.*

This study led to a conclusion at two levels. The first level is about the policy arguments to come to a specific eID scheme and its public and/or private eID means. The second level is about the related side-observations.

4.1 Policy arguments

There is a broad range of different functioning eID means in the countries that were studied, from private to public. While working with the same considerations like availability, inclusiveness, accessibility, privacy and safety, countries come to different conclusions regarding which means to include in there eID scheme. The cultural and historical backgrounds as well as the administrative culture, the extent to which eGovernment is an ambition, the extent to which eGovernment is implemented, and the moment at which the eID means are introduced are important aspects for understanding the decisions of the studied countries.

A continuum seems to be in place, from a public responsibility for the system, to a private implementation. The government plays the central role in designing and managing the eID scheme, while the practical implementation of the production of eID means is mainly done by private parties. Every country that has been studied finds itself in one or another location on this continuum of more private to more public.

Public-private sector competition regarding eID means in the national eID scheme is not, or hardly, recognized. None of the countries have indicated serious discussions between the government and the private sector, or at the political level, regarding the choice of a public, e.g., private eID means in the national eID scheme. One of the elements that surfaced repeatedly is whether the open market for high assurance eID for eGovernment services is mature enough to function without government stimulus.

Developments in some of the larger EU Member States show that discussion regarding important policy considerations have different effects in different countries. It is striking to see that a similar solution (eID cards) was not adopted in France and the UK, but is being implemented in Germany, apparently weighing the same important values such as privacy and access, but coming to different conclusions. These differences seem to be explained from their cultural and historical backgrounds, including the relationship and role of government in the respective societies, leading to a certain understanding of the role of the government in the identity chain. This is also reflected in their implementation of a citizen register and a citizen number (personal identification number (PIN)).

In some systems that make use of private eID means, like Estonia, Luxembourg, Spain and Sweden, a public means was introduced at a later stage, linked to the eID card. This decision was made from the point of view of availability and inclusiveness (to make it possible to spread the eID means to a large section of the population, without excluding anyone).

Use and user friendliness are important considerations. In Denmark and Sweden for instance, ease of use and usage led to pragmatic solutions linked to private means that are (partly) financed by the government. In Austria it was an important argument to come to its multi-carrier strategy. Countries that have introduced a national eID card at a relatively early stage are now often looking for ways to innovate. In some, mobile ID is being introduced; in others, username-password solutions are being studied as an additional means or for broader use.

4.2 En marge observations

Several aspects have been highlighted in the study and have been discussed in chapter 3. Based on these, the following observations are shared.

- There is a distinction between producing the means, the chip, and 'filling' the chip, the process of issuing the card and the renewal or supplementation of the information on the chip. Whether on behalf of the government or not, different steps are taken by private parties. Technique seems outsourced. It is not always easy to differentiate between a public and a private means. Eventually, private parties always play a role in finding a solution.

- In countries that make use of private eID means, the government shares the costs. The United Kingdom, Sweden and Denmark have the most private models and these countries have designed their own financing structures. The United Kingdom and Denmark have done this with the help of generic tenders, and in Sweden a pay-per-use model is in place. The citizen pays the costs for the eID card in countries that have introduced eID card solutions. Text-message verification for mobile ID is an important point of attention. Estonia is an exception; the Estonian government did not pay for the bank eID even when it was the only means that provided access to the eGovernment.

- Mobile ID is emerging. Many early adapters use an active mobile-ID strategy to increase the ease of using eID.

- Having a single point of failure does not seem to be a decisive consideration in the choice for an eID-means strategy. Only Denmark indicates that it is considering this aspect in the next tender for its eID means. Perhaps this is related to the fact that none of the countries state that they have ever experienced an incident that led to any serious discussion in national parliament.

- Some countries allow the private eID means to use the national registration and/or a personal identification number (PIN). Cultural and historic-based arguments also seem to underlie this choice.

Attachment A – Research accountability

The initial research and report in Dutch, and this edited English version, rewritten to be accessible to an international audience of (European) eID experts, were commissioned by the Dutch Ministry of the Interior and Kingdom Relations.

The Director for Citizenship and Information Policy was the senior owner. The day-to-day guidance was in the hands of Ms Corien Pels Rijcken and Mr Carlo Luijten of this directorate. Mr Luijten guided the international version of the report.

At PBLQ HEC, Mr Nathan Ducastel was responsible for the project. He was assisted by Ms Ingrid van Wifferen and Mr Evert-Jan Mulder. This international version of the report was produced by Mr Ducastel, with the assistance of Ms Sacha van den Berg.

The research took place from July to October 2014 and was supported by a Dutch expert group. The international version was written during January–March 2015. Factual information regarding countries selected for a more in-depth study was validated by the eID experts who were interviewed during the initial research with the exception of France, where an earlier email validation of the core information has been reused.

With special gratitude to Mr Freek van Krevel of the Ministry of Economic Affairs, who made the connection between the different eID experts through the eIDAS network and who ensured an excellent starting position for the conversations.

Studied documentation (selection)

Study on impact assessment for legislation on mutual recognition and acceptance of e-Identification and e-Authentication across borders, IntraSoft & TNO (2012).

D2.2 Report on legal interoperability, STORK (2009).

Study on Mutual Recognition of eSignatures: Update of Country Profiles, IDABC/Siemens (2009).

Electronic Identities in Europe: *Overview of eID Solutions Connecting Citizens to Public Authorities,* UL Transaction Security (2013).

Impact assessment accompanying eIDAS proposal*,* European Commission (2012).

eGovernment Benchmark, CapGemini (2014).

eGovernment Member State Factsheets, ePractice Website.

Afwegingskader publieke diensten in het eID-stelsel NL, June 19, 2013.

D.7.3 Business Plans — Consolidated Report & Recommendations, STORK 2.0.

D 3.3.5 Smartcard eID Comparison, STORK.

The evolution of a national eID system building the Swedish identity federation (Swedish eID)
2014-09-08 Swedish eIdentification Board, Presentation.

NemID ekstern statistik rapport nr. 06-2014.

Notitie Forum Standaardisatie FS22-10-07, betreft: Indeling van authenticatiemiddelen, September 25, 2009.

eID Stelsel Nederland, Strategische verkenning en voorstel voor vervolg.

