COMPETITIVENESS AND INNOVATION FRAMEWORK PROGRAMME

ICT Policy Support Programme (ICT PSP)

Towards pan-European recognition of electronic IDs (eIDs)

ICT PSP call identifier: ICT-PSP/2007/1
ICT PSP Theme/objective identifier: 1.2

Project acronym: STORK

Project full title: Secure Identity Across Borders Linked
Grant agreement no.: 224993

D2.2 – Report on Legal Interoperability

Deliverable Id :	**D2.2**
Deliverable Name :	**Report on Legal operability**
Status :	**Final**
Dissemination Level :	**Public**
Due date of deliverable :	**M7**
Actual submission date :	**24 February 2009**
Work Package :	**2**
Organisation name of lead contractor for this deliverable :	**Dutch Ministry of the Interior and Kingdom Relations**
Author(s):	**Ronald Leenes, Bart Priem, Carla van de Wiel, Karolina Owczynik**
Partner(s) contributing :	**AT, BE, DE, ES, FR, IC, IT, NL, LU, PT, SL, SE, UK**

Abstract: This deliverable provides an overview of the legal background of eID in 14 STORK Member States and describes the principle legal issues regarding pan Erurοpean authentication.

Project funded by the European Community under the ICT Policy Support Programme

History

Version	*Date*	*Modification reason*	*Modified by*
0.1	22/09/08	Initial version containing draft NL and UK sections	Ronald Leenes, Bart Priem
0.2	06/11/08	Included draft sections on Austria, Belgium, Germany, Iceland, Estonia, Italy, Portugal, Sweden	Bart Priem, Carla van de Wiel
0.3	07/11/08	Included input from Estonia, Sweden, Slovenia, Iceland, Italy, France, Portugal,	Carla van de Wiel
1.0	25/11/08	Draft deliverable, included overall analysis	Ronald Leenes
1.0b	08/12/08	incorporated feedback from Luxembourg, France, Slovenia and Spain on draft v1	Ronald Leenes
1.0c	12/01/09	Incorporated feedback from Belgium, Iceland, Slovenia, Sweden, wp 2.2 meeting 11 Dec 2008. Incorporated UK report.	Ronald Leenes
1.0 final	23/02/09	Incorporated German comments	Ronald Leenes

TABLE OF CONTENTS

List of figures

List of tables

Executive Summary

The objective of the STORK project and Work Package 2 is to make it possible and uncomplicated to access online public services across the borders in the European Union. It focuses on mechanisms and infrastructure that enable European citizens to identify oneself by using an authentication system.

Deliverable 2.1 proposed an analysis of the authentication solutions adopted by member states, and suggest a technical solution for EU interoperability. Countries share the understanding of a set of level of authentications based on a STORK quality assurance levels scheme. Interoperability is reached after mapping national recognized levels into the STORK-QAA.

Limited to the current status of eID schemes, this deliverable analyses the legal provisions that apply to authentication in the various consortium Member States. Authenticate means, among others, to verify the authenticity of an identity. This deliverable includes issues in the field of the legal grounds behind the national eID structures, the different characteristics and the legislation behind the national eID structures and a description of its consequences for pan-European interoperability. It focuses on mechanisms and infrastructure that enable EU citizens to register and authenticate them.

However, it is not the objective of this deliverable to provide an exhaustive list of legal issues in the field of interoperability. The purpose of this deliverable is to provide an analysis that can serve as a framework for the legal requirements for pan-European eID.

ACKNOWLEDGEMENTS

This Deliverable would not have been drafted without the input from several partners in the STORK project. For the drafting of the country reports, we would like to thank the following partners that provided indispensable information for our analysis:

- Hubert Schier for Austria
- Frank Leyman for Belgium
- Tarvi Martens and Katrin Laas for Estonia
- Jose Fernando Carvajal Vión for Spain
- Martine Schiavo for France
- André Braunmandl for Germany
- Stefano Fuligni, Giovanni Manca and Roberto Pizzicannella for Italy
- Haraldur Bjarnason and Kári Ólafsson for Iceland
- Pierre Clausse for Luxemburg
- Ronald Leenes for the Netherlands
- André Vasconcelos and Fátima Carrão for Portugal
- Davorka Šel, Aleš Pelan, Brane Kren and Katarina Čepon for Slovenia
- Arvid Welin for Sweden
- Neil Clowes, Jim Purves for the United Kingdom.

Moreover, several results from previous European studies in the field of electronic Identity have provided valuable input to this document. In particular, we mention the IDABC studies on ‘Mutual recognition of eSignatures’ and ‘Interoperability for PEGS’[1]. In addition, the country reports provided on the website of the ModinisIDM-project[2] were useful, just as the eGovernment factsheets and other information that is provided by the European Commission’s eGovernment portal www.ePractice.eu

[1] Which can be retrieved from the website of the IDABC on http://www.europa.eu.int/idabc/ (last accessed October 24, 2008)

[2] See: https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/bin/view.cgi (last accessed October 24, 2008)

ABBREVIATIONS

A2A	Administration to Administration
A2B	Administration to Businesses
A2C	Administration to Citizens
AA	Authentication Authority
AP	Attribute Provider
CA	Certification Authority
CRL	Certificate Revocation Lists
CSP	Certificate Service Provider
eID	Electronic Identity
IdP	Identity Provider
IDM	Identity Management
PEGS	Pan-European eGovernment Services
OCSP	Online Certificate Status Protocol
OTP	One-Time Password
PIN	Personal Identification Number
PKCS	Public-Key Cryptography Standards
PKI	Public Key Infrastructure
PUK	Personal Unblocking Key
SP	Service Provider
SA	Supervision Authority
SOAP	Simple Object Access Protocol
SCVP	Server-based Certificate Validation Protocol
SSCD	Secure Signature Creation Device
USB	Universal Serial Bus
TTP	Trusted Third Party
TSA	Time Stamp Authority
TST	Time Stamp Token
VA	Validation Authority
XAdES	XML Advanced Electronic Signature
XML	eXtensible Markup Language
XML-DSIG	XML Digital Signature

Glossary

This document does not contain a glossary, as WP2.2 does not aim to impose any definitions at this point in the STORK-project. In stead, definitions are explained in the text of the document. However, the deliverable aims to contribute to the elaboration of a glossary that is to be drafted during the STORK-project, on the basis of a project-wide discussion and on the definitions provided in other studies, like the ModinisIDM study and the IDABC study on eID interoperability for PEGS.

PART I: INTRODUCTION

1 Overview and introduction

The STORK project aims to make it easier for EU citizens and businesses to access online public services across borders. However, the project does not aim to impose a single eID solution but tests and develops common specifications for mutual recognition of national electronic identities (eID) between participating countries[3].

Part of the STORK project is the Work Package 2 (Wp2), which focuses on 'the interoperability of Trust applications in the various participating consortium members'[4]; it includes an analysis of the possible technical and legal issues in the field of eID interoperability. The legal analysis is reported on in this deliverable (D2.2). Besides this deliverable, the work package also comprises a 'Framework mapping of technical/organisational issues to a quality scheme (D2.1), and a 'Quality authenticator scheme' (D2.3).

1.1 Objective of the deliverable

The purpose of this deliverable is to analyse the legal provisions pertaining to authentication in the various consortium Member States. The deliverable provides an overview of the legal rationale behind different national eID structures, a description of its consequences for pan-European interoperability, and an elaboration of possible solutions for pan-European interoperability5. This deliverable can serve as a foundation for legal requirements for pan-European eID. However, due to the fact that many eID schemes are still under construction, it is not the objective of the deliverable to provide an exhaustive list of legal issues in the field of interoperability.

1.2 Scope

The STORK project and Work Package 2 approach eID interoperability from the perspective of authentication mechanisms. Hence, this deliverable focuses on mechanisms and infrastructure that enable EU citizens to register and authenticate themselves instead of putting the focus on, for example, back office integration of the Administration.

Interoperability, in this deliverable, mainly comprises the possibility of a citizen from a country to use the authentication system from this country to have access to an application in another country[6].

Authenticate means, among others, to verify the authenticity of an identity. The concept of identity is difficult to formalize; it may concern individual, sociological, or cultural dimensions. This deliverable focuses on digital or electronic identities, which are composed by a set of *information (data)* about an entity, and an *identifier* that can uniquely point out this (relatively static) set of information (data).[7]

Identity is not a monolithic concept. Individuals have different partial identities[8] used in different contexts; for example, an individual can be a Dutch citizen, an employee of Tilburg University, a specific avatar in Second Life. He may also have different accounts on the various social network sites, a loyalty card, and a master card. For each of these situations the same citizen uses different digital identities.

Digital identities (and identifiers) can be constructed and issued by different organisations like the telephone company, the Internet provider, a social network site, or an insurance company.

[3] Cf. http://www.eid-stork.eu/, last accessed 22 September, 2008.

[4] STORK Description of Work

5 As mentioned in the STORK Description of Work, p.110

[6] Cf. http://ec.europa.eu/idabc/servlets/Doc?id=30989, p. 14

[7] Cf. D2.1: Inventory of Topics and Clusters on www.fidis.net

[8] Cf. D2.1: Inventory of Topics and Clusters on www.fidis.net; D14.1.c Framework v3 on www.prime-project.eu

When discussing interoperability of eID in this deliverable, we refer to the 'formal' electronic identities, which are the *identities that are constructed out of identity information (attributes), and are recognized by national governments, for application (especially for authentication) in national eGovernment services* (and sometimes in private services as well). Such formal identities may be stored on smart cards or other devices but may also be received from a central authority during an authentication process.

Typical use cases of an interoperable eID are when a citizen of country X can use the electronic identity and authentication scheme of his or her home country for a license application, or when a student from country Y can register for a scholarship in country X with her home authentication scheme, without a need to register herself in country Y.

1.2.1 Scope of legal analysis

The legal analysis in this document comprises a description of the models of the most promising electronic eID schemes of the partners in the STORK project. As it is not possible to carry out a legal analysis without knowing the characteristics of an eGovernment/eID model, the legal analysis is founded by a general description of the Member State’s decisions in the field of eGovernment and a description of the components of the eID model.

Bearing in mind that the resources and time for the deliverable are limited and given the fact that multiple eID schemes are still under construction, it is difficult (if not impossible), to give an exhaustive overview of all the legal interoperability-issues that can arise when national eIDs are being used in a pan-European context. Therefore, this deliverable will mainly focus on the most determinative characteristics of a National eID model, the legal aspects of these characteristics, and their impact on interoperability. In particular this means that the following aspects have been examined:

- Characteristics of the eID, e.g., the terms and conditions for use by the citizen and a relying party, use and exchange of attributes and identifiers, and requirements for obtaining and constructing an eID;
- The Authentication Authority, e.g., are parties obliged to make use of such an authority, how can they connect to the authority, are there terms and conditions, etc.;

1.2.2 Countries

The legal analysis in this deliverable is confined to countries which are represented by partners in STORK, which are: Austria, Belgium, Germany, Estonia, Spain, France, Italy, Iceland, Luxembourg, The Netherlands, Portugal, Slovenia, Sweden, and the UK.

1.3 Target audience

The deliverable is mainly drafted to serve as an input for the other deliverables to be developed in STORK. For example, the document serves as a foundation for deliverable D2.3 (Quality Authenticator Scheme). Moreover, the deliverable provides input for STORK Working Package 4 and Working Package 6.

The deliverable may also provide support to decision makers in the field of electric Identity (both on National as pan-European level). The report can also be interesting to professionals and students that are interested in eID and IDM.

1.4 Overall Methodology

The first step for D2.2 was the analysis of the related work concerning the topic of the deliverable. This includes the IDABC reports and the related work includes (but it is not limited to) the project proposal and the (drafted) documents of the work packages that are related to work package 2 (namely work packages 4, 5 and 6).

The second step was to prepare a questionnaire and distribute it among the member states. The aim of the questionnaire was to collect relevant and updated information concerning the following issues: The legalisation of the systems the member states use for their authentication mechanism. So, based on a list of high priority questions for deliverable 2.2 the questionnaire was sent out to all WP. The partners were asked to answer the questionnaire for their country report. The answers has been taken into account and after having finished all separated country reports the final draft has been created and sent to all WP partners with request for comments. The received comments have been processed and the document has been adapted.

On the 9th of October MOI and MAP organised a WP2 meeting in Madrid and some fundamental issues for D2.2 were discussed on the basis of the first draft. After this meeting the partners were given a week for finalising their country reports and the results from D 2.2. In December at the STORK general meeting in Brussels preliminary results were presented and another meeting of WP2 was held at that time to finalize the deliverable. One of the consortium-memberstates was then in the process of revising their legislation. In communications of the WP leader with the memberstate a solution was reached in including their remarks on their position early February.

1.5 Risk management

According to the STORK Quality Management plan, each deliverable/task has to follow the agreed quality management process and has to be accompanied by a risk analysis. The following tables comprise the identified risks for this deliverable. According the structure of this deliverable the risks are divided into general risks affecting the whole task 2 of WP2 and risks affecting the individual work items only.

The following template was used for the risk analysis:

Threat	Description of a potential danger towards the project.		
Consequence	Description of the negative effect the threat can have towards the project.		
Measure	Description of the measures that can be taken to prevent a threat from happening or to reduce negative effects.		
Chance (C)	Measure defining the likelihood of a threat to happen. The chance is determined as follows:		
	HH	Very High	the threat has very high likelihood to happen (more than 80%)
	H	High	the threat has high likelihood to happen (from 60% to 80%)
	M	Medium	the threat may possibly happen (from 40% to 60%)
	L	Low	the threat has low likelihood to happen (from 20% to 40%)
	LL	Very Low	the threat has very low likelihood to happen (less than 20%)
Impact (I)	Measure of the negative effect on the project. The impact is determined as follows:		
	H	High	The impact is high; substantial measures are required.
	M	Medium	The impact is medium.
	L	Low	The impact is low; few measures are required, usually easily manageable.

<table>
<tr>
<td><b><i>Risk (R)</i></b></td>
<td>Risk = Chance * Effect, representing the priority. The risk is determined using the following table.
<table>
<tr><th></th><th></th><th colspan="3">IMPACT</th></tr>
<tr><th></th><th></th><th>H</th><th>M</th><th>L</th></tr>
<tr><th rowspan="5">CHANCE</th><th>HH</th><td>HH</td><td>HH</td><td>H</td></tr>
<tr><th>H</th><td>HH</td><td>H</td><td>M</td></tr>
<tr><th>M</th><td>H</td><td>M</td><td>L</td></tr>
<tr><th>L</th><td>M</td><td>L</td><td>LL</td></tr>
<tr><th>LL</th><td>L</td><td>LL</td><td>LL</td></tr>
</table>
HH means very high priority, H high priority, M medium priority, L low priority and LL very low priority.</td>
</tr>
</table>

1.5.2 Identified risks

The following talbe defines general risks that apply for this deliverable.

Threat	Consequence(s)	Measure(s)	Chance	Effect	Risk
Few MS-assurance levels cannot be mapped onto STORK Assurance levels	*Limited eID interoperability between the MS.*	▪ Review by WP2 • acceptance of the WP2 results by MS, will come back in 2.3	*M*	*H*	*H*
Most MS assurance levels cannot be mapped onto STORK Assurance levels	*No eID interoperability between the MS.*	• Review by WP2 • acceptance of the WP2 results by MS, will come back in 2.3	*L*	*H*	*M*
Stork-levels are not adopted in the project	*Delay of the project and this may lead to short term, ad-hoc based solutions for eID interoperability. WP6 may, in the absence of assurance levels, define their own levels for the pilots.*	• Involve all partners and take input seriously in order to achieve consensus • Accept D2.1, D2.3 as project standards • Use these standards in the review process of the results of other Work packages	*M*	*H*	*H*
Member states deliver incorrect or incomplete information	*May result in incorrect mapping of the STORK assurance levels. These member states may not be able to participate in the pilots*	• Review by WP2-members and all other consortium MS.	*M*	*M*	*M*
MS do not recognize their contributions in	*May delay the delivery of the assurance level mapping framework for STORK.*	• Review by WP2-members and all other consortium MS.	*L*	*M*	*L*

D2.2					
Providers do not accept the STORK-assurance levels.	*Limited eID interoperability between the MS. No eID interoperability between the MS.*	- MS take responsibility in this. - Monitoring during the pilot phase	*M*	*H*	*H*

Table 1: General Risk List.

1.5.3 Materialized risks

The risk that actually materialized was a slight delay in returning feedback on the first draft of the deliverable. The work package leader managed this situation by sending a reminder and by extending the actual deadline for feedback.

1.7 Quality Management

1.7.1 Acceptance criteria

The acceptance criteria used to evaluate the quality of the deliverable are defined considering the following parameters:

- Deliverable - a description of the deliverable.
- Acceptance criterion – a description acceptance criterion.
- Norm – a description of the norm that is applied to measure conformance.
- Process – a description of the process that is used to test conformance.
- Priority – the priority to meet a acceptance criterion (Low = nice to conform to, Medium = important to conform to, High = necessary to conform to).

1.7.2 The process

The following table reports the criteria adopted for deliverable D2.3 and the ensuing results.

Deliverable	Acceptance criteria	Norm	Process	Priority	Checked
Deliverable 2.2, as mentioned in the DoW	*Conform to STORK template*	*Template issued by QM on 25-11-2008*	*Checked against template.*	*high*	*Yes*
	Language & Spelling	*English (UK)*	*Reviewed by native speaker.*	*high*	*Yes*
	Each member state op wp 2 and wp 6 (pilots) are represented in deliverable 2.2	*Use the same questions for each member state to inventoried the systems they use on a national level*	*Check against sending an e-mail.*	*high*	*Yes*
	Consistency with description in DoW	*DoW version 1.5*	*aligned with DoW.*	*high*	*Yes*
	Contents is fit for purpose	*DoW version 1.5*	*Reviewed by WP2 en WP-leaders*	*high*	*Yes*
	Contents is fit for use	*DoW version 1.5*	*Reviewed by WP2 en*	*high*	*Yes*

			WP-leaders		
	Commitment within WP	*DoW version 1.5*	*Reviewed by WP2 en WP-leaders.*	*high*	*Yes*
	Delivered on time	*Planning for the Work Package*	*Final draft wasl discussed by WP2, Brussels, the 10th of December.*	*High, deadline is 17/12*	*Yes*
Deliverable 2.2, as mentioned in DoW	*Content of D2.2 satisfies to the edge conditions for starting WP2.3*	*DoW version 1.5*	*Reviewed by WP2 en WP-leaders*	*high*	*Yes*

Table 2: Acceptance criteria list and results.

1.6 Reading guide

Part I provides a general overview of the relevant concepts and models on which our legal analysis is based.

Part II contains the general analysis of the legal issues; it starts with an elaboration of the relevant European policies relating to (pan-European) electronic identities. Next it provides an overview of the most relevant European legislation in the field of eID. Finally we will bring together the conclusions to be drawn from the relevant European legal frameworks, as well as the results from the analysis of the country reports.

Part III contains the detailed country report. The report consists of an inventory of the different national eID models, completed by an elaboration on the legal decisions and regulation behind these national eID structures.

1.7 Related work

The STORK project operates in a highly dynamic environment in which technical developments succeed each other rapidly and many eID related research-projects are being carried out. Without providing an exhaustive overview, we would like to mention the following initiatives.

- The Modinis IDM project[9]
- The Porvoo Group[10]
- The Guide-project[11]
- The PRIME and PrimeLife research project[12]
- The FIDIS research project[13]

[9] https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/bin/view.cgi/Main/WebHome

[10] http://porvoo14.dvla.gov.uk/group.html

[11] http://istrg.som.surrey.ac.uk/projects/guide/

[12] https://www.prime-project.eu/; http://www.primelife.eu/

[13] http://www.fidis.net/

Moreover, the STORK project is closely related to European policy in the field of eGovernment, like:

- The Ministerial declarations of Manchester and Lisbon[14]
- The i2010 eGovernment Action Plan[15];
- The European Commission's website www.ePractice.eu, and ;
- The work that results from the IDABC programme[16] amongst which the 'eID interoperability for PEGS' study, the 'Signposts paper towards eGovernment 2010' and the 'Roadmap for a pan-European eIDM Framework'.

[14] Manchester Ministerial declaration of 24 November 2005; Lisbon Ministerial declaration 19 September 2007

[15] (COM(2006) 173 final), see:

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0173:FIN:EN:PDF

[16] http://ec.europa.eu/idabc

2 eID and the pan-European eID perspective

2.1 The European eID interoperability framework

The STORK project is one of many initiatives in Europe regarding eGovernment and eID. The necessity for interoperable eIDs has been recognised in the i2010 eGovernment Action Plan that follows the 2005 Manchester Ministerial Declaration, in which interoperability and electronic identity are defined as "key enablers" for eGovernment in general. Interoperable eIDs are considered essential for achieving the freedoms of goods, services, capital, and services. An example of the necessity of interoperable eID can therefore also be inferred from the Services Directive (2006/123/EC), which inter alia states that:

" [...] all procedures and formalities relating to access to a service activity and to the exercise thereof may be easily completed, at a distance and by electronic means [....]" (Art 8 (1), Directive 2006/123/EC, emphasis by author)

Apart from realizing and facilitating an internal market, interoperable eIDs are considered necessary for reducing administrative burden throughout Europe, which can lead to a better competitive position of the EU-zone as a whole.[17] Interoperable eIDs contribute to achieving the objectives of the Lisbon Agenda.

In addition to the Manchester and Lisbon Ministerial declarations[18] and the i2010 eGovernment Action Plan[19], the interoperability of eID is elaborated in the Signpost Paper[20] and the eIDM Roadmap[21]. These documents describe the targets for electronic identification and authentication in Europe. Key ideas in the Signpost paper are:

- Electronic identity and digital identity cards are separate concepts;
- Respect for a high level of data protection in all handling of data by third parties;
- A citizen-centred approach that underlines personal control even if stewardship over personal data lies at another party[22].