Attachment B – Questionnaire

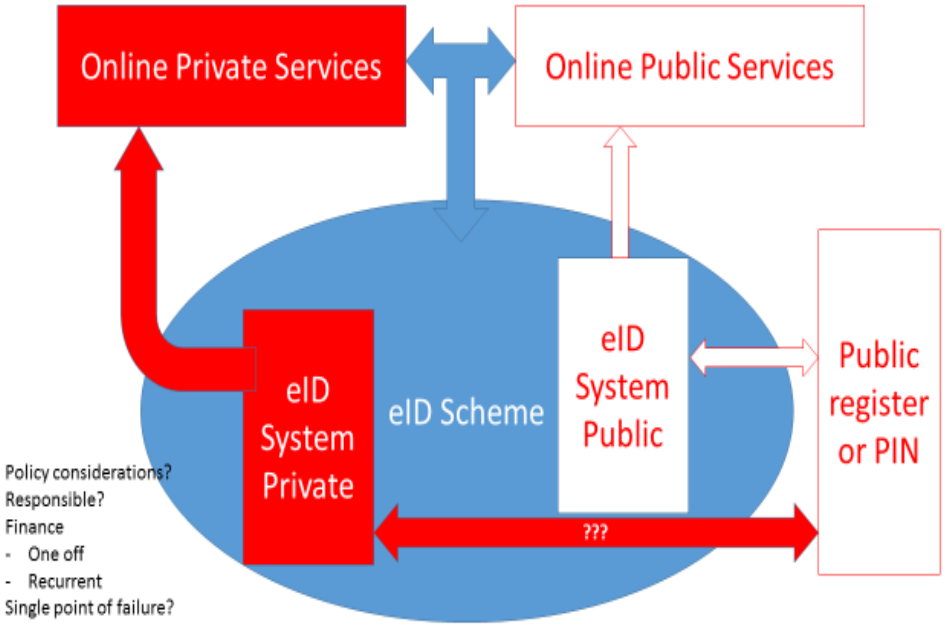
Questionnaire — definition of terms

(National) eID scheme: the set of (formal) agreements and arrangements that make it possible to access online (at least) multiple public services for which electronic authentication is required.

(National) eID system: the infrastructure (including a token) enabling online authentication for online access to multiple public services, such as bank eID, citizen card eID, mobile eID, etc.

Public eID system: a system under the direct supervision and control of the government, rooted in national legislation, which assigns political responsibility.

Private eID system: a privately owned eID system, fulfilling a role in a national eID scheme.



Questionnaire

A) Your National eID Scheme and eID System(s)

1) Who holds political responsibility for your national eID scheme? (In other words: who answers or reports to parliament if considerable (societal) damage occurs from the use of the eID scheme, e.g., fraud?)
    a. Has any incident taken place that led to discussions in parliament? Please describe briefly.
    b. Who holds political responsibility in case a private eID system is used and causes an incident?
    c. Who is liable in case a private eID system is used and causes an incident?

2) Does your eID scheme include a public eID system?
    a. Are private actors involved in realizing the public eID system?

b. If yes, at what stage in the process (of creation to use)?

3) Does your eID scheme include private eID systems?
    a. Who holds (political) responsibility for private eID systems in the national eID scheme?
    b. How is this organised?
    c. Is there a governmental open standards policy in place and upheld for private eID systems?
    d. Does the private eID system make use of a public persons register or public personal identification number (PIN)?

4) How are the initial and recurrent financial costs of your eID scheme covered? What is the approximate budget per year?
    a. Via the general government budget?
    b. Via a pay-for-use model? If so, please describe briefly (citizen or service provider to pay a fee).
    c. Any other?

5) How are the recurrent financial costs of your public eID system covered? What is the approximate budget per year?
    a. Via the general government budget?
    b. Via a pay-for-use model? If so, please describe briefly (citizen or service provider to pay a fee).
    c. Any other?

6) Do private eID systems receive any financial support from the government?
    a. Via the general government budget?
    b. Via a pay-for-use model? If so, please describe briefly.
    c. Any other?

7) Do private eID systems contribute financially to the eID scheme?

8) How many authentications per year go through your eID scheme?
    a. (If applicable) How many are via the public eID system, and how many via the private eID system?
    b. (If applicable) How are they distributed over public and private services?

B) Public and/or Private eID Systems

1) Which eID system(s) function in your national eID scheme?
    a. Public eID system?
    b. Private eID system?
    c. Both?

2) Do all eID systems in the national scheme give access to the same set of services?
    a. If not, what are the exceptions?
    b. Do the services include private services (such as online banking, shopping, etc.)?

3) What were the policy considerations for this choice? (Please consider elements such as: accessibility of services and infrastructure, availability to (exclusion of) citizens, privacy, security, efficiency/costs and competition.) (Note: This is a non-exclusive list.)
    a. Which arguments were dominant in each consideration?

b. Was any discussion consolidated in formal documentation (explanation of law, transcripts of parliamentary discussion, or otherwise)?

4) Was there, at the time of introduction, or is there now, any discussion in your country regarding the choice for public, private or mixed eID systems in your eID scheme?
    a. If so, can you give the key issue(s)?
    b. If not, do you have any indication as to why not?

5) What have been the positive or negative consequences of your choice with regards to
    a. Citizen satisfaction (use) and trust (with regards to the government)?
    b. Reliability (including incidents with societal impact)?
    c. Costs (unexpected effects)?

6) Does your scheme have single points of failure? How is this looked upon? Is it part of the discussion and considerations for the model chosen?

Attachment C – Country selection

A quick scan of EU Member States with regards to the use of public or private eID means in the national scheme, led to the following overview. The overview shows Member States that have a national (generic) eID scheme, organised towards public or private eID means and the aces they give to public or both public and private services.

In a national eID scheme: eID means/services	Public services	Private/Public services
Private		Denmark, United Kingdom
Public	Lithuania, Netherlands (DigID), France	Austria, Belgium, Germany, Hungary, Portugal
Private and Public		Estonia, Finland, Italy, Latvia, Luxembourg, Spain, Sweden

The following remarks, at the time of the research, complete the overview:

- Cyprus is starting to introduce implementation of an eID card and eSignature but does not have a national eID scheme at present and is therefore not included.
- Bulgaria, Czech Republic, Ireland and Poland have eID means that give access to individual online public services but they do not add up to a national eID scheme and are therefore not included in the overview.
- Austria, Estonia, Finland, Lithuania, Portugal and Sweden have or are working on mobile-ID solutions. Other countries such as Belgium, Germany and Spain are investigating the possibilities of offering mobile-ID solutions.
- For Greece, Malta, Slovakia, Slovenia and Romania, we were unable to determine, within the scope of the research, whether access to services included only public or both public and private services.

After the initial overview presented above, in a meeting with Dutch eID experts, the following selection of countries was made for more in-depth study.

Country	Why?
Austria	Started relatively early with the implementation of a successful eGovernment strategy (leading the European rankings) and the rollout of eID means using a multiple-carrier strategy.
Belgium	Started relatively early with the rollout of an eID card with a high assurance level. The Belgian eID card has a very high penetration rate.
Denmark	Has made several aspects of eGovernment mandatory for citizens and therefore relies on eID. It uses a private eID means strategy, through a public government tender.

Country	Why?
Estonia	Introduced an eID means at an early stage to support a successful modernization strategy. The public means is dominant in a mixed eID scheme.
France*	Is an important actor within Europe, but an eID card solution was not accepted.
Germany	Has a contactless solution and has a strict interpretation of privacy protection. As a country, Germany is an important frontrunner in Europe.
Luxembourg	Has a system of public-private partnership with private means; it recently added a public means.
Portugal	Makes use of a public eID means.
Spain	Makes use of a public eID means.
Sweden	Has private means mostly used in a mixed system. Sweden is very advanced with the eGovernment rollout.
United Kingdom*	Is an important actor within Europe, but an eID solution was not accepted. It has now switched to an explicit private strategy for eID means.

*No eID means available at high-level assurance (QAA level 3 or 4).

Attachment D – Country descriptions

Austria

General introduction

In Austria, there was a need for an electronic tool that could uniquely identify citizens and businesses. This eID became the ‘citizen card’. The citizen card is not a specific card. (A mobile phone is also a ‘citizen card’.) Even where it is used in a card-based system, it is not combined with a physical ‘ID card’; rather, it is a multi-carrier model for eID. The citizen card can be used to authenticate users and sign documents securely and electronically. Since Austria introduced and implemented the ‘mobile phone signature’ (a variant of the citizen card) at the end of 2009, it is no longer necessary to have chip cards or card-reading devices, or to install software on a local machine in order to use the citizen card’s functionality.

Austrians feel that in comparison to other systems, the citizen card has many advantages. The normal username-password approach presents a high-security risk, inter alia, due to poorly chosen passwords. Research has shown that many computer users select bad, easy to crack passwords (e.g., their own name) or write the passwords down. Passwords can also be intercepted on the Internet. All of these problems lead to unauthorized access. The 'digital signature' is covered by law and protects against unwanted access and changes to content.

The term 'citizen card' is used to describe an identity management concept that makes it possible to provide electronic services for public administration employees and citizens in a simple and secure manner. Being the electronic identification on the Internet, the citizen card provides unique identification and authentication of users, which is necessary in order to offer certain electronic procedures. When the citizen card’s functionality is activated (e.g., free-of-charge on a citizen's eHealth card), a qualified certificate and an 'identity link' is saved on the storage medium. The identity link establishes a link between the person and the storage medium. This enables the person to be identified at a later time. The authentication and signature certificates are used to sign data and documents. (The card-based solution includes an additional certificate for encryption.)

The eGovernment Act (E-Government-Gesetz) sites the citizen card’s functionality, specifying that the citizen card must contain a qualified electronic signature (§ 2 L 10 E-GovG). In Austria, the qualified electronic signature is the legal equivalent of a handwritten signature as foreseen by the EU Signature Directive, and has unlimited uses in business and administrative affairs, be it in Austria or across its borders.

Since the end of 2009, a mobile phone solution called the 'mobile phone signature' has been introduced. The mobile phone signature (citizen card functionality on a mobile phone) was developed with the support of the European Commission in the large EU pilot project on interoperability of electronic identities called 'STORK'. This solution makes it possible to use qualified electronic signatures with a mobile phone. This is in contrast to the card-based citizen card, as installing software and additional hardware (card reader) is no longer necessary. As the mobile phone does not produce a signature as such but only serves the purpose of triggering the qualified signature in the hardware security module of the provider, there is no requirement for a specific SIM card in the phone. Nor is a smartphone required.

eID scheme and means

In Austria, the federal chancellor is politically responsible for the eID scheme. Although the Austrian eID scheme can be categorized as public, the eID scheme is a closely intertwined system with public and private actors under the supervision of the government, making it a multi-means system. The process of issuing eID

means, however, remains public. The certificates that are used are private. In general, the Austrian eID can be classified as a public means with public-private use.

In Austria, no incident has taken place that led to discussions in parliament. Handing out the certificate on a card can be done by designated public and private organizations such as municipalities, banks and post offices. The card can be a public card like the health card or a card of a private company, as long as it fulfils the requirements. Austria also makes use of mobile ID.

The costs of the Austrian eID scheme are covered by the government. Different ministries with a specific interest in the eID scheme make a contribution to the budget. The budget share covered by each ministry is a political agreement.

Information about the budget for Austria's eID scheme is not available. Certificates are bought by the government to ensure a free service to citizens. In this way, the government financially supports private certificate service providers.

Approximately 650,000 certificates are currently in active use by citizens. Mobile ID is used frequently. Austrian citizens are not obliged to activate an eID. Activation is free of charge. By activating an eID, a citizen signs a contract for proper use of his or her digital signature and the card itself, meaning that the citizen does not hand it over to third parties.

Policy considerations

The Austrian model makes use of a multi-means strategy of public and private cards as possible carriers of an eID means. The Austrian government has decided to work with this strategy, because Austrian citizens will make use of the means that they already have 'in their pockets'. (In Austria, this is the eHealth card rather than any other smartcard.) The higher convenience and better usability led to the rollout of mobile ID in Austria.

The domain of issuing identity is seen as a (fundamental) government task. Therefore, the root identity (basic identity) is a government task. The market can subsequently fulfil different roles, if it meets the criteria of the government. For this reason, the Austrian model has been made as open and as technologically neutral as possible. Protection of identity is important. Therefore, the identifier has not been included on the certificate. The certificate comes from a private certificate authority (under supervision of the government).

Belgium

General introduction

Belgium was included in this study, because it started relatively early with the rollout of an eID card with a high assurance level. The Belgian eID card is widely spread among the population. The eID card contains all the information included on the traditional ID card and serves as an identification and travel document. It is a smartcard containing two certificates. The first one is for authentication and the second one is for generating digital signatures. The Belgian eID card thus provides access to restricted online services. The national register number, the unique identification number for Belgian citizens, appears on the eID card and its microchip. It is used as the unique identifier in the certificate of the eID card.

Almost all electronic signature applications in the Belgian eGovernment sector make use of the Belgian eID card. On the federal eGovernment portal 'Belgium.be', four levels of security exist, depending on the type of eService delivered: (1) no password required, (2) password required, (3) password and token required, and (4) eID only. The eID card can only be issued for natural persons.

In March 2009, the Belgian government introduced an eID card for children under the age of twelve. This special eID card can provide access to children-only Internet chat rooms and to a range of emergency phone numbers, in case the child is in danger. Since July 2008, foreign nationals living in Belgium are entitled to replace their old paper identity with versatile and 'smart' electronic identity cards. They come in two varieties: for EU and non-EU citizens.

eID scheme and means

In Belgium, the Ministry for the Interior is politically responsible for the national eID scheme. On technical issues, the Ministry is often supported by FEDICT (the Federal Public Service for Information and Communication Technology). Only in 2001, when the eID development project took place, was FEDICT responsible for the project.

The eID scheme in Belgium is public. eID means can be used for both public and private services. The most important eID means are the eID card, kids ID, paper token system and the SIS social security card. Several private parties were involved in the realization of the public eID scheme. They are part of the chain of operation. They have tendered, and have been awarded contracts with strict and elaborate SLAs (back-to-back liability).

The approximate overall budget for financing the costs of the Belgian eID scheme is not available. The total costs for putting an eID card in the pocket of every Belgian citizen are approximately EUR 250 million. The programme and maintenance are financed through general budget support. Individual authentications are charged for. Municipalities are free to ask for a fee for the eID card. This is currently approximately between EUR 13 and 17 per eID card. Municipalities are charged an amount of approximately EUR 9 by the national implementer. The number of authentications per year is uncertain, because it is not singled out as the only online web service use. It includes many private and practical offline identifications. The use of the eID card in Belgium is considered successful.

Policy considerations

With the introduction of the eID card, the Belgian government had a robust modernization agenda with strong political leadership. The rollout of an eID means belonged to this modernization agenda in which different actors, among which the Crossroads Bank for Social Security, played an important role. Belgium became a

frontrunner in the area of eID, as it was one of the first countries to introduce an eID card. Now, mobile ID is also being considered as an option. There is an active strategy to use the eID card and to phase out other cards, like the SIS card that is used in social security. The Belgian government consciously chooses to keep identity and identification under its own control. In this way, the government continues to have access to information about the most important actors in society: citizens and companies. In the Belgian context, this is an inalienable task of the government. This is why the Belgian government chose to work with a public eID scheme.