Furthermore, according to the signposts paper, the EU policy framework regarding eID should be:

- Federated and multilevel;
- Based on policies and mutual recognition of national electronic identities[23];

Many of the ideas that were described in the Signposts paper are reflected by the eIDM Roadmap. In addition, this roadmap notes some complementary design criteria for a pan-European eIDM system:

- Reliance on authentic sources;
- Permitting a context/sector based approach;

[17] Cf. Commission of the European Communities. (2005). Working together for growth and jobs. A new start for the Lisbon strategy (No. COM (2005) 24).

[18] Ministerial eGovernment Conference. (2005). Ministerial declaration. Manchester, UK; 4th Ministerial eGovernment Conference. (2007). Ministerial declaration. Lisbon, Portugal.

[19] COM(2006) 173 final

[20] eGovernment Unit. (2005). Signposts towards egovernment 2010: European Commission Directorate General Information Society and Media.

[21] eGovernment Unit. (2006). A roadmap for a pan-european eidm framework by 2010, v 1.0.

[22] eGovernment Unit. (2005). Signposts towards egovernment 2010: European Commission Directorate General Information Society and Media, p. 31

[23] eGovernment Unit. (2005). Signposts towards egovernment 2010: European Commission Directorate General Information Society and Media

- Enabling private sector uptake.[24]

The European eID framework mentioned in the Roadmap needs to serve as a quality mark. In addition, it pays attention to the policy objective of ‘leaving no citizens behind’[25], by addressing the possibilities of *intermediaries management and delegation*.

The Roadmap notes that the principle of subsidiarity needs to be taken into account, and that it is not aimed to impose any technical, organisational, or legal infrastructural choices to Member States[26]. Nevertheless, the Roadmap does state several key principles for a *pan-European* system:

- Usability considerations should be the most pervasive design constraint when creating a pan-European eIDM framework.
- Each Member State should be able to identify users within its borders, if it wishes to allow them access to eIDM services abroad. To this end, the consistent use of suitable identifiers is a necessity.
- Each Member State should issue the means to each user to identify and authenticate himself electronically, if it wishes to allow him access to benefit from eIDM services abroad.
- With regard to mandate/representation authorisations, each Member State should provide the means to manage the competences of the identified users within its borders.
- Each Member State should support online validation mechanisms of identities, competences and mandates, if it wishes to provide eIDM services.
- High-level consensus must be established between Member States on an eIDM terminology in order to guarantee conceptual/semantic interoperability. Appropriate policy and legal measures can be used to corroborate this consensus.[27]

The principles and design criteria for a pan-European eIDM framework do not oblige member states to design or adjust a particular eID system, but it needs to be mentioned that the above described policies can serve as one of the useful tools for assessing national eID initiatives and for the development of interoperability solutions.

2.2 The eID authentication process[28]

Another useful tool for an eID assessment is an overview of a standards eID process, its relevant actors, and its actions. The following description of the eID authentication process provides such an overview and serves as a foundation for the analysis of the national eID schemes in the country reports.

In the light of the target of the STORK project an important component of electronic Identity is the *authentication process*, in which an entity (the citizen) (1) registers for an electronic identity and subsequently (2) proves his or her claims in front of others in the electronic environment. The following description of the authentication process is based on a model described in an earlier study conducted

[24] Cf. The eGovernment Unit. (2005). Signposts towards egovernment 2010: European Commission Directorate General Information Society and Media; eGovernment Unit. (2006). A roadmap for a pan-european eidm framework by 2010, v 1.0.

[25] Cf. the i2010 eGovernment Action Plan (COM(2006) 173 final)

[26] Cf. Roadmap to a pan-European interoperability framework, p. 3

[27] Cf. Roadmap to a pan-European interoperability framework, p. 3 -4

[28] We note that the STORK description of work (DoW) uses different terminology from that of IDABCS. STORK has Identity provider (IDP) instead of CSP, and Service Provider (SP) instead of Relying party. Moreover, STORK recognizes the Attribute Providers (AP), the entities who provide attributes about the user (e.g., age, gender). The remaining of the document adopts the STORK terminology.

by the IDABC in 2007.[29] This model has also been used in a previous STORK Deliverable: ‘D2.1 Framework mapping of technical/organisational issues to a quality scheme’.

As mentioned, the authentication process is composed out of a registration phase and an electronic authentication phase. In the first phase, the registration phase, an entity acquires a (electronic or physical) token for instance a username or certificate for authentication. Normally, acquiring the electronic identity will occur at a government institute of this entity’s domicile. In the registration process, the citizen needs to claim that he or she is entitled to obtain an electronic identity (e.g. by providing a passport) at an authority (e.g. a municipality). The registration phase is characterised by ‘Identity Proofing’ (ensuring that an identity corresponds to a real entity), and ‘Token and Credentials delivery’ (the provision of a token and credentials to be used in an electronic authentication protocol).[30]

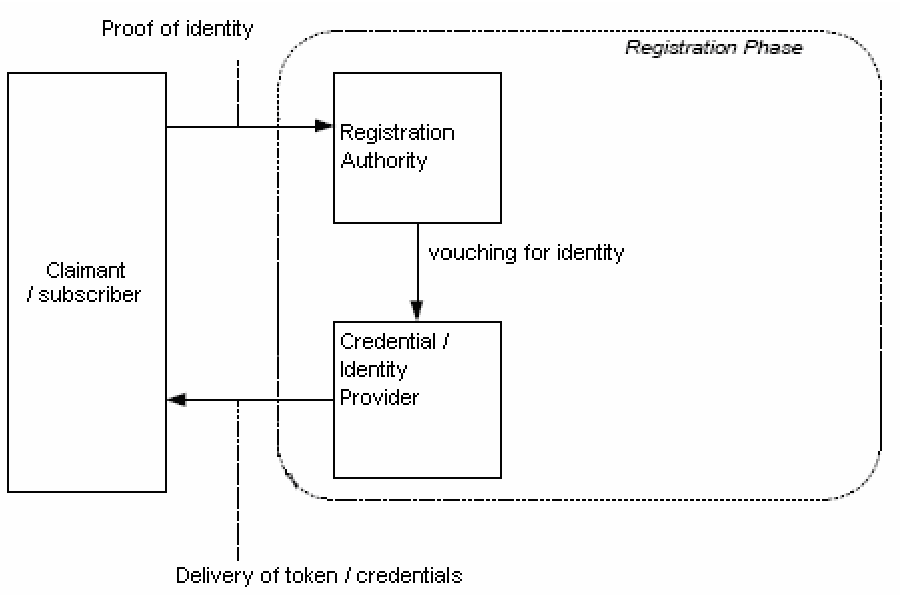

Figure 1: Registration phase (source IDABC 2007).

The second phase is the electronic authentication phase (figure 2). In this stage, the claimant (or a representative that has a mandate to operate on behalf of the claimant), uses the token and credentials obtained in phase one, e.g. for access to an eGovernment service (in this case, a relying party, because this service depends on the correctness of the eID). If the relying party cannot verify the used eID by himself, an authenticating authority will need to assure the relying party that the used eID belongs to the claimant and is authentic. On success, the claimant will then be authenticated and usually, this will lead to an authorisation part (figure 2, in orange) in the process where access to particular resources is handled on the basis of the rights of the produced eID.

In an international context, the relying party can be an organisation that is situated in a Member State that is not the Member State that has assigned the electronic identity. In such a situation, this relying party may need to verify the eID at the authentication party in another Member State. Hence, cross border transfer of an eID can occur between the claimant and the relying party and between the relying party and authenticating authority.

[29] Graux, H. and J. Majava (2007b). Proposal for a multi-level authentication mechanism and a mapping of existing authentication mechanisms. eID Interoperability for PEGS, IDABC.

[30] Cf. STORK D2.1., p. 10

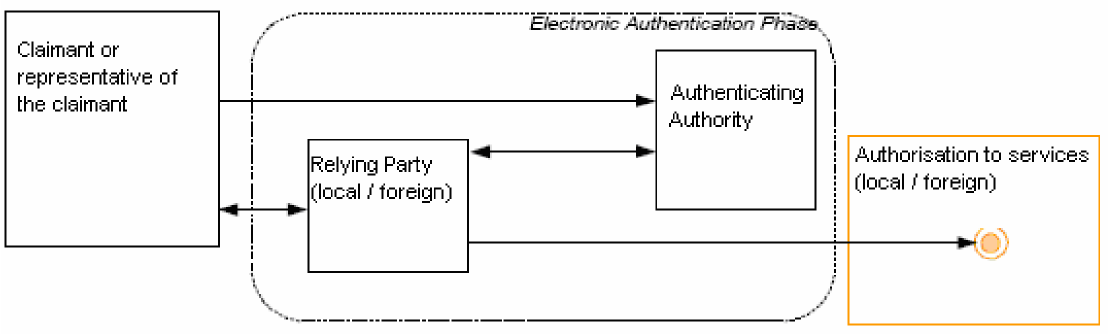
Claimant or representative of the claimant
Electronic Authentication Phase
Authenticating Authority
Relying Party (local / foreign)
Authorisation to services (local / foreign)

Figure 2: Electronic authentication phase (source: IDABC 2007).

For this deliverable we will mainly focus on the two phases of the *authentication process*: registration and electronic authentication. The *authorisation* process (orange) is beyond the scope of the deliverable. We assume, as depicted in figure 2, that authorisation is done after the entity is authenticated and is part of the eGovernment service addressed by the individual.

In some cases this distinction is straightforward. For instance, when a Dutch citizen is moving house from the Netherlands to Austria and requests certain services from an Austrian government, then only authenticating herself as a Dutch citizen on the basis of credentials provided by the Dutch central government may suffice. In other occasions the distinction is less clear. An example would be a Dutch student visiting a Spanish municipal site and requesting a service for students (for instance enrolling for student housing). In that case, the student might need to proof that she is a student, which means that she also needs to carry and provide a credential (e.g. provided by the Dutch 'Informatie Beheer Groep'), which reveals that she is a student.

We recognise that in several instances the cross-border exchange of attributes *that are additional to the content of a formal eID* might be necessary to provide the individual an eGovernment service. Our analysis therefore contains some research in the field of additional attribute exchange (meaning the exchange of information that cannot be directly deduced from the authentication of an eID). However, we can only pay limited attention to attribute exchange, and will focus the analysis on entity authentication. With regard to attribute authentication, the deliverable bears in mind the attributes that are relevant to the pilots that will be developed in WP6, namely:

- Is claimant a student (cf. description WP 6.3)?
- Is claimant of particular age (cf. WP 6.2)?
- What is the (electronic) address of the claimant (cf. WP 6.4 and WP6.5)?

2.2.1 Actors and roles in the Authentication Model

The process of gaining and using such eIDs is, in most countries, linked to the existing citizen's identity and the existing government structure. EID structures are therefore different throughout Europe. For example, some countries may have chosen to include an eID in the original non-electronic identification methods like drivers' license and identity card, or base the eID on such identities, whereas others assign a separate eID, confined to electronic services only. Moreover, the use of identifiers, authentication mechanisms and credentials can be different amongst Member States. Nevertheless, the eID process generally comprises *five* roles, which will be present in most member states' eID models.[31] First of all, there is an (1) authority that **registers** the citizen that wants to obtain an eID. This authority is related to the (2) organisation that **provides** an electronic token and the credentials (hence, the eID) that can be used in eGovernment authentication. In addition, the process of authentication comprises the role of (3) an authority that **authenticates** the token that is used by the citizen. Next to this authenticating party, there is (4) a **relying** party that depends on this electronic authentication for

[31] The roles are derived from IDABC, December 2007

the purpose of interaction or transaction, e.g. in the eGovernment service. Of course, there is also (5) an entity that **claims** a particular identity (e.g. the citizen or a delegate).

Please note that the above describe roles can sometimes be executed by the same party. For example, an identity provider can also be authentication authority, and a registration authority might also be an identity provider.

2.2.2 A framework for analysis

In order to provide a legal analysis of eID solutions and authentication processes and the barriers and opportunities for pan-European interoperable authentication for eGovernment services we need a comprehensive framework. Our model consists of two main concepts that play a central role in the registration (phase) and authentication (phase) of citizens in eGovernment processes: *eID* and *Authentication Authorities*. We have used the term Authentication Authorities in this report rather than Certification Authorities, because the latter term in the strict sense only pertains to Certificates. This would exclude authentication of users in a context where only username and password are used. Authentication Authorities as used in this document entail both Certification Authorities' for digital certificates and username/password verifiers.

For both eIDs and Authentication Authorities we distinguish a number of elements that jointly provide a clear picture of their legal aspects. The two frameworks will be completed for the most relevant eID and Authorities in each country in the report.

2.2.3 eID

- Name – What is the name of the eID? For instance in the Netherlands one of the eIDs is 'DigiD' (level 1), another is 'eNIK' (strictly speaking eNIK is DigiD level 3).
- Form – What form does the eID have? It may be a set of attributes and certificates embedded in a token such as a chip card or consist of bit string, such as in the case of DigiD level 1 (the Citizen Service Number associated to a username and password).
- Eligibility – Who can obtain the eID. Some member states only allow residents to obtain a particular eID whereas others may provide eIDs also to asylum seekers, expats, or individuals with a temporary permit.
- Issuer – Who issues the eID (who is the identity provider)? There can be one authority but there might be several authorities. Moreover, there can both be private parties and public parties that are active in the registration process.
- Attributes – Which attributes make up the eID and what are their features? The eID at least has an identifier (name or identifying number), but may also contain other attributes, such as address, date of birth, etc. Attributes may have special features, for instance, the Dutch identifier BSN, which is part of DigiD is meaningless bit string (9 numerical digits), whereas other numbers can contains gender and date of birth.
- Additional Attributes How can the eID provide access to reliable information about age, address, and about if he or she is a student?
- Responsible authority – Who is responsible for the eID and the issuance of the eIDs?
- Conditions for use – Who may use the eID and what are the obligations for the individual to whom the eID belongs? For instance, the eID (or its attributes) may only be used in the public sector as opposed to the private sector. May the eID be used in the entire public sector, or only to specific areas within the public sector, such as the health care domain or the fiscal domain? The eID may also have conditions such as 'strictly personal'.
- Creation and termination – How is the eID issued and terminated and what are the requirements in the process that affect the trust level associated to the eID?

2.2.4 Authentication Authority

- Name – What is the name of the Authentication Authority?
- What – What eIDs can the Authentication Authority authenticate?
- Responsible authority– Who is responsible for the Authentication Authority?
- Input – What is the input for the Authentication Authority, for instance, username/password? What are the legal conditions/requirements on input?
- Output – What does the Authentication Authority provide as output, for instance a Citizen Service Number (in the Netherlands)? What are the legal conditions/requirements on the output?
- For whom – Who can use the Authentication Authority for authentication: e.g., claimant, relying parties? How can one connect to the services of the Authentication Authority?
- Process – How does the authentication process work? What is the input and what is the output, and what are the legal conditions on input and output?
- Assurance level – Which assurance levels does the Authentication Authority provide? Is this legally governed?

As mentioned before, in the analysis that follows (part II), we have limited ourselves to entity authentication instead of attribute authentication, even though for the sake of the STORK pilots, some specific attributes are part of our analysis. The analysis discusses options for obtaining attributes from attribute providers without going into too much depth because of resource limitations for preparing this deliverable. The focus in the analysis is on authentic registers in the various member states.

By entity authentication we mean: '*the assessment whether an individual is who (s)he claims to be*'. Usually this process results in an identifier associated to the authenticated individual authenticated such as a name and/or some identifying number.

Attribute authentication relates to the question: Does individual X really have attribute Y? For instance, is X a student enlisted in a Dutch institute for higher education, or does Z really live in Prague. Entity authentication is a special case of attribute authentication (namely one where the question, for instance is: is X's name really X?). The reason for restricting ourselves to mainly to entity authentication is that addressing all possible instances of attribute authentication introduces an enormous amount of potential authentication authorities rather than the limited number that can do entity authentication in a particular country. However, in the light of the STORK pilots (WP6), some particular attributes will be part of the analysis.

PART II: GENERAL ANALYSIS

3 European regulation relevant to interoperability

3.1 EC Treaty

Before describing the European regulation in the field of pan-European e-Government services, it is useful to point out that the competence to draft regulation on a European level in the field of electronic identities is, to some extent, bound by Article 18 of the EC treaty[32], which states:

> *"1. Every citizen of the Union shall have the right to move and reside freely within the territory of the Member States, subject to the limitations and conditions laid down in this Treaty and by the measures adopted to give it effect.*
>
> *2. If action by the Community should prove necessary to attain this objective and this Treaty has not provided the necessary powers, the Council may adopt provisions with a view to facilitating the exercise of the rights referred to in paragraph 1. The Council shall act in accordance with the procedure referred to in Article 251.*
>
> *3. Paragraph 2 shall not apply to provisions on passports, identity cards, residence permits or any other such document or to provisions on social security or social protection."*

Hence, the EC treaty may limit the possibilities to draft pan-European regulation on identity cards.[33] The exact limits imposed by the EC treaty are not entirely clear according to a report written for the Porvoo-group.[34] The report did mention, however, that some European regulation has already been drafted with regard to eIDs (e.g. on eSignatures) and that the limitations of Article 18 may only pertain to 'documents', which might make the stipulation less relevant for electronic identities.[35] Nevertheless, when developing solutions for a pan-European use of electronic Identities, one should bear in mind that the competence on a European level is limited.

3.1.1 Directive on the protection of personal data (95/46/EC)

The Data Protection Directive (95/46/EC, 24 October 1995) was drawn up to address the need for pan-European flow of information and the need to have a minimum level of data protection when such information flows across borders. Hence, both the internal market (article 95 of the EC treaty) as the respect for privacy (article 8 ECHR) are core considerations of the Directive.[36]

The Directive provides a set of legal requirements for personal data to be processed throughout private and public services in Europe[37] and has been transposed into national regulation by all Member States. Even though there are differences in the transposition of the Directive in the different Member States,[38] it is likely that the *principles* laid down in the Directive are respected by all Member States.

[32] EU (2006). "Consolidated Versions of the Treaty on European Union and of the Treaty Establishing the European Community." Official Journal of the European Union C 321(E/1).

[33] Myhr, T. (2005). Regulating a European eID: A preliminary study on a regulatory framework for entity authentication and a pan European Electronic ID, The Porvoo e-ID Group.

[34] Myhr, T. (2005)

[35] Myhr, T. (2005)

[36] Cf. art 1 95/46/EC, see also Cuijpers, C.M.K.C., Privacyrecht of privaatrecht? Een privaatrechtelijk alternatief voor de implementatie van de Europese privacyrichtlijn [Privacy law or private law? A private law alternative for the implementation of the European Privacy Directive], Wolf Legal Publishers, Nijmegen, 2005.

[37] In principle, the directive does not discriminate between private and public data processing, even though exceptions exist e.g. in Art. 3(2) Dir. 95/46/EC.

[38] European Commission Communication, 'First report on the implementation of the data protection directive' (95/46/ec) (No. COM(2003) 265 final), Brussels.

The scope of the Directive is broad, in the sense that the concept of *personal data* applies to a broad range of information (text, sound, images) that relate to an identified or identifiable person[39] (art. 2a). The Directive states that an identifiable person is one who can be identified, directly or indirectly, *in particular by reference to an identification number*.

Considering the scope of the directive, we can mention that when data can identify a person by using *reasonable* means this can already be considered personal data (cf. recital 26). Moreover the term *processing*, which is one of the key definitions of the directive, is another term that has a broad scope (art. 2b), as the single retrieval of personal data can be regarded as data processing. Furthermore, a *data controller* (the person to which many stipulations of the directive are addressed, e.g. in article 6) can be every entity that determines the purpose and means of the processing of data (art 2d). This means that both private and public bodies can be considered data controller.[40]

The Directive comprises a set of principles/requirements which make data processing lawful. These principles are to a large extent elaborated in Article 6 of the Directive.[41]

First of all, personal data needs to be processed fair and lawful (art 6(1)a). This means that, amongst others, the method to obtain data needs to incorporate information about e.g. the identity of the controller and the purposes of data processing (art. 10).

A second principle is that the purpose of the data collection needs to be specified and limited (art 6(1)b). In addition, this principle states that such purposes need to be legitimate. The legitimacy of data collection is governed by article 7 of the Directive: legitimacy can be derived from a) unambiguous consent, b) the necessity of processing for the performance of a contract, c) a legal obligation of the controller, d) protection of the vital interests of the data subject, e) performance of a task carried out in the public interest or in the exercise of official authority, and f) necessity of processing for the purposes of the legitimate interests pursued by the controller.

The third principle for lawful processing of data is that data processing needs to be adequate, relevant, and not excessive in relation to its purposes (art. 6(1)c). In addition, the data should be accurate and up to date (fourth principle, art. 6(1)d), and not be kept longer than necessary (fifth principle, art. 6(1)e). Of course, personal data processing needs to be protected against data loss, destruction, and alteration (principle of security, art 17).

Article 8 of the Directive states that the processing of special categories of data is prohibited, except in the instances stated in paragraphs 2 to 7 of this article. In this regard, especially paragraph 7 of article 8 is worth mentioning: '*Member States shall determine the conditions under which a national identification number or any other identifier of general application may be processed*'.

The Data Protection Directive has a direct bearing on the STORK project. First of all, most of the data exchanged in citizen-government interactions are to be considered personal data and hence are covered by the Directive. This means that personal data (including attributes of the claimant) may only be processed if article 7 of the Directive is met. Given the scope of the conditions in article 7 (confined to the individual member states), the most important ground to make the processing of personal data across state borders legitimate is unambiguous consent of the data subject (the claimant). This will not be too problematic when data is provided by the claimant directly (e.g., in an online form), or when data can be obtained from a certificate presented by the claimant (for instance, taken from a certificate

[39] Buchta (ed.), 2004, Requirements version 0 – Part 1, PRIME project deliverable, see http://prime-project.eu

[40] A.R. Lodder & H.W.K.Kaspersen (Eds.) 2002. "eDirectives: Guide to European Union Law on E-Commerce, The Hague/London/New York: Kluwer Law International.