Another important factor was that the market was not mature enough during the rollout. Therefore, there was no discussion about the decision to work with a public eID system. In the realization of the card and the surrounding infrastructure (e.g., card readers), different private parties were involved through tenders. Liability is an important issue and is maintained with contracts and SLAs. The liability of the Belgian government is legally maximized to about EUR 2500. Liability is back-to-back within the entire production chain. The liability for the Belgian government is limited to the correct information on the card, which is fully in line with the information in the 'Rijksregister'. International considerations and links have also been taken into account. The eID card currently has a validity of ten years.

Timing was another very important consideration. The Belgian government was eager to reform and modernize. Political leadership drove the development of eID. The demise of the former ID card infrastructure created an opportunity. Furthermore, there has been no discussion regarding public and private interests. In Belgium, eID is very strongly connected to physical identification. (Mandatory physical identification was introduced early on.) Therefore, it was considered logical that the government would perform this task. Moreover, in 2001, the market and private parties had not yet matured in this area. The principle of 'never outsource your core business' makes it unnatural in the Belgian situation to leave electronic identification to other (private) parties, because citizens and companies are the government's core business.

Denmark

General introduction

Denmark was included in this study, because the rollout of its eGovernment is highly developed. It is an interesting case, since it makes use of private eID means that are tendered by the government and that are based on a national standard for public certificates.

The Danish have implemented eID since 2003 through setting up standards and then tendering to the market to implement and roll out the eID system. This was part of their digitisation strategy. The strategy includes up-to-date laws on the mandatory use of eGovernment, making eID (NemID) a necessary prerequisite.

eID scheme and means

The Danish Ministry of Finance is responsible for the eID scheme even though Denmark works with a private eID means. The eID means can be used for both public and private services. This is organised through contracts and SLAs. There is a national open standard for a public certificate policy in place and is applicable to the private eID system. The certified authority (CA) has to comply with the requirements of the certificate policy.

Denmark introduced NemID in July 2010. It is a digital signature that provides easy and safe access to a wide range of public and private self-service solutions on the web (including eBanking, real estate, insurance and pension funds services). With this digital signature, citizens use the same user ID and the same password and OTP (one-time password) card for online banking, government websites and a wide range of private services online. NemID is the result of the collaboration between the central government, municipalities and regions, the financial sector and a private contractor. More than 80 per cent of the Danish population (fifteen years and above) uses this Danish eID means. A special solution was also developed for the blind and partially sighted in cooperation with the Danish Association of the Blind.

The development of an efficient and secure infrastructure for digital signatures, which continuously supports the demands for a safe and leading knowledge society in Denmark, is the responsibility of the Danish Agency for Digitisation under the Ministry of Finance.

In the early 2000s, the Danish government assessed that rolling out certificates to citizens themselves would not take place on its own, as the market was not mature enough. No services and no means existed yet. The digital strategy of increased eGovernment presupposed widely available eIDs for citizens, and the Danish government wished to break this chicken-and-egg circle. The digital signature (later NemID) was therefore financed by the public sector and distributed to the citizens for free. Even now, the expectation is that without government funding it will be difficult to keep the same high dissemination and use of NemID.

Since citizens were not used to eID, it had to be free of charge and easy to use in order to experience a real take-off. The tender was first won by TDC, a Danish telecom provider. The second tender was won by a combination of banks and TDC, which set up a separate organization for this goal. The security requirements were higher than in the first tender. This organization has now been sold to several investment funds, including an American venture capitalist and a Danish venture capitalist.

The current tender runs until November 2017. For the new tender, all possible options (including a public eID system) are on the table.

No incident has yet taken place that has led to discussion in parliament. If the private eID system is abused and causes a loss, the private company is responsible for the content of the certificate. However, no cases have been reported yet.

The private eID system makes use of the public persons register, so public authorities can look up the connection between the personal identification (PID) number of the certificate and the owner's central persons register (CPR) number. Companies are not allowed to use this service unless the citizen gives consent, but they can use the PID number from the certificate.

The government tender is DKR 205 million for five years. This covers all major operational costs. The other investments in the scheme are made by banks. It was expected that the total investment over five years would be approximately DKR one billion. The government budget is split amongst government actors (central, regional, municipal) according to the practice of 40/20/40 per cent.

In Denmark, private eID systems deliver a financial contribution to the national eID scheme as they have to have a commercial agreement with the provider in order to use or receive and validate NemID. They also add to financing the infrastructure and use it for their own authentications. The financial sector draws the highest number of transactions. Other private actors and government transactions are only a smaller part of the total number of transactions (20–25%).

Policy considerations

The core policy considerations for the choice of infrastructure are a combination of usability and resources in encouraging eGovernment. Because Denmark does not have an official ID card, this was not the preferred choice. Moreover, no political will seemed to exist for an ID card at the time. Denmark does not have a tradition of physical identification through one national ID card. Danish citizens identify themselves using registrations and a combination of paper documents or by their passport or driver's licence, if available. It can be said that the level of validity of central registration is relatively high.

Another factor that was important for the choice of the current eID scheme was the fact that all banks participated in the model and, therefore, the penetration rate of eID in society was high.

Denmark has a tradition of using the private sector for IT operation and implementation. Therefore, the actual choice to tender for a private eID system, based on a public standard that sets out requirements for security, public supervision, etc. did not cause serious concerns. Privacy is not a big concern in Denmark where people have a fair level of confidence in the public sector. When the eID system was introduced, there was no natural market. But there was a strong digital ambition from the government and the public sector in general. The rapid rollout came with NemID, because NemID could be used for Internet banking as well as for public sector eServices.

The cooperation with the private sector has advantages such as following threat and risk profiles in detail. Furthermore, the usability increases. Disadvantages of working with the private sector are a lack of accessibility and a different perception of risks. This requires dialogue. In the new tender, the Danish government will aim for more modularity and flexibility.

The Danish eID scheme has a single point of failure. NemID has sometimes suffered from distributed denial of service (DDoS) attacks and has sometimes been unavailable for extended time periods. These incidents receive attention from the media. Strong protection against DDoS attacks has since been implemented in the infrastructure.

A challenge for the Danish government is that many actors and interested parties require a lot of coordination. Furthermore, the transition from an old to a new eID infrastructure is seen as a challenge as the infrastructure is widely spread and implemented across society. Continuity is therefore of utmost importance.

Estonia

General introduction

Estonia was included in this study, because the rollout of eGovernment is very developed and it started with the introduction of eID means at a relatively early stage. In January 2002, Estonia started with issuing national ID cards, which fulfils the requirements of Estonia's Digital Signatures Act. The ID card is mandatory for all Estonian citizens and resident foreigners over fifteen years of age. It is the primary document for identifying Estonian citizens and residents and it is used in any form of business — public or private. Moreover, it is a valid travel document within the European Union.

Since 2005, the Estonian ID card can be used to vote electronically, create a business, verify banking transactions, or as a virtual ticket. Since 2010, it can also be used to view a person's medical history. As of January 2012, more than 1.1 million people in Estonia (almost 90% of its inhabitants) have ID cards.

In addition to being a physical identification document, the card has advanced electronic functions, facilitating secure authentication and providing a legally binding digital signature for public and private online services. An electronic processor chip contains a personal data file, a certificate for authentication, a certificate for digital signature and their associated private keys, protected with personal identification numbers (PINs). The certificates contain only the holder's name and personal code (national ID code). The data file is valid as long as the identity card is valid (for a period of five years). So are the certificates, which thus have to be renewed every five years.

The 'mobile ID' is an ID-card based identity verification and digital signature solution for users of mobile phones in Estonia. This means that the mobile phone can act as a secure signing device. Thus, similar to the eID card, the mobile ID enables authentication and digital signing of documents, as it has the same legal value as the eID card. The user's certificates are maintained on the telecom operator's SIM card. In order to use them, the user has to enter a PIN. The new mobile-ID service (wireless public key infrastructure (PKI)) was launched in May 2007 by the mobile operator EMT, in cooperation with several banks and the certification centre (AS Sertifitseerimiskeskus). This service allows access to online banking services, without the entering of eBanking codes. To authenticate oneself securely with the mobile ID, the user clicks on a dedicated button in the web environment. Upon completion of this action, the user is requested to enter his or her authentication PIN. Once this operation has been completed, authentication is performed.

The same process applies to the signing of digital documents. In addition, mobile phones can be used to pay for car parking (m-parking) by phoning a certain number or sending a text message. The main advantages of the mobile ID include user friendliness and convenience; the computer no longer needs to be equipped with a card reader, or have special additional software installed.

eID scheme and means

Estonia works with a mixed system of public and private eID means. These eID means can be used for both private and public services. In this mixed system, the public means are dominant. The Ministry of the Interior is responsible for the eID scheme when it comes to issuance. However, the Ministry of Economic Affairs and Communications can also be held responsible if the issue concerns use. The Estonian eID scheme is organised by a police structure.

In case a private eID system is used and causes an incident, on the government side the ministry that runs the service is held responsible. However, the government shares responsibility with the private sector (banks). Because of certain agreements between the public and private sectors, there is a lower risk for both parties.

Both eID systems in Estonia provide access to the same set of services. There is no governmental open standards policy in place for private systems. Banks can do what they like, as long as they operate within the interoperability framework. There are some preferred approaches in place.

The private sector as well as the public sector can make use of the PIN. In Estonia, the PIN is not secret or delicate, because it is rather like a name and does not provide special access.

The financial costs of the eID scheme are covered as follows: for issuing an eID card, the citizen pays between EUR 25 and 50; for using the mobile ID, the citizen pays a small monthly fee of approximately EUR 3.

Policy considerations

A pragmatic solution-centred mentality seems to contribute to a cooperative attitude between governments and between the public and private sectors. One does not want to compete about infrastructure. Banks want to make the shift to a safer eID card (including mobile ID). Considerations with regard to availability were important to realize the strategy of a strong ‘Digital Estonia’. User comfort and use led to the mobile-ID strategy.

France

General introduction

France was included in this study, because it is an important actor in Europe that failed in its attempt to introduce an eID card. The proposal was not passed by the French Constitutional Council (Conseil Constitutionel). France therefore does not have any high-level eID means as yet. The available means are public.

The French government launched an eID card project called INES (Identité Nationale Electronique Sécurisée), which was endorsed by the prime minister and announced in December 2005. The eID card would have contained: traditional data (name, surname, date of birth, address, etc.) together with biometric data (two fingerprints), an identity-related services module containing an authentication certificate and an eSignature field.

The Development Plan for the Digital Economy by 2012, 'Digital France 2012', provided for the deployment of the eID card as of 2009. The deployment is still in progress. The card would have been based on a highly secure eSignature standard. In addition, it was meant to facilitate the direct participation of citizens in the public decision-making process.

eID scheme and means

There is no national eID system in France. France does have a framework for security in authentication, following the available standards and directives. eID solutions (username and password) are widely used in certain sectors such as social security (Amelie), social benefits (CAF) and taxation. The national citizens' portal (mon.service-public.fr) has a federation possibility, linking sectoral solutions to one master solution under the portal.

Currently, a project called 'France Connect' runs, which is in essence an eID federation project aimed at broadening the federation possibilities and adding to the scope of eID. However, this does not fulfil the need for a qualified signature or a high (security) level of eID.

As of now, many services are available online. They include a process step which requires the citizen to print a form, sign it and then send it to the government. In order to increase value, further innovate and digitise government service delivery, it needs to add functionalities.

In France, the electronic services provided online to citizens and enterprises, via the mon.service-public.fr portal, are supported by one common electronic signature solution. Only the electronic certificates provided by qualified certification service providers (CSPs) are eligible for the online interactions of citizens and businesses with the French government. To become recognized as such, the certificates are evaluated against the requirements of the 'General Security Framework'. There are three levels of security, namely: medium, high and qualified. The electronic certificates for businesses are issued to natural entities, but they are to be used only on behalf of an enterprise.

Policy considerations

The French Parliament has rejected the proposed eID card for eServices, which would have offered access to both eGovernment and private services, in line with eIDAS, at the highest security level (qualified signature). Three considerations were of specific importance. The first was the ruling of the Constitutional Council, which said a public eID card should not be used for private services. This was seen as a risk. Second, privacy was a serious consideration. Privacy regulations in France are strict and are upheld by the CNIL (Commission

Nationale de l'Informatique et des Libertés). The CNIL accepted the idea of the card, but gave strict guidelines for implementation. The third consideration was that the card would include biometric information, which led to even more resistance.

For politicians in France, it is more and more important to protect the privacy in the digital society, including security of property and financial transactions. France does not have a national personal identification number (PIN) or a central register, and it is not politically acceptable to create one.

Germany

General introduction

Germany makes use of a public eID system, and it is very conscious of the protection of privacy, which it interprets strictly. In November 2010, the eID card in credit card format, offering more functions, replaced the national identity card. The online function of the new eID card enables cardholders to identify themselves online with the use of a secret personal identification number (PIN) when dealing with government authorities as well as with private service providers (eShopping and eBanking). This made it faster and more economical and secure to open and log in to accounts and to verify address or age information. The introduction of the eID card needs to help with the fight against cybercrime and has to increase public trust in online transactions.

Because of the included microchip, the German eID card provides an online authentication functionality which is usable for both public and private services. Because of the assignment of authorization certificates and mutual authentication, cardholders can be sure that whoever requests their personal data is authorized to obtain it. The German eID card provides further protection against identity theft and offers user-friendly ways to guarantee valid client data for service providers. The German eID card includes the optional electronic signature functionality. It contains biometric identifiers stored on a chip, which satisfies requirements for official identity checks in order to ensure that the national ID cards continue to serve as secure travel documents. The biometric identifiers are restricted for use by the police and in border control, and are not available for online purposes.

eID scheme and means

The German Ministry for the Interior holds political responsibility for the national eID scheme. The national eID system is a public one. The public eID means can be used for both public and private services. Germany has a strong ID-card tradition. With a very high penetration rate for over fifty years, the eID card is a natural development in line with that tradition. Germany is developing a mobile-ID solution using the eID card and a near field communication (NFC) chip in the mobile phone to enable its use as an eID card reader.

Germany has no eID scheme with different types of credentials. It only holds public eID means (the contactless eID card) and its infrastructure. Sector specific eID solutions for one service exist and are used, but they fall outside the scope of this research. They are not interoperable. The German government is trying to phase these out and move towards one eID card.