[41] See for more detailed discussions of the data protection principles for instance Bygrave, L.A., 'Core principles of data protection', Privacy Law and Policy Reporter, vol. 7, issue 9, 2001; Kosta, E. et al., Requirements for privacy enhancing tools, 2008, available at <www.prime-project.eu>, last consulted 15 October 2008; OECD, OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, available at org>, last consulted 29 August 2008; Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, available at <www.conventions.coe.int/Treaty/en/Treaties/Html/108.htm>, last consulted 29 August 2008.

on a smart card inserted into a reader attached to the divide the claimant uses in the interaction). It becomes more complicated when the service provider (relying party) needs to obtain additional data, such as (certified) attributes and these can be, or even have to be obtained, from other sources than the user. In some cases it may, for instance, be possible to collect the data from authentic registers in the claimant home member state. In this case also consent of the user may be required in order to make the processing legitimate.

Also the other requirements of the Data Protection Directive have to be met. The identity of the controller has to be specified, as well as the purposes for the data collection (articles 6 and 10, DPD). Data minimisation has to be observed (art. 6) and data should be accurate and up to date. These requirements may be difficult to meet in cases where no direct access is available to reliable data sources (such as authentic registries). Data security will not be different from what is required in relation to the processing to data originating from the claimants in the service providers own member state.

Special attention needs to be paid to the article 8(7) pertaining to national identification numbers and other identifiers. The requirements for processing these identifiers are defined by the member states. As the country reports show, the majority of the member states do not allow (national) identity numbers to be used outside the member state itself.[42] Given the expressed need by member states in wp2 that they need some form of identifier when a foreign claimant makes use of their services, this may present issues. A possibility to mediate this issue may be to use a one-way transformation function that unequivocally transforms a foreign ID number into one that may be locally stored.

3.1.2 Directive 1999/93/EC on a Community framework for electronic signatures

Since the STORK project mainly concerns authentication, we will not discuss electronic signatures in great detail here, but instead focus on digital certificates as these are used for authentication purposes. The reason why we shortly deal with this subject is because the signature can be part of the certificates. A profound analysis is nevertheless beyond the scope of the current deliverable.

3.1.2.1 Scope of the directive

The purpose of this Directive is to;

- facilitate the use of electronic signatures and to contribute to their legal recognition and;
- to establish a legal framework for electronic signatures and certain certification-services in order to ensure the proper functioning of the internal market.

It does not cover aspects related to the conclusion and validity of contracts or other legal obligations where there are requirements as regards form prescribed by national or Community law nor does it affect rules and limits, contained in national or Community law, governing the use of documents.[43]

3.1.2.2 Terminology

An *electronic signature* means data in electronic form which are attached to or logically associated with other electronic data. It is a technique by which it is possible to secure information in such a way that the originator of the information, as well as the integrity of the information, can be verified. This procedure of guaranteeing the origin and the integrity of the information is also called: authentication. Although the European Directive deals mainly with the use of elecronic signatures as a substitute for hand-written signatures produced by natural persons, it can be used in all circumstances where the origin and the integrity of computer data have to be secured.[44]

"*Advanced electronic signature*" means an electronic signature which meets the following requirements:

[42] Cf art. 8 Directive and Lodder Kaspersen (2002), p. 124

[43] Article 1 of directive 1999/93/EC.

[44] A.R. Lodder and H.W.K. Kaspersen, eDirectives: Guide to European Union Law on E-commerce, Kluwer Law International, 2002, p. 34.

(a) it is uniquely linked to the signatory;

(b) it is capable of identifying the signatory;

(c) it is created using means that the signatory can maintain under his sole control; and;

(d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable;[45]

The signatory is the person who acts in order to generate a signature.

An electronic signature is to be treated legally equal to a hand-written signature when it concerns an:[46]

(I) advanced electronic signature based on

(II) a qualified certificate and

(III) created by a secure-signature-creation device.

And only if the requirements for hand-written signatures are fulfilled.[47]

Since the STORK project mainly concerns authentication, we will not discuss electronic signatures in more detail here, but instead focus on digital certificates as these are used for authentication purposes.

A *certificate* is an electronic attestation which links signature-verification data to a person and confirms the identity of that person. "*Qualified certificate*" means a certificate which meets the requirements laid down in Annex I and is provided by a certification-service-provider who fulfils the requirements laid down in Annex II of the Directive.[48]

In the context of the STORK project electronic signatures are highly relevant. Some member states, such as Austria, Sweden, Spain, and Portugal, have deployed eIDs on smart cards that include two certificates: one for authentication and one for digital signatures.

An important question is what the legal status of these certificates is, especially in the light of the e-Signature Directive. All authentication certificates, by definition, can be used to authenticate the holder (confirm the identity). If a certificate is a *Qualified certificate*, then the proof is stronger (assurance level is higher) than for other (advanced) certificates because qualified certificates are issued and verified in a more tightly controlled process as outlined in Annexes I and II of the Directive. Because of these requirements, users of QCs may expect to be certain that a validated certificate indeed is true and not revoked, and hence CA's issuing Qualified Certificates have a certain liability as described in article 6 of the e-Sig Directive (see below).

The requirements for Qualified Certificates are:

Annex I:

Qualified certificates must contain:

(a) an indication that the certificate is issued as a qualified certificate;

(b) the identification of the certification-service-provider and the State in which it is established;

(c) the name of the signatory or a pseudonym, which shall be identified as such;

(d) provision for a specific attribute of the signatory to be included if relevant, depending on the purpose for which the certificate is intended;

(e) signature-verification data which correspond to signature-creation data under the control of the signatory;

[45] Article 2 of directive 1999/93/EC.

[46] Article 5 (1) of directive 1999/93/EC.

[47] Recital 20 of directive 1999/93/EC.

[48] Article 2 (9) and (10) of directive 1999/93/EC.

(f) an indication of the beginning and end of the period of validity of the certificate;

(g) the identity code of the certificate;

(h) the advanced electronic signature of the certification-service-provider issuing it;

(i) limitations on the scope of use of the certificate, if applicable; and

(j) limits on the value of transactions for which the certificate can be used, if applicable.

Annex II:

Certification-service-providers must:

(a) demonstrate the reliability necessary for providing certification services;

(b) ensure the operation of a prompt and secure directory and a secure and immediate revocation service;

(c) ensure that the date and time when a certificate is issued or revoked can be determined precisely;

(d) verify, by appropriate means in accordance with national law, the identity and, if applicable, any specific attributes of the person to which a qualified certificate is issued;

(e) employ personnel who possess the expert knowledge, experience, and qualifications necessary for the services provided, in particular competence at managerial level, expertise in electronic signature technology and familiarity with proper security procedures; they must also apply administrative and management procedures which are adequate and correspond to recognised standards;

(f) use trustworthy systems and products which are protected against modification and ensure the technical and cryptographic security of the process supported by them;

(g) take measures against forgery of certificates, and, in cases where the certification-service-provider generates signature-creation data, guarantee confidentiality during the process of generating such data;

(h) maintain sufficient financial resources to operate in conformity with the requirements laid down in the Directive, in particular to bear the risk of liability for damages, for example, by obtaining appropriate insurance;

(i) record all relevant information concerning a qualified certificate for an appropriate period of time, in particular for the purpose of providing evidence of certification for the purposes of legal proceedings. Such recording may be done electronically;

(j) not store or copy signature-creation data of the person to whom the certification-service-provider provided key management services;

(k) before entering into a contractual relationship with a person seeking a certificate to support his electronic signature inform that person by a durable means of communication of the precise terms and conditions regarding the use of the certificate, including any limitations on its use, the existence of a voluntary accreditation scheme and procedures for complaints and dispute settlement. Such information, which may be transmitted electronically, must be in writing and in readily understandable language. Relevant parts of this information must also be made available on request to third-parties relying on the certificate;

(l) use trustworthy systems to store certificates in a verifiable form so that:

— only authorised persons can make entries and changes,

— information can be checked for authenticity,

— certificates are publicly available for retrieval in only those cases for which the certificate-holder's consent has been obtained, and

— any technical changes compromising these security requirements are apparent to the operator.

These requirements reveal that Qualified Certificates can be used for different functions (authentication, signature, etc); the Directive is indifferent in this respect. It is up to the individual member states to determine whether they grant certification-service providers the right to issue qualified certificates and whether their eIDs make use of qualified certificates or other certificates. Spain, for instance, has opted for the inclusion of qualified certificates in their DNIe card.

Member states may also determine for which purpose a particular certificate may be used. Most differentiate between the authentication certificate and the non-repudiation digital signature and consider it undesirable that the authentication certificate is used for signature purposes and vice versa. Spain, for instance, has legal prohibitions for using the DNIe card's authentication certificate for signature purposes.[49]

What we see here is that technical, procedural and legal issues are interrelated. Qualified certificates are meant to provide a high level of assurance and are therefore issued in strict procedures involving face-to-face verification of the claimant/citizen. The basic legal effects of these QC's is handled by the e-signature Directive and its transposition in national legislation. Qualified certificates are given significant legal effect because they can be trusted on the basis of the certificate issuing process. Whether a member state implements QCs in their eIDs depends on a weighing of costs involved (issuing QCs is expensive) against the necessity of higher levels of trustworthiness. As the analysis of the country reports shows, the various member states reach different conclusions.

The e-Signatures Directive also harmonises the recognition of signatures in and between member states. To exchange information and trade electronically in a secure way in order to stimulate the Community-wide provision of certification services over open networks, certification-service-providers should be free to provide their services without prior authorisation.[50] Consideration 21 and Article 4 establish that services offered by certification-service-providers in other member states should be accepted.

Art. 4

> 1. Each Member State shall apply the national provisions which it adopts pursuant to this Directive to certification-service-providers established on its territory and to the services which they provide. Member States may not restrict the provision of certification-services originating in another Member State in the fields covered by this Directive.

This means that there should be no legal barriers to have foreign CA’s validate certificates they issued by means of OCSP or CRLs.

Another matter is whether a claimant is permitted to use a particular certificate to authenticate him/her in a particular context. In Austria, there is no restriction on the use of the authentication certificate on the Bürgerkarte for authentication purposes as this would be deemed counterproductive to establishing trust on the internet. Also CA's can impose restrictions on who can make use of their services. Access to validation services (OCSP and CRLs) may be open to anyone without prior arrangements. In other cases, such as Spain, users of certificate validation services need to have a prior agreement with @Firma (the Administration (MAP)) before they can use its services.

The picture that emerges is that the Directive provides a base line aimed at interoperability of certificates and electronic signatures across the EU. The Member States are, however, free to make particular arrangements regarding certificates within their own jurisdiction. They may regulate which (kinds of) certificates are allowed within certain areas and also whether these may be used in cross border transactions. Also certification-service-providers may impose terms and conditions on the certificates they issue. A clear example here is the TOS employed by Chamber SimplySign in the UK.[51]

3.1.2.3 Liability

Providers of qualified certificates are liable for information contained in the certificate and the accuracy of revocation lists. Article 6 provides for a minimum of Certification Authority (CA) liability but also certain limitations.

The minimum liability provisions only apply if a certificate has been issued or guaranteed as a qualified certificate. When this is the case a certification-service-provider is liable for damage caused to any entity or legal or natural person who reasonably relies on that certificate as regards the accuracy and completeness of all the information in the certificate, the identity of the signatory, the complementary usage of signature creation data and signature-verification data if the CA has created them both

[49] See the country report on Spain and the DNIe Royal Decree 1553/2005, of December 23, ruling the national identity card and its eSignature certificates. http://www.dnielectronico.es/marco_legal/RD_1553_2005.html

[50] Recital 10 of directive 1999/93/EC.

[51] See the UK country report.

and for failure to register the revocation of the certificate.[52] Whether the defective certificate is actually qualified or unqualified is irrelevant, decisive is its designation by the CA.[53]

With respect to the STORK project this brings us back to the question whether the certificates employed in the eID are qualified or not. In Member States that require Qualified Certificates as part of their eIDs, a certain liability is placed upon the certification-service-provider, who may have arrangements with the MS government regarding damages. In other cases certification-service-provider may be able to waive liability in their terms of service. Whether this can be done in practice depends on the legislation (civil liability) of the individual member states. As stated above, analysis of this aspect is beyond the scope of the current deliverable.

3.2 Directive 2006/123/EC on services in the internal market

The directive on services in the internal market ('Services Directive') aims to creating a single market for services within the European Union by regulating cross-border services. It is necessary to remove barriers to the free movement of services between Member States and to guarantee recipients and providers the legal certainty necessary for the exercise in practice of the fundamental freedoms of the Treaty.[54] The directive is a residual one: it only applies if no other, more specific directive, regulation or other EC act applies.[55]

The directive sets out to which services directive 2006/123/EC shall apply and to which not (article 2) and what kind of restrictions the Member State where the services are provided may still impose (articles 16 and 17).

Authorisation schemes can only exist when they are (a) non-discriminatory, (b) justified by an overriding reason relating to the public interest, (c) proportionate to that public interest objective, (d) clear and unambiguous, (e) objective, (f) made public in advance and (g) transparent and accessible.[56]

Even though the directive is not focused on eGovernment, it has important aspects and impact on how municipalities and public bodies have to deliver electronic public services. From the point of view of a Local Administration, it is a key document about how eServices must be provided to SME and companies in general.[57] The most important article with regard to eGovernment is article 8;

Article 8

Procedures by electronic means

1. Member States shall ensure that all procedures and formalities relating to access to a service activity and to the exercise thereof may be easily completed, at a distance and by electronic means, through the relevant point of single contact and with the relevant competent authorities.

2. Paragraph 1 shall not apply to the inspection of premises on which the service is provided or of equipment used by the provider or to physical examination of the capability or of the personal integrity of the provider or of his responsible staff.

3. The Commission shall, in accordance with the procedure referred to in Article 40(2), adopt detailed rules for the implementation of paragraph 1 of this Article with a view to facilitating the interoperability of information systems and use of procedures by electronic means between Member States, taking into account common standards developed at Community level.

[52] Article 6 (1) and (2) of directive 1999/93/EC.

[53] A.R. Lodder and H.W.K. Kaspersen, eDirectives: Guide to European Union Law on E-commerce, Kluwer Law International, 2002, p. 59.

[54] Recital 5 of directive 2006/123/EC.

[55] Article 3 of directive 2006/123/EC.

[56] Recital 95 and articles 9 and 10 of directive 2006/123/EC.

[57] Epractice.eu; http://www.epractice.eu/document/4036

3.3 Representation and delegation[58]

The law also regulates that certain individuals can not perform legal acts, such as entering into contracts. But the law also allows empowering a person to act for another person or to conduct a certain transaction.

Representation and delegation in daily life are often taken for granted implicitly. In everyday life, proof of authorisation is not usually required, but when working with electronic transactions, authorisation has to be expressed explicitly. This creates a need for having an electronic form of empowerment and representation. The vehicle for achieving this is the concept of electronic mandates. On the one hand, electronic mandates are the electronic equivalent of conventional mandates for empowering a person, in which a representative acts for another person, referred to as the mandator under certain circumstances. On the other hand, electronic mandates serve to close the gap between private persons and legal entities. Wp2 will only look briefly at this subject,

3.3.1 Electronic mandates

Electronic mandates aim to provide end to end security as the representative is holding a token (i.e. an electronic mandate) asserting that she is empowered to act in the name of another entity and can prove it in front of any application. So it is not an issue for applications to know about a person’s authorisation to represent other entities/persons. Applications just have to verify electronic mandates. This makes it finally easy to manage authorisations.

From a use-case perspective, electronic mandates should serve to describe any kind of representations. Thus it should enable:

a) a natural person to represent a legal person/entity

b) a natural person to represent another natural person

c) a legal person/entity to represent another legal person/entity

d) a legal person/entity to represent a natural person.

By combining multiple mandates of different types (a-d), even more complex situations can be created (by chaining multiple mandates).

Similar to conventional mandates, an electronic mandate should hold:

- identity of the mandator
- identity of the representative
- date and place of issuing
- content and concern of the mandate
- optional restrictions

The electronic mandate should hold the electronic identity of the mandator (i.e. the person who empowers another person to act in her name). This can be achieved in different ways, depending on whether one can resort to national identifying numbers for individuals and legal entities or not. When unique identifying numbers are available, these can conveniently be used to establish a clear relationship between mandator and the representative. Else combinations of other data will have to be used, such as first and last name, date of birth, etc. In the event of having legal entities, analogous identity attributes can be used (e.g. the full name of a company and its unique identifier taken from the commercial register).

[58] Based on input provided by Austria

The scope of the mandate has to be clearly defined in a way that is understandable for the applications that have to handle the mandates (as well as in textual descriptions that are understandable for humans).

In order to assert the authenticity of a mandate, it should be electronically signed, either by the mandator or by an issuing authority.

The concept for electronic mandates should introduce an electronic mechanism for revoking a mandate. The introduction of this technical revocation mechanism would be a great improvement in comparison to conventional mandates and it is especially necessary for electronic mandates. On the one hand, it is sufficient from a legal perspective to revoke a mandate by publicly announcing a revocation. Consider conventional paper-based mandates: if the representative is still in the possession of a paper that pretends to act as a valid mandate, the representative would still be able to act illegally in the name of the mandator. Thus, the only effective way to avoid this problem is to request that the representative destroy the paper mandate, which would prove hard to verify. With electronic mandates, this situation is much more difficult since the representative could create an arbitrary number of copies of the electronic mandate and the mandator could never be sure whether any illegal copies still exist. An electronic revocation mechanism is therefore very desirable for electronic mandates.

Therefore, the introduction of an electronic revocation mechanism is strongly recommended. To make an electronic mandate electronically defeasible, the mandate needs to be registered with a certain revocation service. As a result, electronic mandates may hold an Internet address that provides revocation information on request. When attempting to verify an electronic mandate, the named revocation service has to be asked about the current revocation status by using the serial number of the electronic mandate. A similar revocation mechanism for digital certificates is already widely used and well-established. Thus, the concept of mandate revocation can be made similar to the revocation mechanism of digital certificates.

Delegation, mandates and representation are to a large extent part of civil law which means that there may be significant differences between the EU member states. Also in the public sector we may expect significant differences in how representation is handled in the various member states. In some of the country reports submitted by the country reporters aspects of representation are addressed. Beyond this we can not draw hard conclusions regarding representation and delegation of eIDs.

3.4 Summary of Legal issues

In this chapter we summarise the most important findings of the analysis of the EU legal framework related to interoperable eID as well as the findings of the country reports.

Data Protection Directive

The Data Protection Directive has a direct bearing on the STORK project because most of the data exchanged in citizen-government interactions are to be considered personal data. This means that personal data (including attributes of the claimant) may only be processed if the requirements of article 7 of the Directive are met. The most important ground to make the processing of personal data across state borders legitimate is unambiguous consent of the data subject (the claimant), because legal obligations (as meant in art. 7(c)) are unlikely to exist in a pan-European context. This requirement will not be much of a problem when the data is disclosed by the claimant herself (e.g., in an online form), or when data can be obtained from a certificate presented by the claimant (for instance, taken from a certificate on a smart card used by the claimant). It is more complicated when the service provider (relying party) needs to obtain additional data, such as (certified) attributes and these can be, or even have to be obtained, from other sources than the user. In some cases it may be possible to collect the data from authentic registers in the claimant's home state without the claimants' involvement. In these cases, the relying party still would have to ask the claimant's consent in order to make the processing legitimate.

Also the other requirements of the Data Protection Directive have to be met. The identity of the controller has to be specified, as well as the purposes for data collection (articles 6 and 10, DPD). These requirements should not be difficult to meet (apart from the language in which it is presented) because the same requirements apply to the Service provider's domestic claimants.

Data minimisation has to be observed (art. 6) and data should be accurate and up to date. These requirements may be difficult to meet in cases where no direct access is available to reliable data sources (such as authentic registries). Data security will not be different from what is required in relation to the processing of data originating from the claimants in the service provider's own member state.

Special attention needs to be paid to the article 8(7) pertaining to national identification numbers and other identifiers. The requirements for processing these identifiers are defined by the member states. As the country reports show (and summarised below), the majority of the member states do not permit the use of (national) identity numbers outside their own jurisdiction, and many also pose limitations to the use of these numbers within their jurisdiction. This may pose barriers to pan-European e-Government services.

Certificates/e-Signatures Directive

In the context of the STORK project also the e-Signatures Directive is highly relevant because this Directive also regulates certificates, which are used in the various eIDs in the STORK member states. Many (smart card based) eIDs include two certificates: one for authentication and one for digital signatures.

An important question is what the legal status of these certificates is. All authentication certificates, by definition, can be used to authenticate the (confirm the identity) of the holder. *Qualified certificates* provide a higher assurance level than other (advanced) certificates because they are issued in a more tightly controlled process. Because of these requirements, users of QCs may expect to be certain that a verified certificate meets particular quality requirements regarding content and validity and hence CA's issuing Qualified Certificates have a certain liability as described in article 6 of the e-Sig Directive.

Qualified Certificates can be used for different functions (authentication, signature, etc); the Directive is indifferent in this respect. It is up to the individual member states to determine whether they accredit certification-service providers and give them the right to issue qualified certificates and whether their eIDs make use of qualified certificates or other certificates. Some countries use Qualified certificates for their eID's, others don't (see the list later on in this chapter). This may lead to difficult liability issues because the liability in the case of QC's rests on the CA that issued the certificate, whereas this is more complicated for non qualified certification-service providers. These are likely to have provisions (waiving) regarding their liability in their terms of service. Because there are potentially many certification-service providers this may lead to a complicated mesh of different liability regimes.

Member states may also determine for which purpose a particular certificate may be used. Most differentiate between the authentication certificate and the non-repudiation digital signature and consider it undesirable that the authentication certificate is used for signature purposes and vice versa.