No incident has yet taken place that led to any discussion in the German Parliament. Security and privacy are at the core design of the rollout. These have also been discussed in parliament. Although the German eID scheme can be categorized as public, private actors also play a role in the chain of operation. The private actors have tendered, and have been awarded contracts with strict and elaborate SLAs (back-to-back liability). The ‘Bundesdruckerei’ has been partly brought back under government control. The entire chain is under strict government control. The private sector is involved in delivering card readers, client software, authentication services software and mutual certification (relying on partners’ server certificates).

The public eID is closely interwoven with the citizens register at the municipal level. This is where the connections are made. No central persons register is available in Germany; nor is there a citizen PIN.

The approximate overall budget for the eID scheme in Germany is difficult to calculate because the costs of staff are not calculated in the budgets. It is an infrastructural decision, and use (number of authentications) cannot be monitored. The eID card is financed by the citizen. The price for the eID card is fixed at EUR 29.80. This includes development and maintenance costs of the system. The project costs are financed through general budget support.

It is not known how many authentications go through the German eID scheme per year, because of the lack of a central entity. The system is as decentralised as possible for IT security and privacy reasons, with approximately 150 inter-reliant third parties. Knowing the number of authentications is politically not important, and even unwanted, because of IT security and privacy reasons.

Policy considerations

Germany explicitly chose a public eID system in order to monitor privacy and safety. Its tradition with the ID card is widely accepted among the population. Therefore, the decision to work with a public eID card is a logical one, which is not seriously challenged. A demand from a supplier from the private sector has been firmly turned down.

In Germany, the provision of a means of identification, even electronic identification, is exclusively part of the public sector. This does not mean that no private parties are involved with the production. They are involved, but they all know a certain amount of government control.

The German public is used to and expects the government to provide eID for government services, parallel to the ID-card tradition. Germany does not have a history of using private entities, so this was not an option that could be considered. The use of private means was never seriously considered or discussed, although there was a brief initiative for a public-private partnership from industry, involving private branding of the cards. However, this initiative was abandoned. The decision to do so was based on historical and cultural reasons. The Germans wanted a clear separation between the public and private sector interests.

The German system does not have a single point of failure; the decentralised set-up ensures this. Only offline single points of failure are thinkable at the level of root certification authority (CA) or in the case of the destruction of the vendor.

Luxembourg

General introduction

Luxembourg is an interesting case for this study, because there is a public-private partnership in place with regard to eID. Although the eID means used to be private, public eID means have been added recently. Currently, a central identity infrastructure provides the eID card in Luxembourg. The eID system is maintained by the public CTIE (Centre des technologies de l'information de l'Etat). Certificates are provided by LuxTrust S.A., a public-private partnership that was set up in 2003 to manage the development of a common public key infrastructure (PKI) in order to secure eCommerce and eGovernment. The consortium was awarded the PKI contract in July 2006.

The progressive introduction of biometric documents in Europe forced Luxembourg to have highly secure certification services in order to protect official documents. Consequently, LuxTrust adheres to the relevant international standards in order to be in a position to protect biometric documents issued in Luxembourg.

eID scheme and means

In Luxembourg, the CTIE is responsible for the maintenance of the ID scheme. The national eID card is issued by the Ministry of the Interior. This Ministry is responsible for the public eID card. For LuxTrust's private card, the responsibility lies with the consortium that produces the private card. In case the private eID system is used and it causes an incident, LuxTrust is responsible. This company is partly owned by the state (two-thirds) and partly owned by the private sector (one-third). The responsibility is therefore shared between the public sector and the private sector.

The private and public eID systems exist in parallel in Luxembourg. The private scheme offers access to public services, but cannot be used as an (e)ID card for physical identification. This is only possible with the public card, which is mandatory for each resident citizen of Luxembourg aged 15 years and above.

As mentioned earlier, both private and public actors are stakeholders in LuxTrust, the private consortium that provides eID services (authentication, certificates, cards, etc.). Private actors are involved in all stages of the process. Liability is organised through SLAs. For the public eID card, however, only public authorities have access to the population register and personal identification numbers (PINs). When issuing private cards, other identification documents like passports and driver licences are used to validate the identity of the applicant. So when it comes to issuing eID cards, the private sector is not involved in using the population register.

Citizens of Luxembourg are able to access some public services with the private eID. However, travel identification is only possible with a public eID card. The most important difference between the public and private eID card is that the public eID card is only available to citizens of Luxembourg, while the private eID card is available to everybody. The private eID card offers more functionality for professionals (legal representation, spare versions, etc.).

Since the eID card has been introduced only in July 2014, information about recurrent budgets is not available. Development costs are also not available. However, a pragmatic approach has been used for the reuse of existing infrastructure in municipalities and for the reuse of the personalization environment for issuing passports, driver licences, etc. The fee for one public eID card is approximately EUR 14. This is seen as a real bargain, since it enables access to a range of governmental eServices. The development of private eServices is generally lagging behind. This is seen as a handicap, but can be partly explained by the very recent introduction of this scheme. The private ID card costs EUR 85, and offers extra functionality for professionals. LuxTrust also proposes one-time password (OTP) tokens for about EUR 35, which have reduced functionalities and lower security. Several banks in Luxembourg give these OTP tokens for free to their clients for web banking.

There is no governmental open standards policy in place for private eID systems in Luxembourg. Luxembourg is compliant with international standards (like ICAO).

Policy considerations

In Luxembourg, the eID system had long been managed by LuxTrust, with only private means. LuxTrust itself is a public-private partnership, with the government share being two-thirds. The choice of private means was a pragmatic one, as nothing else was available for a long time. Recently, Luxembourg started with the rollout of a public eID card, which also functions as a travel document. The card is significantly cheaper than the private solution, but offers less digital functionality for professionals. It seems like there has not been any resistance from private partners with the introduction of the eID card. Broad availability and access to as many services as possible have been the main considerations for the introduction of the public means.

The scheme in Luxembourg does not really have a single point of failure. There is a central register for issued cards. This is legally required. But it is not considered as an operationally critical element. One of the main challenges for Luxembourg's eID scheme is that the public eID system uses Java. This causes some issues with the Mac community. This is perceived as a problem. Furthermore, the ICAO chip in the national public eID card is configured so as not to allow updating of data. Therefore, information like an address change cannot be put on the card.

So far there has been no public controversy (such as a security issue) about the eID cards. The only discussion about the eID scheme is with Linux users, since the banking systems do not support Linux.

Portugal

General introduction

Portugal makes use of a public eID system for both public and private use. The citizen card is the Portuguese eID card that provides visual identity authentication with increased security. The process of authentication with biometric information has not yet been implemented, but there are some proofs of concepts. The citizen card allows the holder to provide identification when dealing with computerized services and to authenticate electronic documents. It enables holders to take advantage of a multi-channel delivery system in their interactions with public and private services.

The Portuguese electronic passport (Passaporte Electrónico Português (PEP)) represented the beginning of a new generation of eID documents in Portugal and adheres to the most rigorous security patterns. It preserves the features of the current passport in the identification of its holder, but integrates innovative devices ranging from facial recognition to the incorporation of a contactless chip. All the information contained in the chip can be read only by specialized equipment.