The e-Signatures Directive also harmonises the recognition of signatures in and between member states: services offered by certification-service-providers in other member states should be accepted. This means that there should be no legal barriers to have foreign CA’s validate certificates they issued by means of OCSP or CRLs. In practice there may be restrictions imposed by the member states or CA’s in the member states on who may consult these CRLs or who may use these verification services. Issues may also arise because some eID's may for instance only be used in transactions within the public sector of the holder's member state. In such cases it is not so much the verifying CA that would pose legal barriers to pan-European e-government services, but rather the citizen's home state.

3.4.1 Identity numbers

Many eIDs contain identifiers that are based on, or are equal to, national identification numbers (e.g., Estonian Personal Identification Code, Dutch BurgerSeviceNumber, Spanish DNI number). In most countries, the use of these numbers is restricted and regulated by law. This in effect means that they can not be processed in cross border eGovernment interactions, which includes storage. The Dutch BSN, for instance may only be used by authorized entities that are listed in the Act on the Citizen Service Number, all of which are within the Dutch jurisdiction which limits the use of the BSN to Dutch (e)Government interactions.

In some countries identification numbers may be processed if the data subject consent (e.g., Estonia, Italy, Spain). In these cases the numbers may also be processed (and stored) by relying parties in other member states, provided the claimant agrees to the processing.

Germany does not have national identity numbers, but instead uses combinations of other attributes such as name and date of birth as identifier for individuals. Within certain public sectors, such as taxation, national identifiers do exist, but these may only be used within the context within which they are created, which again prevents using the numbers as identifiers in pan-European eGovernment services.

In Austria, the base identifier (sourcePIN) may not be used at all. Instead derived ssPINs may be used, but only within Austria.

The overview shows significant differences in the STORK member states regarding (national) identifiers and the restrictions on the use of these numbers.

Some STORK members have expressed a need to be able to store identifying data of foreign claimants in the eGovernment transaction process. The brief overview above shows that such identifying data can not be equal to the national identifiers in many member states.

An option might be to create a new identifier on the basis of a national identifier by means of a one-way transformation function and use this new number as the identifier in the relying party's system. This is similar to how derived identifiers (ssPINs) are created in Austria on the basis of a sourcePIN that has to remain secret. By what means this precisely has to be realized is a question that may be answered in D2.3.

	National identifier	Restricted use within MS	Permissible use abroad

AT	ZMR -> sourcePIN -> ssPIN	yes: sourcePIN no: ssPIN	No
BE	National Registry Number	Yes: only authorised entities	No
DE	None (prohibited) sectoral number, e.g. tax number	Not applicable sectoral numbers confined to sector	Not applicable No
EE	Personal Identification Code	Consent or international. agreement, act or regulation	By agreement
ES	DNI	No	Yes by user consent
FR	None, only sectoral (e.g. NIR)	NIR use restricted by law	No
IT	Fiscal number	Yes, mandated by law, or consent	Not applicable
IS	Kennitala	'Any just cause'	Within the EEA (any just cause)
LU	Identity number	Mandated by law	?
NL	BSN	Mandated by law	No
PT	National register number + other numbers	Mandated by law or DPA permission	?
SL	Personal Registration Number (EMŠO), Personal Tax Number, Health Insurance Number.	Mandated by law	not applicable
SE	Personal Identity Number	No	Yes
UK	None	Not applicable	Not applicable

Table 3: Overview of national identifying numbers and use restrictions. A “?” indicates that further information are required in order to draw a conclusion.

3.4.2 Attributes

The eID's in the various Member States differ in the amount and nature of the attributes they contain. On the one extreme we have the Dutch DigiD, which only contains the identifier BSN. On the other extreme we have eIDs, such as the Portuguese Cartão de Cidadão which contains Name, date and place of birth, date and place of issuance of the card, validity period of the card, parents, marital status, title and number of the card, picture and handwritten signature, residence, and National register number, the holder’s address and two digital certificates, one for identification and authentication and one for a qualified electronic signature. In the latter case, some of the attributes may be taken to represent authentic and accurate data (e.g., date of birth), while other data may require further proof or validation (e.g., even name may not be stable, think for instance of married women who may adopt their husband's surname in a number of EU member states).

Whether attributes present in the eID may be used in pan-European eGovernment services varies per member state. For some eID's access to the attributes (typically on the card) is locked by means of a PIN, as is the case in Italy and Spain. This guarantees that the data can only be read with the eID holder's consent. The use of the attributes in the eID in these cases is permitted, as long as the card holder consents. In other cases, access to the data on the card is open to every application that can access the data on the card, such as in Belgium.

Many eIDs do not contain the nationality of the holder, although country of issuance is an attribute present on all eID cards. Iceland's eID card, for instance, contains name, ID and country, but also foreigners may obtain the card. Also in other cases the nationality of the eID holder can not be established on the basis of the eID itself (for instance, a Dutch BSN which is part of the DigiD can also be obtained by foreigners residing in the Netherlands. Whenever the nationality of a claimant needs to be assessed, for instance to be able to distinguish between EU citizens and others, relying parties have to resort to other data than those available in most eIDs.

3.4.3 Authentic registers

In some cases, relying parties may want to obtain more attributes from a claimant than present in the presented eID, or they may want to establish an attribute at a higher level of assurance than offered by the eID (e.g., the address, and even name, present on a smart card may be outdated). In many of the member states studied, authentic registers exist that offer authorised entities access to authentic data pertaining to citizens. At least Austria, Belgium, France, Italy, Iceland, Luxembourg, Slovenia, the Netherlands and Sweden, offer extensive authentic registers that can be consulted to verify or obtain up to date attributes. The access regimes to these registries differ significantly between the member states. In some case the register is open to consultation by anyone, in other cases access is completely confined to authorised entities (e.g., Estonia where everyone with an ID-card can access the X-road register), or even entities mandated by law (e.g. the Netherlands where access to authentic registers is regulated by law).

Access to authentic registries may in some member states be obtained when a 'Memorandum of Understanding' exists between the relying party and the authentic register (or the responsible government actor), as in Italy, or when a contract exists between Relying party and authentic register (e.g., Iceland, Sweden).

3.4.4 Type of eID

Prevalent forms of authentication are username/password and (qualified) certificates which either consist of soft (X.509) certificates or hard certificates when embedded on smart cards or devices such as USB media (in ROM). The different forms are discussed in more detail below.

3.4.5 Username/password

Username/password combinations are used in many member states, especially for low risk services. Most often, username and password are associated to e-IDs created in the context of a particular service, e.g., Iceland where many government services have their own eIDM system. These are impractical for PEGS precisely because they are associated to a particular service provider.

A number of member states have portals (usually federated identity management systems) that handle the authentication of citizens for a number of services. Examples are the Dutch gbo.Overheid (DigiD), the UK Government Gateway and the French mon.service-public.fr. These systems pose either practical problems with respect to pan-European public service delivery, or suffer from legal barriers in relation to PEGS. The UK Government Gateway could in principle handle the log-in of UK citizens for foreign services, but this would require each relying party to sign up for the Gateway, which is rather impractical[59]. Legal issues are more serious obstacles. The Dutch DigiD can not be used for cross border authentication given the current regulation, because it restricts the use of DigiD to governemental entities that are permitted to use the Dutch Citizens service number, which currently means Dutch entities.

STORK MS	eID	portal	cross border restrictions
AT	?	?	?
BE	username/password	yes	no
DE	?	?	?
EE	?	?	?
ES	site specific	www.060.es and others	–

[59] Enrolment could, as far as we can see, be realised by means of contracts.

FR	–	mon.service-public.fr	Portal uses Liberty Alliance specifications. Identities are self registered by citizens
IT	?	?	?
IS	Tax password	island.is (SAML tokens)	No
LU	–	–	–
NL	DigiD	GBO.overheid	yes, not permitted
PT	?	Citizen's portal	?
SL	–	–	–
SE	?	?	?
UK	UKGG username/password	UK Government Gateway	no

Table 4: STORK member states predominantly using username/password eIDs. A “?” indicates that further information is required to draw a conclusion.

3.4.6 Certificates and smart cards

Many STORK member states have deployed certificates in the form of smart card hosted certificates. Some others employ soft certificates (that may be downloaded to hardware such as smart card or usb media, in some cases).

The following table lists the types of authentication certificates employed in the different eIDs.

STORK MS	eID	type of certificate	cross border restrictions
AT	Bürgerkarte	Qualified	No
BE	BELPIC	Advanced for authentication, Qualified for electronic signatures of documents	yes
DE	None	–	-
EE	Estonian ID card	Qualified	?
ES	DNIe	Qualified	Yes, formal agreement with @firma. See notes in country report for details.
FR	currently: none future: National eId Card Certificates provided by supervised CSP	Advanced or Qualified (TBC) Advanced or Qualified (TBC)	No No
IT	CIE CNS	Qualified	see Codice dell'Amministrazione Digitale
IS	PKI certs (Islandsrot)	Qualified	No
LU	LuxTrust smart card	Qualified	No
NL	None	Not applicable	Not applicable
PT	Citizen card	Qualified	?

SL	PKI cert	Qualified	No
SE	e-legitimation	Advanced (/Qualified)	?
UK	Soft	Advanced	no

Table 5: Authentication certificates employed in STORK member states. A "?" indicates that further information is required to draw a conclusion.

Because many STORK member states use qualified certificates in their eIDs, a number of legal issues are handled by the eSignature Directive 1999/93/EC. Even though there are differences in the national transpositions of the Directive into national legislation there is also much common ground in how the certificates are created and in their legal effects. On the technical level a number of requirements pertaining to the process of issuing certificates are described in the Directive as outlined in the previous section. For qualified certificates this means that they have a comparable assurance level. The legal effects of, especially the Qualified certificates, are also relatively clear. For instance, the basic liability for damages in the case of invalid certificates is regulated. Analogous to the legal effect of electronic signatures in relation to traditional signatures, we may expect authentication certificates (for Qualified certificates) to have the same legal effect as authentication with identity documents in a face-to-face setting. Differences exist in the way en entity can obtain eIDs in the various member states and therefore who can obtain authentication certificates. Also the use of these certificates is regulated. Some member states promote the use of certificates in order to create trust in online transactions and this may include posing very few restrictions on using them in pan-European eGovernment transactions.

Differences also exist in who may verify authentication certifications by means of OCSP and CRL mechanisms. This depends on the conditions imposed by the different CA's, but also on national regulation within the various member states. Some CA's, for instance require prior contractual agreement with users of verification services. Table 4 lists the primary CA's and their use conditions.

STORK MS	CA's	Use conditions	cross border restrictions
AT	Austrian Data Protection Authority	?	?
BE	Belgian Government (outsourced)	No, CRL/OCSP public	none, CRL/OCSP public
DE	None	–	-
EE	TRÜB Baltic S AS Sertifitseerimiskeskus	?	?
ES	@Firma MITYC, FNMT,CATCert	prior registration @Firma	not likely according to ES representative
FR	Qualified CSP	No	No
IT	CIE: National Center for Demographic Services CNS: accredited CA's	?	?
IS	Islandsrot & Fullgilt Audkenni	OCSP: no	No
LU	LuxTrust	No	CRL/ public OCSP
NL	None	?	?
PT	SCEE	No	No
SL	SIGEN-CA	No	No
SE	BID, Steria, Nordea, TeliaSonera	Agreement	No

UK	Chamber SimplySign, Equifax	prior contractual relationship	Yes, prior contractual relationship

Table 6: CA's in the STORK member states. A "?" indicates that further information is required to draw a conclusion.

3.4.7 Delegation

Delegation and representation is explicitly addressed in some of the member states. Austria, for instance has addressed these issues in the Austrian E-Government Act, and the Bürgerkarte is designed to contain information about representation, details of which can be found in the Austrian country report. Sweden is to issue Swedish corporate eIDs (e-tjänstelegitimation) for natural persons in their capacity as employee or contractor. This card is to contain information about the representative and the mandator. Information about the other STORK member states is missing. A more detailed analysis of the legal issues involved in delegation and representation in pan-European e-Government services is beyond the scope of this deliverable.

3.4.8 Liability

As already discussed, the eSignature Directive provides the backdrop for liability for CAs issuing certificates. In cases where there is a qualified signature on a token available articles 5 and 3 provide the legal basis for accepting the certificate. These provisions should in principle make cross-border verification of certificates possible.

Furthermore article 6 states (inter alia):

> "1. As a minimum, Member States shall ensure that by issuing a certificate as a qualified certificate to the public or by guaranteeing such a certificate to the public a certification-service-provider is liable for damage caused to any entity or legal or natural person who reasonably relies on that certificate:
>
> > (a) as regards the accuracy at the time of issuance of all information contained in the qualified certificate and as regards the fact that the certificate contains all the details prescribed for a qualified certificate;
> >
> > (b) for assurance that at the time of the issuance of the certificate, the signatory identified in the qualified certificate held the signature-creation data corresponding to the signature-verification data given or identified in the certificate;
> >
> > (c) for assurance that the signature-creation data and the signature-verification data can be used in a complementary manner in cases where the certification-service-provider generates them both;
>
> 2. As a minimum Member States shall ensure that a certification-service-provider who has issued a certificate as a qualified certificate to the public is liable for damage caused to any entity or legal or natural person who reasonably relies on the certificate for failure to register revocation of the certificate unless the certification-service-provider proves that he has not acted negligently.
>
> 3. Member States shall ensure that a certification-service-provider may indicate in a qualified certificate limitations on the use of that certificate. provided that the limitations are recognisable to third parties. The certification-service-provider shall not be liable for damage arising from use of a qualified certificate which exceeds the limitations placed on it.
>
> 4. Member States shall ensure that a certification-service-provider may indicate in the qualified certificate a limit on the value of transactions for which the certificate can be used, provided that the limit is recognisable to third parties.
>
> The certification-service-provider shall not be liable for damage resulting from this maximum limit being exceeded."

In principle the CA issuing qualified certificates is liable for damages arising out inaccuracy of the information contained in the certificate at the time of issuance (1a and 1b). The various member states may have particular arrangements to address specific damages.

In Estonia, the situation is the following. The national ID-scheme organisational scheme consists of triangle consisted of CMB (a state agency), TRÜB and SK (the CAs). From card-issuance point of view – all the responsibility lies on CMB. CMB has contractual agreements with TRÜB and SK detailing relevant outsource of responsibilities. From certificate issuance point of view – all the responsibility of certification procedure relies on SK. CMB, TRÜB, banks and also hotline for certificate suspension act as Registration Authorities of SK. SK has an insurance policy (required by the DAS) in excess of 5 million kroon (around €32,000) for covering possible damages caused by misbehaviour of SK or it’s contractual partners in certificate issuance or validation information provision process.[60]

In the case where no Qualified certificates are used or available, liability issues in pan-European eGovernment services are much more complex and need further analysis.

3.4.9 Other legal issues discussed in the country reports

Spain notes: It seems reasonable that each participating member state should review their respective legislations, because as indicated in the Article 90 of LOPD (Law for Protection of Personal Data) for any *incident, notification and administration procedures should exist*, and any incidences, that may affect the personal data, must be registered.

3.4.10 Pilot participation

On the basis of the country reports we can list a number of country specific issues regarding participation in the wp6 pilots.

Austria appears to have an eID scheme based on qualified certificates and chip cards. Many fundamental legal requirements for accepting certificates from other member states appear to be met (experiments with Belgian, Estonian, Finnish and Italian cards have been conducted and seem to have a legal foundation) and the Austrian Bürgerkarte seems useable in PEGS. The Austrian identifiers (sourcePIN and ssPINs) may not be used outside Austria.

Belgium has an eID scheme based on normalized and qualified certificates and chip cards. Given the fact that providers of e-ID applications are only allowed to use the national register number in certain cases upon authorisation from the sectoral committee on the Rijksregister, the eID possibly can not be used for cross border authentication. Only certain categories of authorities and instances qualify for this permission.

Germany currently does not have a suitable eID for PEGS. This may change during the time-frame of the STORK project.

Estonia has a smart card system with qualified certificates. Identity numbers may be used across the borders provided the data subject gives his/her consent. We have found no legal obstacles for Estonia's participation in the STORK pilots.

France uses a username/password based portal for federated identity management in the public sector. For the STORK pilots, authentication has to be done through mon.service-public.fr. The French social identifier, NIR, may not be used outside France. During the time frame of the STORK project, the future National eID card with 2 certificates should be implemented thus allowing a strong authentication through mon.service-public.fr.

Italy has a smart card system with qualified certificates. Data on the cards is protected by PINs, which guarantees consent of the holder regarding data disclosure. Authentic registers may be queried when a memorandum of understanding exists with the Ministry of the Interior.

Iceland uses qualified certificates. The eID schemes rely mostly on national ID-numbers for individuals. There are few restrictions on the use of the national ID-number. National registries can be queried when prior agreements with the registries exist.

Luxembourg is in the initial stages of introducing a smart card based solution to eID. Some services use username/password based authentication. It is unknown whether there are legal barriers to participating in the STORK pilots.

[60] From IDABC, ENTR/05/58-SECURITY/SC1/EE_Profile, p. 15

The Netherlands have an eID system which can only be used inside the Netherlands. Authentication is username/password based through a central authentication service (DigiD/GBO.overheid). The service (from the perspective of relying parties) may only be used by registered entities, which limits the user group to those entities that are authorised to use the Dutch national identifier (BSN). These are in turn defined in the Wet algemene bepalingen BurgerServiceNummer and currently restricted to the Dutch public sector. As it stands Dutch regulation provides serious legal barriers for Dutch participation in the STORK pilots.

Portugal has a smart card with qualified certificates. The ID number(s) (civil number, fiscal identification number, health identification number, social security number) included on the card may not be processed or stored unless authorised by law or by permission of the Data Protection Authority.

Slovenia is at the brink of introducing smart card based e-ID cards. Currently citizens can obtain e-government services by means of username/password for low sensitivity services and qualified digital certificates for higher levels of assurance. Slovenia has an extensive set of authentic registries. Because of the nature of the data kept in the CRP all its users are required to have proper legal basis.

Spain has a smart card with qualified certificates protected by PIN. Current DNI Law requires consent of the data subject for processing of the information on the card. In the STORK project scope no restrictions to international data transfer are expected.

Sweden uses a system of soft certificates issued by a large number of CA's. The SPAR catalogue holding basic identity information of Swedish citizens, originating from the National Population Registry, is open for all parties through a contract with SPAR. Before the contract can be signed the need of relevant information is decided.

The **UK** has a central authentication portal based on username/password combinations, as well as soft certificates (which plays only a very modest role in the UK eID landscape). There seems to be no legislative legal basis for the username/password based scheme, instead users (both citizens, who agree to terms and conditions and relying parties which enter into memorandums of understanding) enter into contracts with UK Government Gateway. The soft certificates are also handled by contractual agreement between users and CAs.

The conclusion that legal barriers preclude some participants to take part in the pilot is not a final conclusion. In this deliverable we have not looked for solutions to the legal barriers to participating in the pilots. Deliverable D2.3 will propose solutions to legal barriers, such as using cryptographic techniques to transform ID numbers that may not be used outside particular MS into identifiers that may be used across borders, extending the list of permissible users of authentication schemes, etc

Part III: COUNTRY REPORTS

4 Country report: Austria[61]

4.1 Structure of the Administration

The responsibility for Austria's eGovernment strategy/policy lies with the Federal Minister for Women, Media and Regional Policy Heidrun Silhavy. And the responsibility for legal and organisational issues of eGovernment at federal level lies with the ICT department of the Federal Chancellery. This includes coordination of technical infrastructure, programme and project management, budget controlling and procurement, and international issues in the area of eGovernment and security. Responsibility for implementation lies with individual State (*Länder*) and Municipal Governments.

4.2 Debate (and history)

Central to the Austrian eID is the Austrian citizen card which was launched in a Cabinet Council in November 2000 with the intention to employ smart card technology to facilitate access to public services. The government decided to enhance the health insurance card to be issued to each citizen by electronic signatures. However, already in early stages of the project the intention has been declared to remain open to the market, i.e. to remain open for other smart cards or other technologies.

To define the requirements a white paper “Weißbuch Bürgerkarte” was published in 2001. This white paper defined the general requirements of an eID and IDM system from the government’s perspective. Subsequently, technical standards have been developed that consist of a technology neutral XML-based interface “Security Layer” and a set of minimum requirements that a technology needs to fulfil in order to constitute an “Austrian citizen card”. The minimum requirements include the need of being capable of generating or verifying electronic signatures without specifying mandatory cryptographic algorithms, thus allowing for RSA, DSA, or ECDSA. Common signature formats are defined (such as cryptographic message syntax or XML design). A further requirement is that two key-pairs are given – one as a supplement of the handwritten signature (qualified signature or administrative signature) and another one for other digital signatures or to encrypt data.

4.3 eID model

The legal basis was established in March 2004 with the Austrian E-Government Act.

The starting point of the eID scheme is the ZMR number stored in the Central Register of Residents, which is a unique identifier for each natural or legal person residing in Austria, and the sourcePIN derived from it using cryptographic operations, which is stored on the Citizen Card. A sector-specific PIN is cryptographically derived from the sourcePIN. This sector specific PIN identifies the citizen uniquely within a particular sector of state activity or within a private sector organisation.

The IDM model is based on a so-called identity link. This is an electronic attestation that establishes a link between personal identification numbers (the sourcePIN) and electronic signatures as a separate signed data structure. The act also provides the data protection principles that need to be observed. The act regulates identification of the citizens using the citizen card and provides rules for electronic representation and acting as proxy.

All cards issued by citizen card issuers are ready to be activated as citizen cards, but the citizen decides whether to actually activate the electronic signature (apply for a digital certificate) and to activate an identity link.

The software required with the citizen’s PC to implement the technology-neutral interface “Security Layer” has been procured by the government as a general license and is made available for free. To complement the citizens’ eID infrastructure at the server side the Austrian government has procured so-called “Modules for Online Applications” (MOAs). The MOAs are basic modules that are made

[61] Based on analysis by the TILT team complemented by a country report written by Hubert Schier.

available free of charge. MOAs implement the processes required at the server side for identification, signature verification, signature creation, or electronic delivery.

4.4 Principal legislation and policy documents

Legislation:

The main legal framework for the eID card is:

- the E-Government Act (E-Government-Gesetz; E-GovG) is the overall legal basis for Austrian eGovernment and for closer cooperation between all authorities providing eGovernment services. Regarding eIDM, the law defines the citizen card concept and its use in the public sector using sector-specific PINs and in the private sector using private sector-specific PINs, respectively. The most important principles are: freedom of choice between means of communication for submissions to the Public Administration; security for the purpose of improving legal protection by creating appropriate technical means such as the Citizen Card and unhindered access to information.
- the Federal Act on Registration of 1991, last amended 2006; the Law defines the Central Register of Residents.
- the Source PIN Register Regulation has been enacted on 2nd March 2005. Part 4 deals with electronic representation. It defines the activities of the sourcePIN Register Authority that are necessary to implement the citizen card concept, inter alia the creation of the identity link or electronic representation.
- the Supplementary Register Regulation of 1st August 2005 defines the operation of the Supplementary Registers to include natural or legal persons that are not covered by existing registers.
- the Administrative Signature Regulation has been enacted 16th April 2004; it defines the technical requirements for citizen cards that, in an interim period until end of 2007, need not be based on qualified signatures

Other relevant legislation includes:

- the Electronic Signature Act (*Signaturgesetz; SigG*) which came into force on 1 January 2000. The Act legally recognizes electronic signatures satisfying certain security requirements and provides some evidential value to less secure electronic signatures. Furthermore, the law specifies requirements to enterprises issuing qualified certificates and defines the conditions for the acceptance of certificates of foreign origin. The conditions for the use of electronic signatures in the public sector, as well as for the use of Citizen Cards and sector-specific personal identifiers are regulated by the E-Government Act.
- the Signature Order of 2nd February 2000, last amended in 2004

The Signature Act has transposed the e-Signature Directive. Electronic signatures are defined for natural persons only.

Policy:

- the E-Government Sectors Delimitation Regulation has been enacted in 2004; it defines the sectors of State activity that are distinguishable in the sector-specific eIDM model.
- The Constitutional Law on Access to Information (*Auskunftspflichtgesetz*) became effective on 1 January 1988**.** This Freedom of Information law contains provisions on access to public information for the federal and regional levels. It stipulates a general right of access and obliges federal authorities to answer questions regarding their areas of responsibility, in so far as this does not conflict with a legal obligation to maintain secrecy. However, it does not permit citizens to access documents, just to receive answers from the government on the content of information. On the basis of the provisions of this constitutional Law, the 9 Austrian Länder have enacted laws that place similar obligations on their authorities.
- The Federal Procurement Act 2006 (*Bundesvergabegesetz 2006; BVergG*), replaced the Federal Procurement Act 2002 and repeals the eProcurement Regulation 2004. The new Federal Pro-

curement Act 2006 finally transposed all the EU public procurement directives, including their provisions regarding e-procurement, into national law.

4.5 Analysis

The need for an eID is formulated in article 3 of the Austrian E-Government Act which states that in some cases the unique identity of the person desiring access and the authenticity of his request has been validated.

> 3. (1) In the context of electronic communications with controllers in the public sector within the meaning of Paragraph 5(2) of the Datenschutzgesetz 2000 (Data Protection Act 2000), BGBl. I 1 No 165/1999, rights of access to personal data (Paragraph 4 No 1 of the Datenschutzgesetz 2000) in which there is a protected interest in confidentiality within the meaning of Paragraph 1(1) of the Datenschutzgesetz 2000 may be granted only where the unique identity of the person desiring access and the authenticity of his request have been validated. Such validation must be provided in a form which can be verified electronically.
>
> (2) Identification of a person may otherwise be requested in communications with controllers in the public sector only insofar as this is necessary in an overriding legitimate interest of the controller, in particular, where it is an essential requirement for performance of a task assigned to the controller by statute.

eIDentity: Bürgerkarte

The Citizen Card (Bürgerkarte) was introduced in the eGovernment Act (E-Government Gesetz).[62] The Bürgerkarte is not just one single card, in principle, any card that allows the user to produce secure electronic signatures and can store certain personal data is suitable as a Citizen Card. The citizen card is a technology-neutral concept that allows for different technical solutions, including smart cards and mobile phones. The regulation defines the minimal requirements that an eID token needs to fulfil: electronic signatures and storage of the identity link or electronic mandates. Quality criteria are defined such as security requirements for the electronic signatures, or the interface between Web-applications and the citizen card.

Form

The Austrian eID concept does not foresee just one single type of Citizen Card. In principle, any card which makes it possible to sign electronically in a secure form (qualified signatures) and to store personal data is suitable for use as a Citizen Card. Thus, membership cards issued by certain entities (e.g. the Federal Economic Chamber, etc.) or even bank cards can include Citizen Card functionality. A further platform is the health insurance card which is issued to each citizen. In addition, the Citizen Card concept can also be applied to mobile phones, enabling Austrian citizens to electronically sign documents and securely transact with government by using a mobile phone (the mobile phone service is currently ceased). The Citizen Card is thus not dependent on a particular form of technology, and it is entirely up to the citizen to choose the technology he prefers to use in order to identify himself electronically.

Regardless of whether a chip card, mobile phone or USB equipment is used, the chosen medium has to meet certain security requirements essential for a Citizen Card (qualified electronic signature, identification and data memory). An implementation of the Citizen Card concept can be found on the national health insurance card (e-card) which thereby can be used for secure communication with the Public Administration.

The Bürgerkarte contains a unique identifier that is derived from base register identifiers, the sourcePIN[63], stored in a so-called identity link (Personenbindung). For Austrian residents this sourcePIN is derived from the ZMR-Zahl in Central Register of Residents CRR (Zentrales Melderegister) on the basis of TripleDES encryption (128 bit binary or 24 digit base64 number). The card also contains an

[62] http://www.buergerkarte.at/de/index.html

[63] Article 6. (1) Austrian E-Government act: The person concerned shall be uniquely identified in the citizen card by his source identification number (sourcePIN).

identity link, an attestation that is created by the sourcePIN Register Authority during the issuance process of citizen cards. It links a citizen's electronic signature provided to the citizen by the citizen card issuer to the 'sourcePIN' derived from the base registers[64]. The electronic identity also holds the name and data of birth. The sourcePIN may only be stored in the identity link in the citizen card and is therefore under sole control of the citizen.

Eligibility

Every citizen who has a residence registered in Austria has a ZMR number stored in the Central Register of Residents, for which the Ministry of the Interior (MOI) is in charge. However, since the ZMR number is subject to special legal regulations, it cannot be used for identification purposes in eGovernment. Instead, a strong encryption process is used to derive a sourcePIN from the ZMR number, which is allowed to be stored on the Citizen Card. The sourcePIN Register Authority verifies by way of an electronic signature that a link has been established between the citizen card holder and his sourcePIN for the purposes of unique identification. The functions of the sourcePIN Register Authority are carried out by the Data Protection Commission, situated within the Federal Chancellery, which does normally not issue paper based identities. For persons not residing in Austria, a so-called Supplementary Register exists taking the function of the ZMR as regards the provision of a basis for calculation of the sourcePIN.

Everyone listed in the Central Register of Residents CRR (Zentrales Melderegister) can apply for a Bürgerkarte. This is the case for Austrian citizens residing in Austria.

Non-nationals with residence in Austria may be registered in the Supplementary Register for Natural Persons SRnP (Ergänzungsregister für natürliche Personen). If they have a health insurance card, a bank card or an Austrian mobile phone that can be activated as citizen card, they may activate this as a Bürgerkarte. If not, an SSCD that can be activated as citizen card can be purchased by the certification service provider A-Trust.

For legal persons, the Register of Company Names (Firmenbuch), the Central Register of Associations (Zentrales Vereinsregister), and a Supplementary Register of Other Data Subjects (Ergänzungsregister für sonstige Betroffene) complement the eGovernment base registers.

The Austrian eIdentity infrastructure also allows for the inclusion of non-nationals not residing in Austria by allowing them to use their home-country's eID (smartcards at this point). The integration into the Austrian eID middleware 'citizen card environment' has already been done for eID cards from *Belgium, Estonia, Finland, and Italy*.

The eGovernment Act and the sourcePIN Register Authority Regulations allow substituting the identifiers from the base registers by so-called substitute sourcePINs. This is handled in the Austrian eGovernment Act (article 6).

"art 6. (5) Austrian eGovernment Act: "For the purpose solely of validating recurring identity, a person may, at his request, be provided with a substitute sourcePIN by the sourcePIN Register Authority, where proof of the data required under subparagraph 3 is not furnished. The substitute sourcePIN shall be generated on the basis of data on the person concerned – for example, name and date of birth and place of birth or serial number of a certificate – which, as a whole, can be expected to distinguish that person sufficiently. It must be possible to recognise the number as a substitute sourcePIN."

Prerequisite for online registration in the supplementary register (done transparently in course at the first login of a citizen card-enabled application) is a qualified signature. Whether a certain qualified signature fulfils the criteria for unique identification is laid down in a special regulation, which has to be decreed by the Federal Chancellor for each specific foreign country. The citizen card middleware implements the signatures listed in these regulations.

[64] E-Government-Gesetz – E-GovG, art. 4 (3).

Thus, the requirement set out for the foreign eIDM token is rather similar to the requirements for Austrian citizen cards, i.e. that an electronic signature needs to be available and some source identifier is used. Whether a certain qualified signature fulfils the criteria for unique identification is laid down in a special regulation, which has to be decreed by the Federal Chancellor for each specific foreign country. The citizen card middleware implements the signatures listed in these regulations.

Authorities may establish the nationality of a person by searching the central register of residents with or without citizen card. Nationality is part of the data required for registration, but no information about nationality is stored on the citizen card. However, to use this information for other administrative purposes than citizen registration, the registration data has to be "certified", i.e. cross-checked with official documents and flagged in the database.

Issuer

The number of card issuers is not restricted, and there can both be private and public parties. All citizen cards are logically linked to the sourcePIN Register Authority as identity provider. For the time being, the following citizen cards do already exist:

- 'a.sign premium' card of the certification service provider a.trust
- national health insurance card
- student service cards
- ATM and bank cards with electronic signatures
- public servant identification documents for Federal Ministries
- cards issued by various chambers

The sourcePIN Register Authority is the identity provider that asserts the sourcePIN as a signed SAML record, the so-called identity link that is stored on the citizen card. Note, that the identity provider is invoked during the issuance of a citizen card only. The electronic signature of the sourcePIN Register Authority on the identity link is used during the online process, thus no identity provider is consulted during use of a Citizen Card.

In connection with the Citizen Card, a Certification Service Provider is responsible for verifying the citizen’s identity as part of the registration procedure as well as requesting the identity link (i.e., additional identity component) from the sourcePIN Register Authority.

At the moment, a.trust is the only CSP issuing the so-called “qualified certificates” in Austria. Other CSPs from any of the EU Member States may offer their services in Austria as well.

Responsible authority

The functions of the sourcePIN Register Authority are carried out by the Data Protection Commission, situated within the Federal Chancellery, which does normally not issue paper based identities.

A primary source of the eIDM system is the Central Register of Residents that determines the data quality. The registration authorities (the mayors) have an obligation to maintain the data and to correct errors under the Registration Act (Meldegesetz).

Attributes

The Citizen Card stores only data that is absolutely necessary for electronic identification. In addition to the name and surname, this includes the date of birth and the sourcePIN. For electronic signatures, the Citizen Card contains public-key certificates, but without additional personal data.

Some Citizen Card implementations like the health insurance card or ATM cards do of course store additional information, but these data cannot be read by unauthorised Citizen Card applications.

Additional attributes may be obtained from the Central Register of Residents. The data residing in this register is marked verified when data is checked by the authority entering the data (see art. 17 Austrian eGovernment act).

If cross-border exchange of additional data is necessary for the pilots, like e.g. for student mobility, then this additional data will have to be retrieved from separate sources. The eID (citizen card) may help in accessing it.

Conditions for use

The Austrian eID can be used for eGovernment purposes as well as in the private sector. It would be absolutely counterproductive to restrict its usage to specific areas. For natural persons, identification is by definition strictly personal, except for the case of electronic mandates.

The unique identifiers sourcePIN and also the sector-specific PINs are legally protected by the eGovernment Act. Storing the sourcePIN is prohibited for any application; only the citizen card holds the sourcePIN in the identity link. The sector-specific PINs may only be stored by the sector that has created the identifier. The same holds for private-sector specific PINs.

Representation of non-natural persons is handled using electronic mandates. The power to represent is checked by the sourcePIN Register Authority during issuing the electronic mandate.

Creation and termination

The Bürgerkarte has different incarnations: chip card, for instance the national health insurance card (eCard), mobile phone, USB equipment. Activation of the citizen card usually consists of the creation of electronic signature certificates by a certification service provider and creation of an identity link during the certificate creation process. The holder of an appropriate card, can either activate it online, or go to one of many registration offices in Austria (see www.buergerkarte.at/en/aktivieren/online.html).

The activation process depends on the actual token used:

- Bank cards require the activation process for qualified certificates. Application for the certificate can be made via the Internet. Registration requires physical presence at a registration office (banks, notaries) and showing a photo ID.
- The health insurance card can either be activated via the Internet where identification is proven via a registered letter in a quality that requires showing a photo ID to the post official, or with physical presence at a registration officer (social insurance organisations).
- To register a mobile phone as citizen card, the application is made via the Internet. Registration requires physical presence at a registration office of the mobile phone service provider.
- Other tokens such as student service cards or public servant service cards can involve delegation of the registration officer duties to personnel departments or student offices.

Not the eID but the electronic signature for its authentication can be revoked by request to the certification service provider (rendering future electronic signature of the particular eID invalid, the identifiers are not changed).

4.6 Authentication Authority (including CA's*)*

Name: none

In the citizen card issuance phase, the sourcePIN Register Authority asserts by way of an electronic signature that a link has been established between the citizen card holder and his sourcePIN for the purposes of unique identification. The functions of the sourcePIN Register Authority are carried out by the Data Protection Commission, situated within the Federal Chancellery.

During usage, authentication is carried out by the service provider by using conventional signature validation procedures. No external authentication authorities are used. The communication is between the citizen (Citizen Card) and the service provider who may consult certificate status information (OCSP or CRL) which is however not considered an AA, but just a revocation service (cf. Directive 1999/93/EC, Annex II).

MOA SS/SP (integrated with MOA ID) implements these protocols and communicates with the service of the certification authority that issued the certificate used with MOA ID.

4.6.1 MOA ID[65]

This module is used to uniquely identify and authenticate users securely who want to conduct online procedures with their citizen cards. The server-side MOA and the client-side citizen card software interact with each other to carry out identification and authentication using the identity link and the signature on the citizen card.

This logon process ensures the highest level of security for accessing records and accounts, carrying out bank transactions, and for all branches in which personal information and data is stored.

The MOA ID links a session to specific user data from the identity link, such as the sector-specific personal identifier, which the MOA ID calculates from the sourcePIN on the citizen card. The MOA ID includes functionality for accessing the citizen card environment, communicating with the browser and citizen card environment, authenticating and identifying citizens, businesses and authorities using the digital signature and identity link, calculating the ssPIN and forwarding the user's login information to the subsequent application. The layout of the Web pages that are used in these processes can be changed to match the organisation's corporate design.

After authentication is successfully carried out, the application requests the login data from the MOA ID over a Web service or a Java interface. Alternately, a proxy component can be used to transmit the login data over other protocols (e.g., in a HTTP header parameter) for Web applications that do not support Web services or internal Java calls. This makes integrating authentification processes into existing online applications easy and uncomplicated. However, new eGovernment applications should be designed so that proxy components are no longer necessary.

Through the use of sector-specific personal identifiers in business applications, the eGovernment Act allows the citizen card to be used for identification purposes in the private sector. The upgraded features developed in the MOA WID project for the creation and use of sector-specific personal identifiers have been integrated into the newest version of the MOA ID.

Public authority procedures can also be carried out online by third-parties on someone else's behalf, as long as a valid electronic proxy authority agreement exists between the parties. The MOA VV was originally created for this purpose. It was able to authenticate electronic proxy agreements and recognize proxy limitations. The functionality of the MOA VV was also integrated into the MOA ID+.

For professional representatives (e.g., lawyers, civil engineers or administrative officials, who have authority to act in accordance with §5(3) E-GovG), the certificate extension of the signature certificate in the citizen card shows that the representative is authorised to conduct electronic transactions on behalf of the principal. After the representative logs in with the citizen card, the MOA ID is able to forward his identification data along with data of the principal to the application. In contrast to electronic proxy representation, where the data of the representative can be viewed in the XML structure of the proxy agreement, the principal is identified by entering attributes such as name, date of birth and place of birth on the login pages. The principal is identified over a Web service from the sourcePIN Authority, which sends his registration data (e.g., his ssPIN) back to the MOA ID. The MOA ID then sends the data on the subsequent application.

What

No authentication authority is involved when using the Citizen Card. The service provider validates the citizen's qualified signature (created when entering the application) and the sourcePIN Register Authority's signature on the identity link (created during issuance).[66] Both validations may include consolation of a revocation service, but not an AA.

Assurance level

For the time being only for the level of a qualified signature an agreed level and a scheme of liability and supervision exists without further regulation required.

Therefore the Austrian eID concept limits itself to one single alternative for the time being:

Level 0 - Free access without further identification needs

Level 1 - Access using qualified signatures/Citizen card

[65] See Administration on the Net, p. 114

[66] Art. 4 (4) Austrian E-Government act : 'The authenticity of a submission made using the citizen card shall be validated by the electronic signature contained in the citizen card.'

Other

In order to ensure the protection of data, authorities are not allowed to store the sourcePINs of natural persons in their applications. The authorities may identify natural persons only by their sector-specific personal identifier (ssPIN). The ssPINs are derived from the respective person's sourcePIN. This process must be irreversible and it must not be possible to calculate the original sourcePIN back from the ssPIN. An ssPIN is valid only for the sector of activity of the authority under which the initiated procedure falls. Personal identifiers from other sectors may only be used in encrypted form.

Representation

Representation and delegation are handled in the Austrian E-Government act and can be handled by the Bürgerkarte.

On a technical level, an electronic mandate in Austria is a specific XML structure which is electronically signed by an issuing authority, i.e. the Source-PIN Register Authority. The issuing authority just asserts that the electronic representation bases on an existing and already established authorisation.

Electronic mandates are held by the representatives. Every time the representative makes use of a mandate, she has to use her own e-ID (Citizen Card) to prove her own identity. She must also declare to the e-Government application that she is acting rightfully in the name of the mandator by showing the electronic mandate.

The electronic delivery service[67] was one of the very first e-Government applications in Austria which accepted electronic mandates. Mandates are especially important for the Austrian electronic delivery service since legal entities are only able to register for electronic delivery with the use of electronic mandates (a private person has to act in the name of a legal entity). However, mandates are an important element of electronic identification systems in general and thus enrich the e-Government framework.

Austrian E-Government Act article 5: Citizen Card and Representation:

> 5. (1) Where the citizen card is to be used for submissions by a representative, a reference to the permissibility of the representation must be entered in the Citizen Card of the representative. This occurs where the sourcePIN Register Authority, having been presented with proof of an existing authority to represent or in cases of statutory representation, enters in the citizen card of the representative, upon application by the representative, the sourcePIN of the data subject and a reference to the existence of an authority to represent, including any relevant material or temporal limitations. The permission to receive documents (Paragraph 35(3) second sentence of the Service of Documents Act - ZustG;, BGBl. Nr. 200/1982) must be entered separately. Paragraph 4(3) shall apply mutatis mutandis to the entries in the Citizen Card which are required .
>
> (2) In cases of professional representation no particular proof of authority as in (1) to represent is required if the general authority to represent is evident from the notice of professional entitlement according to the professional regulations in the signature certificate. In this case, the sourcePIN Register Authority shall, upon application of the professional representative, provide the sourcePIN of the data subject directly to the citizen card enabled application where the official procedure is carried out. The general authority does not include the permission according to Paragraph 35(3) second sentence ZustG.
>
> (3) Provided that such a service is offered by authorities, officials (Organwalter) authorised especially for this purpose may, at a person's request, lodge applications for that person with all authorities, irrespective of their material and organisational competence, in procedures in which a Citizen Card may be used. The specific instruction issued by the citizen shall be documented and kept by the authority in an appropriate form. Applications shall be lodged using the citizen card of the official. The general competence of an official to lodge applications for citizens must be apparent from the signature certificate in the official's Citizen Card. In this case, the sourcePIN Register Authority shall, upon application of the official, provide the sourcePIN of the data subject directly to the citizen card enabled application where the official procedure is carried out. The general authority does not include the permission according to Paragraph 35(3) second sentence ZustG and the authorisation for deliveries (Paragraph 9(1) ZustG).
>
> (4) If the citizen card is used for acting as representative ((1)-(3)) it must be assured that

[67] The Austrian electronic delivery service is the electronic equivalent of postal registered letters. Public authorities may send notifications and documents through this service to citizens. In exchange, the citizen has to sign an acknowledgement of receipt.

1. the sourcePIN of the representative is also provided to the citizen card enabled application
2. the sourcePINs are only used for the generation of ssPINs by the citizen card enabled application

4.7 Conclusions

The Austrian eGovernment Act governs many aspects relating to the Austrian eID, some details are regulated in bylaws. Austria has a strong eID in the form of the Bürgerkarte which can be implemented in different forms: smart card, mobile phone and even USB devices.

The Bürgerkarte consists of a sourcePIN which is cryptographically derived (irreversible) from the ZMR number (citizen registration number) in the Central Register of Residents (for Austrian Nationals) or a registration number from the supplementary register for non nationals. The sourcePIN is linked to the rightful holder of the card by means on an Identity link, which is created by the sourcePIN Register Authority. The identity link (a digital signature) is stored on the Bürgerkarte.