The digital 'key mobile' is a complementary and alternative authentication mechanism to the citizen card. It is a form of secure online authentication for citizens to the public administration. It is based on a system similar to eBanking solutions, through the introduction of username, password and a single-use code with limited validity, sent by a text or e-mail message to a mobile phone or e-mail account recorded by the citizen for that purpose.

Portugal's main objective is to make available a complementary authentication solution through mobile devices for access to electronic public services. Such solutions are safer than access via username and password (more security to the state) and simpler for the citizen (more effectiveness and efficiency to citizens and companies).

eID scheme and means

In Portugal, the Agency for Administrative Modernization (AMA) is a public institute whose mission is to identify, develop and evaluate programs, projects and measures to modernize and simplify administration; to implement interoperability among all systems; and to promote, coordinate, manage and evaluate the distribution system of public services within the policies set by the Portuguese government. The AMA defines the strategy for eID and develops and evaluates activities related to eGovernment and operates at a technical or operational level for electronic identity cards (citizen cards) and mobile digital keys. Portugal also has accredited entities within the Electronic Certification System of the State (SCEE).

Private entities are subcontractors that provide the main public eID citizen card. The Portuguese government uses a tender procedure to involve private parties in the process. The subcontracted private entities may issue qualified certificates that are legally equivalent to public eID. The essence of the Portuguese eID scheme is public, but the Portuguese government has accredited entities within the SCEE. The SCEE is an infrastructure of public keys that supports electronic signatures and other electronic security services activated by public keys (algorithms). The SCEE architecture constitutes a hierarchy of trust that guarantees the electronic security of the government and the strong digital authentication of electronic transactions among several public services and organizations, and between the government and citizens and businesses. It allows interoperability with the infrastructures that fulfil the necessary rigorous authentication requirements through adequate technical mechanisms and compatibility in terms of certification policies, primarily within the scope of the EU Member States.

The financing of the eID scheme is covered by the government budget and financial support from the European Commission. There were approximately 5,700,000 authentication processes and 114,000 authenticated users with eID in 2013. Portugal works with a mixed system of a public and private eID. To avoid any ambiguity

regarding these notions, perhaps the most relevant public eID systems in Portugal are the eID card and mobile digital key.

In Portugal, there are different ways of accessing public services with the eID card, the mobile digital key, and other means. Depending on the level of security associated with the reporting mechanism, Portuguese citizens can access different services. For example, Portugal has already finished efforts to implement services such as eAcademia, eBanking and eGov4Business of the STORK 2.0 Pilot. Portugal is planning to extend the scope to other private services (e.g., insurance, shopping) in the future.

Policy considerations

Portugal has provided its ID card with the eID functionality. This eID card replaces five other cards. Adding an eID functionality to the 'old' ID card was a logical step, because some citizens have a regular ID card that is valid until 2019, and according to current Portuguese law, there are old ID cards with a lifelong validity. Accessibility of services and the development of eGovernment and EU regulations are important considerations for implementation. There has not been any discussion about the choice for a mixed eID system. Portugal's choice was largely based on its historical evolution of information systems.

Spain

General introduction

The Spanish eID card (DNIe) makes it possible to digitally sign electronic documents and contracts, to identify and authenticate citizens in a secure digital environment and to provide them with easy, straightforward, fast and convenient access to eServices. The card is valid for ten years, but the electronic certificates contained in it must be renewed every 30 months. Over 38 million Spanish citizens hold a DNIe card. Most government bodies (central, regional and municipal) and businesses provide eServices enabling the use of the DNIe.

The multi-PKI (public key infrastructure) validation platform provides free eID and electronic signature services for eGovernment applications. The national validation platform provides a secure service to verify the status and validity of the qualified certificates, as well as the electronic signatures created by citizens and businesses in any eGovernment service. The validation platform is offered as a cloud service to national, regional and local eGovernment services, and as software to be deployed by entities with a high demand for signature services.

eID scheme and means

In Spain, the political responsibility for the national eID scheme lies with the Ministry for the Interior. Under this Ministry, the Directorate-General of Police is responsible. The Spanish eID scheme includes a public eID system with universal coverage, and a mix of other public and private systems that may be used optionally. Several private actors (technology providers) are part of the chain of operations, via tenders. The eID cards are issued at police stations.

Spain works with an eID scheme within a legal framework: the law regulates the rights of citizens for electronic means. It states which means citizens can use in order to communicate with the government. DNIe is mandatory for every public administration, but not for citizens.

For DNIe, all systems in the national eID scheme provide access to the same set of services. However, the service provider decides which other eID means, apart from DNIe, it accepts, and some regions differ. One of the main considerations for this choice is the state model with the regions. In Spain, the regions have a lot of autonomy. On a national level, there are not so many instruments to implement a common eID, only the DNIe, since it is the national identity card. Regional identity cards were considered an option. Availability was one of the main considerations. The DNIe is mandatory for the regions as well as for the national government. From the start, use by the private sector was part of the plan.

No serious incidents have taken place that led to discussions in parliament. eID was only discussed once or twice because of security reasons. If a private eID system is used and causes an incident, the liability lies with the company with the certificate. The Ministry of Interior supervises the implementation of DNIe.

The governmental open standards policy that is in place and upheld in Spain is the EU Regulation. In Spain, private parties issuing the certificates are allowed to register the PIN. The DNIe is partly financed by the general budget and partly by the fee for the card (whether the citizen activates it or not). Private eID systems do not receive any financial support from the government. There is a free market.

Under the Ministry of Finance and Public Administration, the office of the national Chief Information Officer hosts the ‘Cl@ve’ project to create an eID system based not on certificates, but on shared keys.

Policy considerations

In the Spanish context, the ‘reach’, or availability to all citizens, of an eID means was an important consideration for the decision to work with a public eID system. The federal government had limited competences regarding the regions. Therefore, the national (e)ID card is the only option to guarantee availability. But activation and use are disappointing. For this reason, mobile ID is also being considered.

In Spain, the law allows multiple eID means. The national eID means is the eID card. But there is an alternative eID system (allowed by the law) that consists of a combination of public and private eID means based on electronic certificates and it is being used more often. Because the costs are calculated in different ways (the costs of the national eID means are paid by the citizen and the costs of the transactions through the alternative systems are sometimes paid by the citizen when the electronic certificate is issued, and sometimes paid by the service provider when validating those certificates), there are regions that do not accept some of these eID means. Within this eID scheme, there is a discussion about the balance between public and private means, because the public eID certificate is issued for free and therefore competes with private eID means.

Furthermore, Spain (just like France) is working on a federation project in order to combine the different username-password systems that are active for the supply of government services to one solution (the Cl@ve project).

At the introduction of the eID scheme, there has been discussion regarding the choice for a mixed eID scheme. Topics that were discussed were DNIe, the Royal Mint and which scheme should be used to register for eIDAS. The competition between the Royal Mint and private issuers also became a discussion. The Royal Mint does not charge citizens; it charges service providers. Private solutions charge the citizen. Some regions are reluctant to accept Royal Mint certificates, because they charge the service providers, and these providers do not want to bear those costs.

In Spain, the single point of failure is the platform for validation. There are two platforms in different data centres, operated by two different public bodies (one by the Ministry of Finance and Public Administration, the other by the Royal Mint).