The sourcePIN is kept under control of the Bürgerkarte holder. Relying parties may only use sector-specific personal identifiers (ssPINs) irreversibly derived from the sourcePIN. Creation of an ssPIN requires consent of the Bürgerkarte holder.

The Bürgerkarte allows for the authentication of the user without resorting to an Authentication Authority (although a revocation list may be consulted).

The Bürgerkarte only contains first name, last name, and date of birth. Furthermore an ssPIN could be provided, derived from the (secret) individual's sourcePIN). Additional attributes have to be obtained from the Central Register of Residents.

The Bürgerkarte allows for identification, electronic signatures, and (optional) representation.
Given the reliance on qualified electronic signatures, the Signature Act is relevant.

The Austrian infrastructure allows for the use of foreign smart cards (specifically those from: Belgium, Estonia, Finland, and Italy).

5 Country report: Belgium[68]

5.1 Structure of the Administration

Belgium is a federal constitutional monarchy. Executive and legislative powers are divided between the federal government, 3 regions and 3 communities (Dutch, French, German).[69] Each region and community has its own legislative and executive powers in its respective fields of competence, and its own parliament and government to exercise these powers. Legislative power at federal level is held by a bicameral parliament. The Federal government holds executive power at federal level.

The Belgian eGovernment structure consists amongst others of several web-portals, both on a federal as a regional level (e.g. www.belgium.be, launched 2002). Belgium has been a pioneer in the development and deployment of eID cards. Belgium plans to have 8 million eCards in circulation by the end of 2009. The eID card should replace a number of other cards for identification and authentication.

The Belgian eGovernment structure relies on the ‘authentic sources principle’. Some of these authentic sources are the National Register, The Crossroads Bank for Social Security Register, and The Crossroads Bank for Enterprises.[70]

An important (federal) actor in the field of eGovernment in Belgium is the Minister for Enterprise and Administrative Reform (responsible for the computerisation of the public services). This Minister holds responsibility for the work of the Agency for Administrative Simplification and that of the Federal Department for ICT (Fedict), which defines the common eGovernment strategy. Another actor, the Crossroads Bank for Social Security (CBSS), implements eGovernment services in the social sector.[71]

On a regional level, political responsibility for eGovernment lays at the prime ministers of the three regions. Local eGovernment initiatives are managed by the local authorities, in particular the municipalities.

5.2 Debate (and history)

EGovernment initiative in Belgium was launched in 1999 with a federal policy declaration called ‘The way to the 21st century’. Several other initiatives have succeeded this initiative, like the ‘Five Star Plan for the Development of the Information Society’ (2000), 'E-Gov - Towards electronic government in Belgium' (2001), the start of the development of the eID card in 2000 and its launch in 2003, and the eGovernment interoperability framework (2005).

5.3 eID model

The core component of the Belgian eID model is the electronic identity card, which needs to be rolled-out by 2009. The eID card contains a certificate for authentication purposes and a certificate for qualified signatures.

The National Registry (Rijksregister, since 1983) is an information processing system responsible for the information regarding the identification of natural persons.[72] The Registry is kept up to date with registers managed at the communal level (centrally kept, but locally maintained[73]). Identification of

[68] Based on analysis by the TILT team complemented by a country report written by Frank Leyman.

[69] Epractice.eu factsheet

[70] http://www.epractice.eu/document/3287

[71] http://www.epractice.eu/document/3285

[72] Fidis D16.1

[73] IDABC PEGS country report belgium, p. 14

the Belgian citizen is primarily based on the National Registry Number.[74] Many of the attributes stored in the authentication certificate of the eID card are obtained from the National Registry.

5.4 Principal legislation and policy documents

Legislation[75]:

- Law on the protection of private life with regard to the processing of personal data (1992) (M.B., March 18, 1993)
- Law laying down a legal framework for electronic signatures and certification services (9 July 2001)
- The Law of 15 January 1990 establishing and organising a Crossroads Bank of social security.
- Law on the use of Electronic Signature in Judicial and Extra-Judicial Proceedings (20 October 2000)
- Law transposing the directive 2003/98/EC on the re-use of public sector information (7 March, 2007)
- Royal Decree establishing the procedures and time limits for the handling of requests for public sector information re-use (29 October 2007)
- Act of March 25, 2003, amending the Act of August 8, 1983 governing the National Registry of natural persons and the Act of July 19, 1991 considering the registries of population and identity cards and altering the Act of August 8, 1983 governing the National Registry of natural persons. (B.S. 28 March 2003) (N. 2003 – 1169, S–C 2003/00234)
- Royal decree of March 25, 2003 considering the Identity Cards (B.S. 28 March 2003)
- Royal decree of March 25, 2003 considering a transitional arrangement for the electronic Identity Card (B.S. 28 March 2003).
- Ministerial Decree of March 26, 2003 governing the model of a basis-document envisioning the lay out of an electronic Identity Card (B.S. 28 March 2003).
- Royal Decree of November 30, 2003 altering Royal Decree of the Royal Decree of March 25, 2003 considering the transitional arrangement for the Electronic Identity Card. (B.S. 12 December 2003).
- Royal Decree of June 5, 2004 determining the system of rights for inspection and correction of the data the is recorded electronically on the Identity Card and the data that are recorded in the population registries or in the National Registry of natural persons (B.S. 21 June 2004)
- Royal Decree of September 1, 2004 altering the Royal Decree of march 25, 2003 considering transitional arrangement of the electronic Identity Card (B.S. 15 September 2004).
- Royal Decree of September 1, 2004 considering the decision to generally introduce the electronic Identity Card (B.S. 15 September 2004)

Policy:

- Resolution on a seamless eGovernment in order to implement the second co-operation agreement (2006).
- eGovernment interoperability framework BELGIF (2005).

[74] FIDIS D16.1

[75] http://eid.belgium.be/nl/Achtergrondinfo/Wetteksten/index.jsp; http://www.epractice.eu/document/3284

- The 'Fed-e-View' study (2004).
- The 'Kafka' initiative (2003).
- A co-operation agreement is signed in March 2001 for the development of a common platform for eGovernment services.
- Parliamentary review of eGovernment in Belgium, 'eGovernment at the Federal, provincial and local level' (January 2001).'E-Gov - Towards electronic government in Belgium' (August 2001).
- The ‘Five Star Plan for the Development of the Information Society’ (2000).
- The federal policy declaration entitled 'The way to the 21st century', which marked the official launch of eGovernment in Belgium (1999).
- Several ‘Computerisation strategic notes’ (issued annually until 2007).

5.5 Analysis

eIDentity: the Belgian eID Card (Belgian Personal Identity Card, BELPIC)

Name

The Belgian eID Card is the legal Identity Card for Belgians. Its purpose is to replace the functions of the preceding ID cards (travel document and proof of identity) as the official Belgian identity card, but adds several functions to them, like Internet authentication, electronic signatures, and the possibility to apply for official documents.[76] Moreover, in the future the Identity Card can be put into action as e.g. a library card, for making hotel reservations, etc.

The eID card has the form of a bank card protected with a pin code. The card contains a microchip with signed identity data, namely the holder’s name, date of birth, address, photograph, …, and X.509 digital certificates allowing authentication through the interenet or electronic signature of documents. The identity data, such as address, are not incorporated in the certificates. For use in the electronic environment, the card needs to be inserted into a card reader.[77]

Form

The format, distribution, and use of the Belgian identity Card are governed by the Act of July 19, 1991 considering the population registers and Identity Cards, which was amended by the Act of March 25, 2003 that introduced the electronic Identity Card (eID). The identity card contains a set of visual information (including a photo), a microchip (with certificates), and an optical field. As already mentioned, the Belgian eID should be used in combination with a card reader.

Eligibility

The identity card is only applicable to natural persons. The general eID card is issued to Belgian citizens and people mandated to reside in Belgium.[78] The card is mandatory for citizens over the age of 12.[79] For children below the age of twelve and for foreigners other electronic cards are under development, like the Kids-ID project.[80]

[76] See http://eid.belgium.be/nl/Welke_kaarten_/eID/

[77] See: http://www.cardreaders.be/en/default.htm

[78] eID interoperabilit report belgium, p15

[79] Royal Decree on identity cards (Koninklijk Besluit betreffende de identiteitskaarten, 25 maart 2003, N. 2003 - 1170) art. 1.

[80] http://eid.belgium.be/nl/Welke_kaarten_/Kids-ID/

Issuer

Cards are issued by the municipalities,[81] on behalf of the National Register. The cards are produced, initialised, and personalised by a private company[82]. Certificates are managed by Certipost, which is a joint venture of Belgacom and the Belgian Post, acting as the credential service provider. Card readers are issued by several organisations.[83]

Responsible authority

The responsible authority is the Ministry of the Interior.[84] The process of issuance and use of the Belgian eID is monitored by the Sectoraal comité van het Rijksregister, which resides under the Belgian Data Privacy Commission (Commissie voor de bescherming van de persoonlijke levenssfeer).[85]

Attributes

The visual information stored on the cards contains all the data that was originally printed on the traditional identity card, except the holder's address.[86] Moreover the visual part of the card contains a hand written signature of the holder.[87]

The card contains:

- National ID number – incorporates information on gender and date of birth
- last name
- first two first names
- first letter of the third first name
- nationality
- place of birth and date of birth
- gender
- place of issuance
- validity dates (start, end)
- photograph of the holder
- signature of the issuing civil servant and the card holder
- National Registry Number
- authentication-certificate and an electronic signature certificate
- place of residence of the holder[88]

The card does reveal the user's National Registry Number. The national register number is a unique identification number for Belgian citizens, appearing on the e-ID and its microchip. The legal framework for the use of the national registry number is laid down in

[81] IDABC PEGS Belgium Country report, p22.

[82] ZETES NV, see www.zetes.com

[83] Cf. www.cardreaders.be

[84] Royal Decree on identity cards (Koninklijk Besluit betreffende de identiteitskaarten, 25 maart 2003, N. 2003 - 1170) art. 12 para 2.

[85] Art 15 of the Act of August 8, 1983 governing the National Registry of natural persons.

[86] IDABC PEGS Belgium Country report.

[87] The Belgian Electronic Identity Card (overvieuw), De Cock et. al. (KUL)

[88] art. 14 B.S. 28 March 2003

- the law of 8 August 1983 on the national register
- the royal decree of 5 June 2004 laying down access and rectification rights of data electronically stored on the identity card and of information data stored in the population registers or the national registry

The national registry number was originally intended to be used for public sector applications only. As a result, only a limited number of institutions are allowed to use the national registry number in their internal processes.

With regard to the use of electronic signatures in eGovernment applications, the national register number is particularly relevant because it is used as the unique identifier in the certificate of the e-ID card (but not in commercial CA certificates). Furthermore, the national register number is also envisaged to become the identifier to be used in the future for all back-office information exchanges in eGovernment applications regarding all persons who hold such a number.

Providers of e-ID applications are only allowed to use the national register number in certain cases upon authorisation from a sector committee, which is a subdivision of the national privacy commission.[89] Only certain categories of authorities and instances qualify for this permission.

Nevertheless, a royal decree can determine the cases in which no authorisation is required. This is for instance the case for the exchange of information between institutions of social security.[90]

Conditions for use

Starting point is that everybody may ask for a proof of identity. Persons, however, are not always obliged to give this evidence. Authentication is bound by the Act on the protection of private life with regard to the processing of personal data, especially with regard to the proportionality of the request for data. Moreover, the legal restrictions for the use of the National Registry Number apply to the request for authentication. In some instances, an entity is obliged to prove his or her identity (Art 6 par. 7 of Act July 19, 1991 considering the registries of population and identity cards, etc.)[91]

On the condition that one complies with the Act on the protection of private life, the use of the eID card can also be requested by private parties.

The National Registry Number that is provided in the eID may not be used, processed, or stored, by parties that are not authorised to do this by the Sectoral Committee for the National Registry[92]. Several authorities that are mentioned in the Law qualify for such an authorisation.[93]

Creation and termination

The eID card is valid for five years to prevent imitation and forgery.[94] The eID card is mandatory for all citizens over the age of 12. The card is unusable before activation by the citizen. Hence, there is an option not to use the certificates on the card and only use it as secure identity data storage.

With the eID card, the holder of the card can verify which data of his is stored in the National Register. Updating this information is however not possible. When a citizen's address changes, the address recorded in the chip can be altered at the city hall.

[89] Article 6 of (N. 2003 – 1169, S–C 2003/00234)

[90] See the IDABC report ENTR/05/58-SECURITY/SC1/BE_Profile

[91] http://eid.belgium.be/nl/binaries/FAQ_NL_tcm147-22451.pdf Juridische FAQ bij de eID, p. 5

[92] http://www.privacycommission.be/nl/sectoral_committees/national_register/. Article 6 of (N. 2003 – 1169, S–C 2003/00234)

[93] http://eid.belgium.be/nl/binaries/FAQ_NL_tcm147-22451.pdf Juridische FAQ bij de eID, p. 7

[94] http://www.belgium.be/nl/familie/identiteit/identiteitskaart/kenmerken/

If an eID gets lost or is stolen, citizens can make use of the ‘card stop’ function, by informing the police or the municipality.[95]

5.6 Authentication Authority

Services that allow the user to use the eID card (including private sector applications) communicate with the middleware on the client PC (provided by the federal government (FEDICT) developed by ZETES[96], but also available from other providers) that allows the PC to read the card data.

Name

The authentication of the claimant is performed by the middleware running on the client's (claimant's) PC. Communication between service and client takes place through standard SSL/TLS protocol.

For the validation of electronic signatures created by means of the e-ID both Certificate Revocation Lists (CRLs) or the Online Certificate Status Protocol (OCSP) can be used:

- http://status.eID.belgium.be/ to retrieve the status of a certificate or to retrieve a CRL or a delta CRL;
- http://ocsp.eID.belgium.be/ for the OCSP responder.

5.7 Conclusions

The BelPIC can be used without resorting to an AA or CA. However, the certificates can be validated (through a CRL or OCSP).

Given the fact that providers of e-ID applications are only allowed to use the national register number in certain cases upon authorisation from the sectoral committee on the Rijksregister, a subdivision of the national privacy commission, the eID possibly can not be used for cross border authentication. Only certain categories of authorities and instances qualify for this permission*’*[97]

[95] http://eid.belgium.be/nl/Card_Stop/index.jsp

[96] http://ec.europa.eu/idabc/servlets/Doc?id=29071, p16

[97] IDABC eID interoperability for pegs, National profile Belgium, p.31, article 6 N2003–1169, S–C 2003/00234.

6 Country report: Estonia

6.1 Structure of the Administration

Estonia is a parliamentary republic. Legislative power lies within the unicameral parliament, called the State Assembly (Riigikogu in Estonian). Estonia’s Head of State is the President. The Government, exercising executive power, is formed by the Prime Minister and a total of 14 ministers.

Estonia is divided into 15 counties and 227 urban and rural municipalities (towns and parishes), whose powers and responsibilities are established by the Local Government Organisation Act of June 1993. The government of each county is led by a County Governor, who represents the national government at regional level. Local self-government is exercised solely at the municipal level.[98]

The Ministry of Economic Affairs and Communications holds political responsibility for the development and implementation of the state information policy.[99]

The backbone of the eGovernment environment is the X-Road network of distributed and central servers. X-Road is a platform-independent secure standard interface between databases and information systems (to connect databases and information systems) of the public sector, which has a common user interface and a standard authentication system. The X-Road enables secure access to nearly all Estonian national databases; ensures the necessary availability, integrity and confidentiality of electronic document exchange over the Internet servicing Estonian residents, the state and local government authorities.[100]

The issuance process of ID-cards and the development of PKI infrastructure is managed through a tight co-operation with public and private agencies. The production and personalisation of ID-cards, as well as certification services are outsourced by service contracts to TRÜB AG. TRÜB AG has two sub-contractors: AS Sertifitseerimiskeskus (hereinafter: SK) and Trüb Baltic AS. [101]

6.2 Debate (and history)

In 1997 the first steps were taken to develop an electronic ID card. In 2000 the digital signature act has been approved by the parliament. This act regulates the work of Certification Service Providers (CSPs) which have to be in the National Certificate Service Provider Registry. Identity documents in Estonia are regulated by the Documents Act. [102] Estonia started issuing national ID cards in January 2002. The card fulfils the requirements of Estonia’s Digital Signatures Act and is mandatory for all Estonian citizens and permanent resident foreigners over 15 years of age.

Estonia plays a proactive role towards the interoperability of electronic signatures in the EU, by proposing the ‘Universal Electronic Signature’ (http://www.openxades.org/ues/) concept, launching www.openxades.org and signing a Memorandum of Understanding with Finland in 2003. Due to the slow international uptake in the deployment/usage of the eID particularly in field of eSignatures, these initiatives have not been widely followed. [103]

[98] Factsheet - Estonia - Country Profile; epractice.eu, April 2008.

[99] Factsheet - Estonia - Actors; epractice.eu, April 2008.

[100] IDABC interoperability for PEGS country report Estonia, November 2007, p.10.

[101] IDABC interoperability for PEGS country report Estonia, November 2007, p.10.

[102] Modinis IDM Country report Estionia.

[103] Factsheet - Estonia - National Infrastructure; epractice.eu, April 2008.

6.3 eID model

Actors in ID-card issuance and management are the Citizenship and Migration Board (CMB) which is responsible for document issuance including Estonian ID-cards, the production and personalisation of ID-cards, as well as certification services are outsourced by service contracts to TRÜB AG and the last actor is the Certification Centre.

The ID-card consists of private keys and certificates. In the certificates the national unique ID number is stored and used as a key in every database.

Besides ID-card there is also mobile PKI in place (called "Mobile-ID") which is currently provided by just one GSM operator (EMT) and haw around 10 000 users.

Banks have their own means for authentication to Internet banking services. Usually people have password cards but OTP tokens are also used (10-15%). Banks do support PKI-based login as well and are encouraging people to use ID-card and Mobile-ID. In the same time they still are providing authentication services to third parties.

There is no official policy for authentication levels. The public administration encourages use of PKI-based methods (ID-card and Mobile-ID) whereas usage of "bank authentication service" using passwords is still supported by many services. [104]

6.4 Principal legislation and policy documents

Legislation:

The main legal acts concerning e-IDM systems are the Identity documents act[105], the Digital signature act[106] regarding ID-card certificates, the Population register act[107] and the Personal data protection act[108] regarding the Personal Identification Code (PIC).

The legal basis for the issuance and usage of certificates on ID-cards is the Identity documents act.

The Estonian legislation distinguishes between the authentication and digital signing. The general regulation (not application based) about digital signatures exists in the Digital signature act. The Digital signature act provides the necessary conditions for using digital signatures and the procedure for exercising supervision over the provision of certification services and time-stamping services. The Digital signature act was drafted in accordance with the European Councils regulation in EC 1999/93. [109]

With the rise of cyber-theft, banks have been starting to change their thinking and policies towards provisioning of the authentication services and use of password cards in general. As a result, a co-operation agreement was signed between major banks, major telecom companies and the Government in May 2006 with code-name "Computer Protection 2009".[110]

[104] Country report Estonia by Tarvi Martnes and Kartrin Laas, Estonia.

[105] English: (2004) http://www.legaltext.ee/text/en/X30039K10.htm. NOTE: dead link, document found here: http://www.unhcr.org/refworld/category,LEGAL,,,EST,4728ab1b2,0.html

[106] English: http://www.legaltext.ee/text/en/X30081K4.htm.

[107] English: http://www.legaltext.ee/et/andmebaas/ava.asp?m=022.

[108] English: http://www.legaltext.ee/text/en/X70030. htm.

[109] IDABC interoperability for PEGS country report Estonia, November 2007, p.20.

[110] http://www.sk.ee/pages.php/02030201,1107

There are no general regulations about authentication or legal acts which would define the hierarchy of the different authentication systems.[111]

Policy:

Few issues related to eID use in public sector are addressed in document "Estonian IT Interoperability Framework" http://www.riso.ee/en/files/framework_2005.pdf

Otherwise there are no written policy documents besides of legislation in place.[112]

6.5 Analysis

eIDentity: Identity card (ID-card)

Name

Identity card e.g. ID-card and mobile-ID.

The eID is a multifunctional card: it is a regular identity document, it functions as an electronic identity and it can be used to generate digital signatures.[113]

The eID is meant to be the primary document for identifying citizens and residents and its functions are to be used in any form of business, governmental or private communications (identification document) and as a travel document (within the EU). In addition to being a physical identification document, the card has advanced electronic functions facilitating secure authentication and legally binding digital signature for public and private online services.[114]

The new mobile-ID service (wireless PKI) was launched in May 2007 by mobile operator EMT, in cooperation with several banks and the Certification Authority AS Sertifitseerimiskeskus (SK). This service allows accessing Internet banking services without entering eBanking codes.[115]

Form

The ID-card has three main functions: visual identification, authentication and digital signing. The identity card e.g. ID-card is the physical polycarbonate card containing a contact chip with a personal data file (all data personalised to the visual card) and two X.509 certificates:

1. authentication certificate for electronic identification, encryption and digital signing of e-mails;
2. digital signature certificate for creating electronic signatures according to the Estonian Digital Signature Act.

The certificates contain only the holder's name and Personal Identification Code (PIC). In addition, the authentication certificate contains the holder's unique e-mail address. Associated with the certificates are two private keys which are protected by two different PIN codes. The certificates are suspended if the card is lost and verifiers should query the certificate database.[116]

The ID-card certificates are linked to the various registers through the PIC, which functions as a unique identifier for Estonian citizens and residents in eGovernment services.[117]

All the above mentioned data except photo and handwritten signature are also present on the chip in electronic form, in a special publicly readable data file. The chip also contains two certificates, allow-

[111] IDABC interoperability for PEGS country report Estonia, November 2007, p.19.

[112] Country report Estonia by Tarvi Martnes and Kartrin Laas, Estonia.

[113] Modinis IDM Country report Estonia.

[114] Factsheet - Estonia - National Infrastructure; epractice.eu, April 2008.

[115] Factsheet - Estonia - National Infrastructure; epractice.eu, April 2008.

[116] Modinis IDM Country report Estionia.

[117] IDABC interoperability for PEGS country report Estonia, November 2007, p.9.

ing the authentication of the citizen and the use of a qualified electronic signature and their associated private keys protected with PIN codes. [118]

Although the ID-card is an important eIDM system, it is not the most used system today. Estonia has relatively long tradition of Internet banking and nearly everyone has access to it. Banks are providing authentication services to third parties, including eGovernment systems. The PIC has also here the function of unique identifier in the authorisation process.[119]

Another eIDM system is the Mobile-ID. It is a development of the traditional eID card-based authentication and digital signing; the SIM card of one's mobile phone has become an identity document just like the eID card. Similarly to the eID card, the mobile-ID enables authentication and digital signing of documents. 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 code.

Eligibility

ID-card is mandatory for Estonian citizens from age 15 and up [120] (younger than 15 have an option to apply for ID-card) and all aliens residing permanently in Estonia on the basis of a valid residence permit or right of residence irrespective of their age.[121]

Identification information with regard to legal persons is provided through the Centre of Registers and Infosystems. Although companies and organisations have a unique register code, there is no such thing as "eID of the company". All transactions with regard to legal persons are performed by physical persons using their personal eID; corresponding access rights are maintained separately. [122]

Issuer

Issuance of ID-card as well further operations is done in close public-private partnership.
Documents are issued by the CMB (Citizenship and Migration Board) regional offices.

CMB is the government organisation responsible for issuing identification documents including ID-card and maintains the Database of Identity Documents (and related personal data). CMB is the identity provider:

- CMB processes applications for ID-card;
- decides on the issuance of documents and;
- hands ID-cards with PIN codes over to applicant;

AS Sertifitseerimiskeskus (SK) functions as CSP and Validation Authority:

- maintains the electronic infrastructure for issuing and using the certificates on ID-card;
- issues the certificates and personal data file on the ID-card chip;
- develops and maintains the associated services and software;

TRÜB Baltic AS personalizes ID-cards. [123]
The reliability of ID-card is based on the chain of documentation (application processing, personalisation etc), where the actual physical document is one of the most important links. An important role in the issuance process of ID-cards and related identity management is played by the database of identity

[118] Country report Estonia by Tarvi Martnes and Kartrin Laas, Estonia.

[119] IDABC interoperability for PEGS country report Estonia, November 2007, p.9.

[120] Para 5 (1), jo para 19 Identity documents act.

[121] Para 7, jo para 19 Identity documents act.

[122] IDABC interoperability for PEGS country report Estonia, November 2007, p.9.

[123] Country report Estonia by Tarvi Martnes and Kartrin Laas, Estonia.

documents issued by the CMB.[124] This database contains the information on all issued identity documents (including the ID-card) and relevant data of document users and document applicants that are necessary for the issuance of identity documents to the eligible persons. The main purpose is to ensure that the eligible person has the appropriate document (included by identification of the person and check of the right to the identity document). The database also contains the data of all valid and non-valid documents and document applications the person has submitted. Since 2001 the face images of document users are entered into the database. Most of the population is documented, therefore it is possible to verify the information submitted by applicants against the entries of the database and check his/her identity. If the applicant has not yet had a document issued by the CMB, he/she needs to provide additional source documents proving the applicant has the right for the identity document (citizenship).[125]

The identity documents for aliens are issued on the basis of his/her residence permit or the right of residence in Estonia. So the database has a connection with national Aliens‘ registry (CMB is the responsible authority). The database consists of a central online database and a paper database (source documents etc). The issuance process (including logistics etc.) and personalisation process of ID-card is based on and monitored by the online database. [126]

Responsible authority

CMB is the responsible authority for issuing ID-card. CMB has contractual agreement with TRÜB detailing the relevant outsourcing of responsibilities (sub-suppliers are Trüb Baltic AS and AS Sertifitseerimiskeskus).

From a certificate issuance point of view – all the responsibility of certification procedure relies on AS Sertifitseerimiskeskus (TRÜB has the contract for supply the certification service). CMB, TRÜB Baltic AS, banks and also hotline for certificate suspension act as Registration Authorities of AS Sertifitseerimiskeskus. AS Sertifitseerimiskeskus has an insurance policy (required by the Digital Signatures Act) in excess of 5 million kroon (around €32,000) for covering possible damages caused by misbehaviour of AS Sertifitseerimiskeskus or its contractual partners in certificate issuance or validation information provision process.[127]

Attributes

An electronic processor chip contains a personal data file as well as a certificate for authentication (along with a permanent email address (Forename.Surname@eesti.ee) for eCommunications with the public sector) and a certificate for digital signature, and their associated private keys protected with PIN codes. The data file is valid for as long as the identity card, and so are the certificates, which have to be renewed every five years.[128]

It should be noted that, while the signature certificate is considered to be qualified, the authentication certificate has deliberately not been given this label. This choice was justified by concerns of legal certainty: the authentication certificate should not be used for signature purposes, and for this reason only the signature certificate is considered qualified. This way, parties are expected to take adequate precautions to ensure that the authentication certificate is not misused.[129]

[124] The legal base is the decree of the general director of Estonian Citizenship and Migration Board from 19th March of 2003 no 72.

[125] IDABC interoperability for PEGS country report Estonia, November 2007, p.13.

[126] IDABC interoperability for PEGS country report Estonia, November 2007, p.13.

[127] IDABC interoperability for PEGS country report Estonia, November 2007, p.24.

[128] Factsheet - Estonia - National Infrastructure; epractice.eu, April 2008.

[129] Country report Estonia by Tarvi Martnes and Kartrin Laas, Estonia.

Both personal certificates must contain the following data:

1. certificate issuer data;
2. certificate owner data;
3. certificate validity data;
4. technical certificate data.

Personal certificates contain the following technical certificate data:

1. certificate format version;
2. certificate serial number;
3. certificate signing algorithm;
4. validity period of the certificate;
5. public key in the certificate and its presentation algorithm;
6. CSP public key identifier;
7. person's public key identifier;
8. key usage;
9. certificate policy identifier and reference;
10. reference to CDP (CRL Distribution Point);
11. person's e-mail address (only in authentication certificates);
12. CSP additional data;
13. extended key usage (only in authentication certificates);
14. identification of qualified certificate.

To secure the card there are a number of complex physical security elements, and the owner is the only one who knows the PIN codes and PUK code necessary for using the card electronically (signing documents digitally, for example). The authenticity of the digital signature is verified and conveyed to the other party by the Certification Center Ltd, which maintains a list of suspended and revoked security certificates.

The 11-digit PIC consists of:

gender/century of the birth digit (1),

date of bight digits (2+2+2),

three random digits (3)

and one checksum digit (1).

Use of the PIC is regulated with the Personal Data Protection Act which states in §16 that:
"Processing of a personal identification code is permitted without the consent of the data subject if processing of the personal identification code is prescribed in an international agreement, an Act or Regulation."
As a result, almost all databases in all sectors (including private sector) would ask for permission to process the PIC and use PIC as a primary key in database records to identify persons. This makes cross-usage of the databases technically possible.[130]

Exchange of information

As mentioned before certificates contain the name of the person, the PIC (containing gender/century of the birth digit and the date of birth) and persons e-mail address. The ID-card does not contain additional information about the holder. The data can be found in different databases. The most databases are accessible for citizens, local governments and public sector through the platform-independent se-

[130] IDABC ENTR/05/58-SECURITY/SC1/EE_Profile

cure standard interface between databases and information systems of the public sector – X-road. X-road is accessible for these users through authentication with the ID-card or by use of authentication services provided by the Estonian commercial banks.

To exchange the additional data across borders – for example data about address and study has to be agreed in bilateral contracts between persons/organisations that need to exchange the information. Please note that according to Estonian Personal Data Protection Law, the data subject has to give the written consent in this case.[131]

Conditions for use

ID-cards can be used for authentication and digital signing in all kind of e-services (public as private sector services). There are no restrictions. There are restrictions to use the Bank e-ID and an obligation to use ID-card or the other PKI based eIDs for the authentication in certain services. This approach is service-based.

Terms of use for ID-card shall be introduced to the ID-card applicant. Terms of use for ID-card contain reference and requirements of the certification policy that shall be followed in certification and certification servicing procedures.[132]

Creation and termination

Termination of ID-card or revocation of certificates can be done by CMB or SK registration authority by request of ID-card holder. Suspension of certificates can be done by CMB, SK registration authority or Help Line. The Help Line shall take Client calls 24 hours a day 7 days a week. There is no electronic transaction possible with suspended certificates. It is possible to terminate the suspension of certificates. The data about all operations with certificates are immediately recorded in the certificate database.[133]

CMB of the Ministry of Interior is responsible for document issuance including Estonian ID-cards. ID-cards are provided centrally whereas CMB has around 18 offices across the country. CMB partners with private sector for card manufacturing/personalisation and certification services as illustrated below.[134]

The card issuing process consists of the following steps: [135]

- The applicant fills in and submits application for the card to CMB indicating the office where he or she would like to receive the card. Applications for issuance of ID cards can be submitted to CMB:

- in person (80 %)

- by mail

- digitally through a website (requires ID card with valid certificates);

- CMB enters the data into the information system (The database of identity documents issued by the CMB);

[131] Country report Estonia by Tarvi Martnes and Kartrin Laas, Estonia.

[132] More about terms of use for ID-card certificates can be found on

http://www.pass.ee/index.php/pass/eng/id_card/terms_of_use_for_the_national_id_card_certificates. See certification policy of Estonian ID-card in more detail:

http://www.sk.ee/pages.php/0203040504 (look for ESTEID-SK policy).

[133] Country report Estonia by Tarvi Martnes and Kartrin Laas, Estonia.

[134] Country report Estonia by Tarvi Martnes and Kartrin Laas, Estonia.

[135] IDABC interoperability for PEGS country report Estonia, November 2007, p.17.

- CMB decides to issue the document. (Since the most of the submitted applications are recurrent applications, the information submitted by applicants is verified against the entries of the database. If the applicant has not yet had a document issued by the CMB, he/she needs to provide additional source documents proving the applicant has the right for the identity document);
- The personalisation order is then pieced out based on the scanned and alphanumeric data presented in the application and entered into the information system;
- CMB forwards the personalisation order to TRÜB Baltic AS;
- The procedure of the personalisation of the card are carried out in the following steps:
  - TRÜB Baltic AS personalises the physical card layout;
  - TRÜB Baltic AS gives the card the order of generating private keys (internal function of the card, the keys will never leave the card) and prepares the secure PIN envelopes;
  - TRÜB AS formulates certificate requests (2 per card) and forwards them to SK;
  - SK issues the certificates, stores them in its directory and returns the certificates to TRÜB Baltic AS;
  - TRÜB Baltic AS stores the certificates and personal data file on the card chip;
  - TRÜB Baltic AS prepares the final delivery envelope, enclosing the card, secure PIN envelope and an introductory brochure;
  - TRÜB Baltic AS hands the final delivery envelope over to CMB;
  - CMB sends delivery envelope to the local office specified in the original application (done using security couriers);
- Applicant receives the delivery envelope (containing card and PIN codes) from the local office of CMB;
- Upon receipt of the card, the card and certificates are activated.

The most popular method for authentication today is to use Internet bank authentication. Virtually all banks provide authentication service to third parties. This works in practice as follows:

- the user logs into the Internet bank (using the appropriate method)
- the user selects “external e-service”
- user’s PIC is securely communicated to the e-service
- user continues work with selected e-service

There are basically 3 methods for logging into Internet bank:

- password cards (with 24 codes) – around one million cards issued
- PIN-calculators – estimated 50 000 in use
- ID-card – over one million issued

Password-based authentication is the most (estimated – 90%) used method for Internet bank logging today. It is considered relatively secure as these password cards are issued personally in the bank office. Trustworthiness of banks is generally considered as good. Considering this, it is not surprising that number of eGovernment services make use of the bank authentication.

Mobile-ID

In order to authenticate oneself securely with the mobile-ID, the user will click on a dedicated button in the web environment. Upon completion of this action, he/she will be requested to enter his authentication PIN number. Once this operation completed, authentication is performed. The same process applies to the signing of digital documents.[136]

Digital signing with the mobile-ID has the same legal value as that of the eID card. When using the mobile-ID, no separate eID card and card reader is needed, as the phone itself already performs both functions.

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 in it. One of the objectives of the Computer Protection 2009 initiative is to get at least 200 000 people using the mobile-ID for authentication and digital signing by 2009.[137]

6.6 Validation Authority

In the PKI environment there is no need for any Authentication Authority. Authentication is performed between Service Provider (SP) and certificate holder in direct manner. For verifying certificate validity the SP user services of Validation Authority.

VA services are provided by AS Sertifitseerimiskeskus (hereinafter: SK) and Trüb Baltic AS in Estonia. SK serves validity information of ID-card certificates using standard OCSP protocol.

For Mobile-ID SK runs a proprietary SOAP-based webservice for performing full authentication process involving user interaction in mobile phone and certificate validation. From that perspective SK acts as AA with Mobile-ID.

SK takes full contractual liability of correctness of validation information – OCSP responses are signed. For extra protection SK runs an internal secure log system recording all OCSP responses issued. This log contains also records about changes of state of certificates.

SK validation and Mobile-ID services are available to everyone in contractual basis.

Interoperability

The system is designed to be used with almost any foreign ID-card provided that it provides Microsoft CAPI compatible CSP and OCSP service is provided. It has been demonstrated that Digidoc system works perfectly with Finnish and Belgium ID-card. Digidoc supports today both classical XAdES-X-L format with time-stampinstamp) used in Estonia.[138]

Liability issues

The national ID-scheme organizational scheme consists of triangle consisted of CMB, TRÜB and SK. From card-issuance point of view – all the responsibility lies on CMB. CMB has contractual agreements with TRÜB and SK detailing relevant outsource of responsibilities. From certificate issuance point of view – all the responsibility of certification procedure relies on SK. CMB, TRÜB, banks and also hotline for certificate suspension act as Registration Authorities of SK. SK has an insurance policy (required by the DAS) in excess of 5 million kroon (around €32,000) for covering possible damages caused by misbehaviour of SK or it's contractual partners in certificate issuance or validation information provision process.[139]

6.7 Conclusions

Estonia has a widespread system of eID cards, comprising the national ID card, bank cards and mobile-IDs. All make use of digital certificates that are issued in a controlled process. Central to the eID

[136] Factsheet - Estonia - National Infrastructure; epractice.eu, April 2008.

[137] Factsheet - Estonia - National Infrastructure; epractice.eu, April 2008.

[138] From IDABC, ENTR/05/58-SECURITY/SC1/EE_Profile, p. 26

[139] From IDABC, ENTR/05/58-SECURITY/SC1/EE_Profile, p. 15

is the unique PIC (Personal Identification Code (PIC). Use of the PIC is regulated with the Personal Data Protection Act and requires a legal basis (consent of the holder and rooting in Act, Regulation or International Agreement).

Authentication of the holder can be performed locally by the client middleware. VA services are provided by AS Sertifitseerimiskeskus (hereinafter: SK) and Trüb Baltic AS.

7 Country report: France[140]

7.1 Structure of the Administration

France has the characteristics of a parliamentary democracy. Legislative power lies with a bicameral parliament. Some powers of the State are transferred to the regions (22), counties ("departments") (96), and municipalities (36.500).[141]

Some of these administrative authorities provide e-services. For example, the ministry of finance offers VAT declaration and Income Revenue declarations to be done electronically since 2004. These are the most commonly e-services used.

The Minister for the Budget, Public Accounts and Civil Service carries political responsibility for eGovernment. This Minister is 'rapporteur' of the Council for the Modernisation of Public Policies (CMPP), which decides on the actions that need to be taken with regard to the modernisation of the French State.[142]

Official documents (identity cards, passport and driver's license) are under the responsibility of the Ministry of Interior but they are delivered by municipalities or departmental administrations.

In 2003, an agency called Agence pour le développement de l'Administration Electronique (ADAE) was created and replaced in 2006 by the Direction Géneral de la Modernisation de l'Etat (DGME). One of the missions of both organisations was to define policies for e-administration or e-gov services. Three documents are going to be published, drafts already exist, which are general directories: one for interoperability, one for security and one for accessibility.[143]

One component of the French eGovernment structure is the website 'Service-Public.fr', which was launched in October 2000 and gives access to more than 40 online services to citizens.[144] This portal will be complemented with an application called mon-servicepublic.fr which will be the single access point to all e-gov services. Mon-servicepublic.fr will also provide a

.

7.2 Debate (and history)

French initiatives in the field of eGovernment date from before 2000, with for example the introduction of the electronic health insurance card (Vitale Card) and the drafting of the Governmental Action Programme for the Information Society (1998), succeeded by, amongst others, the launch of an eGovernment portal in 2000 (service-public.fr), a Plan for a Digital Republic in the Information Society (Re/SO 2007, 2002), a Common Interoperability Framework (2002), he creation of the ADAE in 2003, the PSAE Plan and ADELE Action Plan (2004) and the electronic ID card project (launched 2005).

The launch of the national French eID card, called INES, was planned in 2005 but has been subject to a societal debate, which resulted in a critical report from the French Internet Rights Forum requesting that the eID scheme would be revised in order to address privacy and security issues.[145] Another de-

[140] Based on analysis of the TILT project team and a coutnry report by Martine Schiavo and Perica Sucevic, France.

[141] www.epractice.eu factsheet France

[142] CF. www.modernisation.gouv.fr

[143] Country report France by Martine Schiavo and Perica Sucevic, France.

[144] IDABC eSignatures report on France

[145] IDABC country report France on eID interoperability

bate considered the Vitale Card, which is used for identification and authentication purposes in the health domain since 1998. The card's security measures and management have both been subject to debate, which resulted in the introduction of an updated version of the Vitale Card.[146]

A new project for a national e-ID card with some personal attributes and 2 certificates (one for authentication, one for signature) is under study and the eId card should be delivered before the end of 2009 if the legislation is passed. This eID card is also under the responsibility of the Ministry of Interior but will be delivered by municipalities or departmental administrations.

Many services are provided through a central portal http://www.service-public.fr/demarches24h24. Through this portal the French government offers a large series of electronic services to citizens, professionals and local communities (collectivités locales). The objective was to create 300 additional new electronic services in 2007. The most frequently used services are 1) requests for a birth certificate, 2) notifications of home address change, and 3) access to the health insurance account. The portal is permanently modified and updated.[147] The portal in 2007 offered about 40 online services to citizens. These services are classified in 9 themes: a) my family, b) my health, c) my work, d) my studies, e) my "papers" (mes papiers), f) my life as a citizen, g) my travel, h) my home and i) my taxes. Typical services are: applications for family allowances or student's scholarships, notification of home address changes or exchange of health insurance forms. The "work" category contains services such as: requests for unemployment insurance, online calculation of pension, online job search, etc. Under "my life as a citizen" the users have e. g. possibilities for online payment of traffic fines, online application for automobile registration (so-called "carte grise"). The portal offers further online requests for all kinds of administrative certificates (for example: birth certificate) and, of course, online tax declaration.

7.3 eID model

In France, there is no common ID number. ID numbers can only be used within the scope of the sector which has generated these ID numbers (i.e. security social numbers can only be used in the social sector). Information about natural persons is recorded in a national directory (RNIPP), which can not be accessed through the internet. Every individual that is born in French territory or who becomes a beneficiary of the French Social Security obtains a National Registration Number (NIR). Use of the directory and the NIR is regulated by the French Law on Informatics and Liberty and Decree 83-103 of January 1982. Use of the NIR as a common identifier is prevented and requires permission by the CNIL. The NIR is based on gender, and year, month, province, and city of birth of the individual. Hence, the number carries information about the individual it relates to.

Official documents are: identity cards, passport and driver's license. There are under the responsibility of the Ministry of Interior but they are delivered by municipalities or departmental administrations.

Currently, the e-gov services are service providers but also identity providers and attributes providers. Some services first register the citizen by providing a username and password and then allow them to identify and authenticate themselves. Other e-gov services allow the citizen to choose his/her username and password.[148]

The eID model in France in the field of social security relies on the use of the Vitale Card (a smart card). Some municipalities offer local public services accessed with a Daily life Card.[149] As mentioned

[146] http://www.epractice.eu/document/736

[147] Source IDABC, ENTR/05/58-SECURITY/SC1/FR_Profile. This reflects the status on the 1st of March 2007.

[148] Country report France by Martine Schiavo and Perica Sucevic, France.

[149] Cf. http://www.cvq.fr/

above, the national identity card project should become an important means of electronic identification in the future, but has been delayed due to public debate.[150]

A new service will be launched at the end of this year: mon.service-public.fr. This service will allow the citizen to create his/her personal account to access some e-gov services. It will be the single access point to all the e-gov services. The citizen chooses his/her username and password and so creates his/her account. After he/she can federate all identities he/she already has for other e-services. When the identities are federated, and when he/she is authenticated by mon.service-public.fr, he/she can access the other e-services without being authenticated again.

It will be always allowed to access the e-gov services directly by using the specific username and password for these services. Being first authenticated by a service will not allow the federation of identities without being authenticated again by mon.service-public.fr.

Mon.service-public.fr will provide a secure storage space to register personal data or personal relevant documents to be exchanged with e-gov services.

Mon.service-public.fr and the partner e-gov services are based on the Liberty Alliance specifications.

When the national eID card will be available, the citizen will be authenticated by mon.service-public.fr with his/her authentication certificate.