Sweden

General introduction

Sweden makes use of a private ID system. The private eID means can be used for public and private services. Most Swedish citizens make use of private means in order to access government services. Sweden's eGovernment is very developed. In October 2005, the Swedish government introduced the 'official' electronic ID card containing biometric data. This 'national identity card' (nationellt identitetskort) is not compulsory and does not replace previous paper ID cards. It can be used as a proof of identity and citizenship and as a valid travel document within the Schengen area. It complies with ICAO standards for biometric travel documents; it is issued by the passport office and is manufactured by the same supplier as the biometric passport. The contactless chip not only contains a digital picture of the holder, it also has a traditional chip that may be used to securely access eGovernment services in the future.

Swedish citizens use non-official electronic ID cards issued by Swedish Post, software-based electronic IDs like the Bank ID (developed by the largest Swedish bank) and Steria eID to access certain eGovernment services. Any physical person with a Swedish personal identification number (PIN) can obtain an eID. This number appears on the eID and its microchip.

Legal entities can also use an eID. In this case, two types of certificates come into question, namely the server and stamping certificates for authentication and signing, respectively. The certificates contain the name of the organization and the organizational number and may also contain a URL. The contact person ordering organizational certificates must have an authorization for this purpose from a person authorized to sign on behalf of the organization.

Furthermore, Steria has introduced a new type of eID in Sweden: an organizational certificate for personal use. This type of certificate contains the organizational number, the name of the organization, as well as the name and the role of the person. It is worth mentioning that none of the organizational eIDs contain a PIN, since it is considered to be sensitive information.

As the eIDs are issued by different suppliers, the authority that provides eServices must be able to authenticate users, verify eSignatures and apply for revocation checks in different ways and towards different eID suppliers.

eID scheme and means

In Sweden, a small agency is responsible for the rollout of eID. It is connected to the tax agency, but it is a separate legal entity. It operates under a board made up of private and public high-level figures. In Sweden, the agencies do not have a political responsibility even though they receive their budgets from the government. The ministries can cut budgets and relieve heads of agencies, and they are held responsible if anything goes wrong. As mentioned earlier, the eID means that are most used are private (banks) with STORK QAA level 4. The Swedish government pays a fee per authentication. Several authentications for the same service in one month are calculated as one. Out of nine million Swedes, five million use an eID. Earlier, the Swedes 'bought the means' (certificate), now they buy the 'validation control'.

No incident that led to discussion in parliament has taken place yet. The Swedish eID system is a private one. In case a private eID system is used and causes an incident, the (non-political) responsibility lies with the agency, and the liability lies with the companies offering the validation. In case a private eID system is used and causes an incident, the company that offers the validation is responsible. This is organised through contracts and SLAs.

In Sweden, there is no governmental open standards policy in place and upheld for the private eID system. Every identity provider can use its own system as long as it uses the prescribed identity insertion. This is mandatory in the scheme and makes the broker function redundant. The Swedish eID scheme is open to all

providers that follow the framework guidelines. The private eID system makes use of a public persons register and the PIN. Privacy considerations are not deemed important. It also includes address information.

The current approximated yearly budget for the eID scheme is EUR 2.5 million. As of July 2016, a new financial scheme will be implemented. This relies on a monthly fee per user for validation per government organization; the cost is set at 25 cents. This fee is slightly higher than the 22 cents paid for the validation control by the government to the validation providers, the difference covering organizational costs.

Private eID systems do not deliver a direct financial contribution to the eID scheme. However, issuing goes via the banks and initial investments in the infrastructures. Approximately 300 million authentications per year go through the national eID scheme (of which approximately 80 million are for government services).

Policy considerations

The most important policy considerations for the setup of the eID scheme in Sweden were technical. The Swedish government was hesitant to take technical responsibility and chose a pragmatic model. The government has introduced standards and tests these standards, which include an open market for private (and public) suppliers of eID means. If a party meets the standards, it can join the system.

The exclusion of citizens (not having eID means produced by private actors) was not considered a great risk, but in 2006 the electronic citizen card was enabled in the scheme to further manage this risk. De facto, banking authentications mostly dominate the system. There were no cultural issues concerning the trustworthiness of banks. Not even during the banking crisis.

In Sweden, it is normal for personal data and numbers to be used frequently by different government organizations. Moreover, banks are very much trusted, even in times of crisis. Although the banking solution did not completely cover the eID issue, it was practical and offered a quick take-up. With the upcoming introduction of an eID function on the eID card in 2016, a solution has been found for the issue. Based on considerations such as inclusion, it has been decided to make it possible to also use the public ID card as an eID means. With that decision, a public carrier has been added to the eID system, which thus became a mixed system de jure. In fact, the actual transactions are largely transactions that go through banks

The Swedish eID scheme does not have single points of failure, because there are several means that can be used as an eID. Challenges for the Swedish eID scheme are that working with many actors automatically means that the process needs much coordination. Also, the transition from old to new eID infrastructures is seen as a challenge. The model that was chosen in Sweden stimulates competition and innovation. An important consideration regarding this choice was the fact that all banks participated in the model and, therefore, the penetration rate of eID was very high in society. For the banks, eID created higher customer value and lowered the costs of their eID systems.

United Kingdom

General introduction

The United Kingdom was included in this study, because it is an important actor in Europe, with an explicit, private strategy for eID means. The private eID means can be used for public services.

GOV.UK Verify is the new way to prove who you are online. It replaces the 'Government Gateway' as the main identification platform and a central registration and authentication engine. GOV.UK Verify means people will be able to access their government records and services securely and safely, without having to use postal or face-to-face services.

GOV.UK Verify is a new service, being delivered in a new way for the first time anywhere in the world. The UK is working to establish a new market of identity assurance services. Setting up GOV.UK Verify has enabled the UK to aggregate demand for identity assurance services across the central government. It is therefore able to attract the required interest and investment from the market.

Rather than the government seeking to verify individuals' identity online and manage their login credentials, the UK is using a range of certified companies that users can choose from. The certified companies operate according to published governmental standards. The five contracted certified companies are:

- Experian (joined GOV.UK Verify public beta in October 2014)
- Verizon
- Digidentity (joined GOV.UK Verify public beta in December 2014)
- The Post Office
- Mydex

The UK has procured services, not specific technology or processes. This is how the UK supports the development of a diverse marketplace of providers and takes advantage of innovation and the unique capabilities of different providers.

eID scheme and means

In the United Kingdom, the Minister for the Cabinet Office holds political responsibility for the national eID scheme. eIDs are issued by different private parties. They check a person's identity using a range of sources of evidence, held in both the private sector and the public sector. That evidence may include passports, driving licences, credit reference information and, in order to establish identity remotely, possibly also facial recognition on passports and driver licences. These private parties need to meet certain requirements set by the government and they need to be certified by an accredited body. The Cabinet Office runs a central hub to connect eID providers.

Liability is set out in the contract between the identity provider and the cabinet office — essentially, as long as the identity providers are doing everything required by the standards, they will not be at fault. No incidents have yet taken place that led to any discussion in parliament.

The United Kingdom spends tens of millions of pounds on the national eID scheme. The financial costs are covered by the general budget and by a budget related to cyber security.

At present, all private eID means provide access to the same set of services.

Policy considerations

The UK government wanted to keep in mind the privacy discussion while deciding to develop a private eID system. The government wanted to reduce the risk of there being a perception of a ‘Big Brother’ state.