Only the electronic certificates provided by ‘qualified’ Certification Service Providers (CSPs) are recognised for being used by citizens and businesses for online interactions with the Government.[151]

7.4 Principal legislation and policy documents

Legislation:
1999/93/EC on electronic signatures:

- Law n°2000-230 of 13 March 2000 implementing Directive 1999/93/EC by adapting the civil rules of evidence in order to make electronic signatures legally acceptable.
- Decree n°2001-271 of 30 March 2001: for enforcement of the article 1316-4 of Civil Code and relative to the electronic signature
- Order of 26 July 2004 relative to the recognition of the qualification of the certificates service providers and to the accreditation of the bodies which certify them.

95/46/EC Data Protection Directive:

- Law n°2004-801 of 6 August 2004 relating to the protection of individuals with regard to the processing of personal data modifying law n° 78-17 of 6 January 1978 relating to data processing, files and liberties.

2002/58/EC privacy and electronic communication:

- Decree n°2005-862 of 26 July 2005 relating to the conditions to create and manage networks and to provide e-communication services.

2006/123/EC Services Directive:

- To be transposed before 28 December 2009**.**

Other legislation and regulation :

[150] IDABC country report France on eID interoperability

[151] http://www.epractice.eu/document/3350

- Law number 2004-1343 of 9 December 2004 (simplification law). Allowed the government to rule by way of ordinance in matters related to electronic administration and e-gov services.
- Ordinance n°2005-1516 of 8 December 2005 for the enforcement of the previous law, relating to the electronic exchanges between administration users and administrative authorities and between administrative authorities.
- This ordinance announces a General Security Directory which lays down the rules which must be respected by the functions of the information systems participating to the security of the exchanged data.
- It announces also a General Interoperability Directory which lays down the rules which must be respected to ensure the interoperability of the information systems.
- Decrees relative to this order are in preparation (they will be published before the end of this year). One of these decrees is relating to the qualification of the trustworthy service providers and to the accreditation of the bodies which certify them. Once qualified for a service and a security level, the trustworthy service providers can request that the qualified offer is referenced, some interoperability tests are performed. Then the offer can be used for all administrative information systems requiring this type of offer and this security level. The supervision is done by a State body: DGME.

The General Security Directory should be published by the end of this year. A draft is available on Internet.

The General Interoperability Directory should be published at the beginning of next year. A draft is available on Internet.[152]

- Loi no. 2004-575, June 2004 (i.e. on liability of certification service providers)
- Decree of 2 March 2007 relative to the Interoperability general frame of reference.
- Decree no. 2002-535, April 2002 (security level of IT products and systems)

Policy:

For historic purposes only, these documents are outdated.

- Electronic Administration Strategic Plan (PSAE) / Electronic Administration Action Plan (ADELE) (2004)
- Action Plan RE/SO 2007 for a Digital Republic in the information society (2002)
- The Governmental Action Programme for the Information Society (1998)
- Development of the Digital Economy by 2012, Plan France Numérique 2012 http://francenumerique2012.fr/
- Following this plan, a plan for the egovernment services is in development.

7.5 Analysis

eIDentity: Username and password:

Some services first register the citizen by providing a username and password and then allow them to identify and authenticate themselves. Some of the e-gov services allow the citizen to choose his/her username and password. Most of the actual e-gov services replace the filling in a form or allow printing an official document.

Form: Username and password

[152] Country report France by Martine Schiavo and Perica Sucevic, France.

Eligibility:
Everyone can apply for an 'account' at the governmental portal http://mon.service-public.fr/.

7.6 Authentication Authority

Currently, all service providers are also authentication authority. With mon.service-public.fr, a centralized AA will be available. This AA will be the one for the French citizen involved incross-border service.

Name
mon.service-public.fr

What:
Presently, username and password chosen by the user and optionally an OTP via SMS

Responsible authority
mon.service-public.fr is under the responsibility of DGME.
Input:
Username and password chosen by the user and optionally an OTP via SMS.
Once authenticated, the user has access to his/her account and can federate all identities he/she already has for other service providers provided that these service providers are partners of mon.service-public.fr

Output:
A federation key and the level of authentication are sent to the service provider (ID FF1.2, IDW SF 1.1, SAML 1.1)
There are no partners from the private sector planned now.

For whom
Mon-service.public.fr can be used by everyone now.
A relying party can use the AA of mon-service.public.fr only if it is a partner and can handle Liberty Alliance based identity exchanges.

Process
Input : Username and password
Output : access given to mon-service.public.fr or a federation key and the level of authentication are sent to the service provider(ID FF1.2, IDW SF 1.1, SAML 1.1). Legally, the authentication process must comply with the General Security Directory.

Assurance level
Because the user can choose his/her username and password for mon-service.public.fr and as there is no control, there is no assurance.

eIDentity: National eID card
The future National eID smart card should be based on the ECC standards. It should be divided in 2 parts, one part similar to the passport as a travel document, and the second part for the e-services. It should replace the current plastic national ID card.

As a national ID card, it will be under the responsibility of the Ministry of Interior and will be delivered by municipalities or departmental administrations. The enrolment should be done by providing Identity documents in person by the citizen. Two certificates should be incorporated on the eID card (level 2 or 3 stars TBC)

The future eID card has to follow the General Security Directory rules for the e-gov services. The General Security Directory defines 3 security levels for certificates.

The authentication certificate which should be stored in the future national eID card should be used to authenticate the user. With a level 3 stars authentication certificate, the citizen is allowed to access all e-gov services requiring 1, 2 or 3 stars security level authentication certificates. The registration to the e-gov services has to be performed.
The future national eID card should also store some attributes as for example: name, surnames, date of birth, gender, place of birth and address.

Form:
A personal authentication certificate stored in a smart card (eID Card)

Eligibility:
The eID card will be delivered only to French citizens.

Issuer
The eID card is issued by the Ministry of Interior. It must be requested through municipalities or departmental administrations and is delivered by them.

Responsible authority

The Ministry of Interior.

Attributes

The future eID card should contain 2 certificates, one for authentication, and one for signature .
The future national eID card should also store some attributes as for example: name, surnames, date of birth, gender, place of birth and address
Attributes not stored in the eID card will have to be requested to the right ministry. This functionality does not exist now. It has to be developed for all attributes.

Conditions for use

The future national eID card should be used for the e-gov services. It should be a personal ID card and should contain 2 personal certificates. There are some discussions about the use of the eID card in the private sector especially for the use of the certificates.

Creation and termination
The eID card and the 2 certificates should be issued for 5 years. The certificates should be 2 or 3 stars security level.

Authentication Authority

Currently, all service providers are also authentication authority. With mon.service-public.fr, a centralized AA will be available. This AA will be the one for the French citizen involved incross-border service.

Name: mon.service-public.fr

What:
Presently, username and password chosen by the user and optionally an OTP via SMS
In the near future, the authentication certificate in the eID card.

Responsible authority
mon.service-public.fr is under the responsibility of DGME.

Input (looking for better term)
Authentication of the user should be done on the basis of the ID card. The certificate should be validated via the VA/AA.
Once authenticated, the user has access to his/her account and can federate all identities he/she already

has for other service providers provided that these service providers are partners of mon.service-public.fr

Output
A federation key and the level of authentication are sent to the service provider(ID FF1.2, IDW SF 1.1, SAML 1.1)
There are no partners from the private sector planned now.

For whom
In the near future, only French citizen with a national eID card should be authenticated using a certificate. mon.service-public concerns only the e-gov services related to citizen,
A relying party can use the AA of mon-service.public.fr only if it is a partner and is based on Liberty Alliance.

Process
Input: certificate from the eID card
Output: access given to mon-service.public.fr or a federation key and the level of authentication are sent to the service provider(ID FF1.2, IDW SF 1.1, SAML 1.1). Legally, the authentication process must comply with the General Security Directory.

Assurance level
With the national eID card and the authentication certificate protected by PIN, the assurance will be high.

7.7 Conclusion

France at present only seems to have a weak authentication scheme for eID's based on username/password, although digital certificates do exist, also for citizens. These certificates play a very limited role. The actual certificates are mostly provided for persons acting on behalf of a company and are used with e-gov services related to companies. They are provided by qualified Certificate Service Providers.

8 Country report: Germany[153]

This section is based on TILT analysis of available sources and on review from the MS. No country report from Germany has been received.

8.1 Structure of the Administration

Germany is a Federal republic made up of 16 states (‘Länder’), which have their own legislative and executive bodies. On a federal level, Germany has two chambers with legislative power: the Bundestag and the Bundesrat.[154] Most government services are offered by municipalities, of which most are governed by state law, instead of federal law.[155] Citizen Identity documents are within the responsibility of the federal government (due to the Federalism Reform Agreement),[156] but its success depends on agreements made with state governments and municipalities.[157] The federal government need to cooperate with state governments to implement far-reaching decisions.

A German eGovernment framework is provided by the ‘Deutschland-Online’ initiative. This initiative mainly comprises the coordination and coordination between the federal government, the federal states (16), the districts (300), and the municipalities (+ 13000). Deutschland-Online and its succeeding Deutschland Online Action Plan comprises five priorities: development of integrated eServices, Interconnection of Internet Portals, development of common infrastructures, common standards, and experience- and knowledge transfer.

Other eGovernment initiatives are described in the ‘eGovernment 2.0 programme’, the ‘Federal IT-steering Strategy’, and ‘BundOnline 2005’.[158] The eGovernment 2.0 programme is part of the strategy of modernization of the Administration (Zukunftsorientierte Verwalting durch Innovationen). One of the eGovernment 2.0 programme initiatives (which is aligned with the European i2010 Action Plan) comprises the introduction of an electronic identity card and electronic identification concepts.[159]

The German eGovernment Strategy responsibility lies at the Federal Ministry of the Interior (BMI-Bundesministerium des Innern). Other important roles and responsibilities lie at the Office of the Federal Government Commissioner for Information Technology and the . Moreover, all governments have a Chief Information Officer. Other bodies that are relevant to mention are the ‘Conference of State Secretaries responsible for eGovernment’, and the ‘Office of the task Force Deutschland Online’.

8.2 Debate (and history)

The development of eGovernment in Germany originates from before 2000. For instance, in 1996 a plan for ICT-enabled change in public administrations was presented called ‘Info 2000: Germany’s way to the Information Society’. Several other plans have succeeded this initiative, like the ‘D21 initiative’ (1999) and the ‘eGovernment manual’ (2001). Germany launched its government information

[153] The information in this chapter was provided by André Braunmandl.

[154] Factsheet epractice.eu

[155] IDABC interoperability for PEGS country report Germany.

[156] IDABC interoperability for PEGS country report Germany, p. 10.

[157] IDABC interoperability for PEGS country report Germany, p. 10.

[158] Factsheet Epractice.eu.

[159] Factsheet, Epractice.eu p. 9

and services portal ‘Bund.de’ in March 2001, and was the first European Member State to implement eSignatures legislation in 1997, which was adapted to the European Directive (1999/93/EC) in 2001.

Germany has experience with the developments of smart cards because of their development of the German Office Identity Card (pilot project), and the German health card project.[160] The German smart cards used for identification and authentication are part of the common German ‘eCard Strategy’.

As mentioned, the electronic Identity Card is part of the eGovernment 2.0 programme. It facilitates identification on the Internet. Electronic Identity Cards, which should be introduced by 2010, will include optional electronic signature functionality and storage of biometric data.[161]

8.3 eID model

Germany just passed[162] its new "Personalausweisgesetz" (National ID law). Starting in November 2010 all German citizen will be able to receive a new eID card. This legislation sets high standards in case of data protection and data security. It will introduce the concept of mutual authentication of eService provider and eID-card holder. That is, each citizen will have the possibility to get a new ID-card with eID functionality. This eID functionality can be used to authenticate to eService providers that own a valid access certificate. The concept of the access certificate is new in the field of eID and needs to be explained.

Each service provider that intends to make use of the new authentication possibilities of its customers has to apply for an access certificate at the corresponding issuing authority in Germany. The service provider will need to specify its identity, the intended purpose that requires an online authentication and he needs to specify which attributes are needed. The issuing authority checks the request with regard to German law, esp. the data protection standards. If everything is found to be in order, the access certificate is granted. The intended purpose is stored in the granted access certificate, giving access to the needed attributes if consented by the citizen .

During the authentication procedure, the service provider has to present his access certificate to the authenticating eID-card holder, who is informed about the given intended purpose. He is presented a list of the requested attributes, as specified in the access certificate. The service provider can not request further attributes that are not specified in his access certificate. The eID-card holder has to give consent to each requested attribute.

This procedure introduces a mutual authentication eService provider and eID-card holder. Each one can be sure of each others identity. A secure end to end encryption is established.

In contrast to other European solutions, Germany does not have any central registers, controlled be the administration. All relevant information will be stored on the eID-card, under control of its holder (secured by PIN). Informed consent is guaranteed by construction. The resulting system is open to eGovernment and commercial applications likewise (publicly available eID infrastructure).

8.4 Principal legislation and policy documents

8.4.1 Legislation (Federal):

- Grundgesetz für die Bundesrepublik Deutschland, 1949 (Constitution)
- The Identity Card Act (Personalausweisgesetz)

[160] Modinis IDM country report Germany.

[161] Epractice.eu factsheet p 23

[162] Bundestag: December, 18th 2008, Bundesrat: February, 13th 2009

- The Passport Act (Passgesetz)
- Federal Data Protection Act (2003)(*Bundesdatenschutzgesetz*). Coverage:"to protect the individual against violations of his personal rights by handling person-related data." The law covers collection, processing and use of personal data collected by public federal and state authorities (as long as there is no state regulation), and by non-public entities (i.e. companies, clubs, etc), if they process and use data for commercial or professional aims.
- Digital Signature Act (2001)(SigG), which came into force on 22 May 2001 and implements EU Directive 1999/93/EC.
- General Administrative Regulation Governing the Electronic Office ID Card (April 15, 2008)

8.4.2 Policy:

- Decision on the introduction of the eID (elektronischen Personalausweises), 23.07.2008
- Implementation plan 2008 of ‘Focus on the Future: Innovations for Administration’, including the E-Government 2.0 programme. (2008)
- The new National IT Strategy (2008)
- Future-oriented public administration through innovations (2006), inclusing the e-government 2.0 programme.
- The eCard Strategy (Kabinettsbeschlusses 9.03.2005)
- Deutschland Online (2003)
- Information Society Germany 2006 (2003)
- The eGovernment Manual (2001)
- BundOnline 2005 (2000)

8.5 Conclusions

Germany will have an electronic identity that can be used within STORK. Until the official start date (November 2010) Germany will provide STORK with appropriate prototypes.

9 Country report: Italy[163]

CIE	Electronic Identity Card (“Carta d’identitá elettronica”)
CNS	National Service Card (“Carta Nazionale dei Servizi”)
PSE	Electronic Residence Permit (“Permesso di soggiorno elettronico”)
CNSD	National Center of Demographic Services
INA	National Index of Registry Offices
SAIA	Access and Interconnection System for Identification Data
AIRE	Registry Office for Italians living abroad
SSCE	Emission Circuit Security System

9.1 Structure of the Administration

Italy has been a parliamentary republic since 2 June 1946. Legislative power is held by a bicameral Parliament made up of a Chamber of Deputies and a Senate. The Head of State is the President of the Republic, elected by Parliament. Executive power is exercised by the Government, consisting of the Prime Minister and the Ministers jointly constituting the Council of Ministers.

Italy is organised in 20 Regions with autonomy on many fields. The regions have legislative power together with the state in matters of concurrent legislation, except for fundamental principles that are reserved to state law. The regions have exclusive legislative power with respect to any matters not expressly reserved to state law. Municipalities and provinces have regulatory power with respect to the organisation and fulfilment of the functions assigned to them.[164] The majority of e-government services are delivered at local (in particular municipalities) level. Relevant services (e.g., taxes and social security) are delivered at central level. Other services are also delivered at regional and provincial level.

Identity documents are issued by the municipalities based on the base of formats and regulations established by the Ministry of Interior. The same responsibility (on regulating and issuing) is valid for the electronic form of the identity document.[165]

In order to meet the juridical, administrative and technical requirements, the following organisational structures and technical components have been introduced:

- CNSD (National Center of Demographic Services): this organisation is a sub-organisation of the Ministry of the Interior and provides several services that allow the identification of registered citizens.

The main CNSD services are:

- INA (National Index of Registry Offices): this service is a national registry referring to the personal data of all registered citizens. Public authorities can query, validate and update such data. For each entry the INA holds a pointer to the local authority of the citizen in case more detailed information is needed. The INA can be used by all interested authorities for querying and validating a citizen’s personal data. The INA is also used in the issuing process of the eID for validating the citizen’s personal data.

[163] Based on analysis by the TILT team complemented by a country report written by Stefano Fuligni, Giovanni Maca and Roberto Pizzicannella/

[164] Factsheet - Italy - Country Profile; epractice.eu, June 2008.

[165] Country Report Italy by Stefano Fuligni, Giovanni Manca and Roberto Pizzicannella for Italy.

The registry must be kept up-to-date. All municipalities are therefore responsible for updating the INA by communicating a change of residence, immigrations, emigrations, births and deaths.

- SAIA (Access and Interconnection System for Identification Data): a network system, which can be used by municipalities to interchange and communicate a citizen's personal data.
- AIRE (Registry Office for Italians living abroad): it is the pendant to the INA and holds the data of Italians living abroad.
- Civil state: a registry holding the civil status of all Italians

- Secure Information Structure: the "Backbone" is a network that enables a secure and certified communication structure between Public Authorities. Municipalities can transparently access the CNSD services in a secure way without having to care about security issues. The organizational and technical autonomy of the municipalities remains untouched by accessing the network using so called Trusted Anchor Point.

- SSCE (Emission Circuit Security System): this IT structure is used for the rollout of the eID and primarily act as Public Key Infrastructure. It handles the data exchange and validation of personal data for card emissions as well as the revocation checking of eID certificates in governmental processes.[166]

9.2 Debate (and history)

The history of the Italian eID, the "Carta d'identitá elettronica" (CIE) goes back to 1998, where l'AIPA (the former CNIPA ("National IT Center for the Public Administration")) conducted a survey for potential technologies of the CIE. The Ministry of the Interior went for a smart card with an optical strip.

After a number of test roll-outs, the rollout CIEs to all Italian citizens older than 15 years started in 2005.[167]

To accelerate the distribution of an instrument for online identification, the "Carta Nazionale dei Servizi" (CNS) initiative has been started by the CNIPA, as the rollout of the CIE for each citizen will last several years. The CNS has the same smart card characteristics as the CIE, but allows issuing to all persons living in Italy. The CNS will be issued to citizens in certain pilot regions and is expected to be operational by the end of the year 2006.

9.3 eID model

In Italy there are two eID schemes: the Italian Electronic Identity Card ("Carta d'identitá elettronica" - CIE) and the National Service Card ("Carta Nazionale dei Servizi"- CNS).

The CIE is a hybrid card that covers two functions. It will replace the traditional identity card, and will also be an instrument for authentication and identification in e-Government processes. The Italian eID is not solely intended for e-Government environments, but can also be used as a health insurance card, fidelity card or fiscal document.

The CIE fulfils three main tasks. It will replace the paper based identity card for a simplification in traditional governmental processes. Moreover, it will be an international travelling document according to ICAO and ISO. Last but not least it enables the use of e-Government applications.

In order to identify a physical person, a fingerprint template will be stored on the chip. An image of the fingerprint is stored in the optical strip. According to the Italian law, the templates are not stored in a central database. As the smart card allows the storage of additional data, the CIE can be used in other

[166] Modinis IDM Study, National IDM Profiles, Italian Profile, 2005 and Country report Italy form Italy.

[167] Country Report Italy by Stefano Fuligni, Giovanni Manca and Roberto Pizzicannella for Italy.

sectors (even private sectors) as well. For instance, the blood type can optionally be stored on the card (CNS only).[168]

The experimental phase for the CIE for Italians living abroad is in progress and can already be used for some services in the application range of e-Voting.

9.4 Principal legislation and policy documents

Legislation:

The Italian eID was introduced by law of May 15, 1997, No. 127, while technical rules for the issuing of the card have been firstly supplied by d.p.c.m. of October 22, 1999, No. 437 and by d.m. 19 of July 2000 (Attachments A and B).[169]

The last version of technical rules is supplied by d.m. November 8, 2007 (Attachments A and B).

For the CNS the most relevant legal sources are the D.p.r. March 2, 2004, No. 117 and the CDA.

- The eGovernment Code (*"Codice dell'Amministrazione Digitale"*), entered into force on 1 January 2006, is aimed at providing a clear legal framework for the development of eGovernment and for the emergence of an efficient and user-friendly public administration. Laying down a number of rules, obligations, recommendations and targets to promote the use of ICT in the public sector, it is intended to contribute to removing obstacles to further eGovernment development. The eGovernment Code regulates electronic signatures and confirms their full legal validity. The Italian so-called *"firma digitale"* (digital signature) is compliant with the "qualified signature" as in the Directive 1999/93/EC.
- The Law on Administrative Procedure and Access to Administrative Documents of 7 August 1990 provides for a limited right of access to administrative documents. The Law states that those requesting information must have "an interest to safeguard in legally relevant situations". It applies to "administrative bodies of the state, including special and autonomous bodies, public entities and the providers of public services, as well as guarantee and supervisory authorities".
- The Data Protection Code entered into force on 1 January 2004 and is meant to update, complete and consolidate Italy's data protection legislation since 1996 by introducing important innovations and conforming national legislation to European regulations, in particular the Data Protection Directive (95/46/EC) and the Directive on privacy and electronic communications (2002/58/EC).
- The Legislative Decree on Electronic Commerce came into force on 14 May 2003. It regulates the use of electronic commerce means in Italy as well as the information that eCommerce websites shall compulsorily provide to purchasers.
- The Electronic Communications Code entered into force on 16 September 2003. It transposes four of the directives of the EU regulatory framework for electronic communications, the ePrivacy directive being transposed in the Data Protection Code.
- The Legislative Decree no. 10 of 23 January 2002 brought the Italian electronic signature regulations into line with the Directive 1999/93/EC on a Community framework for electronic signatures.[170]
- The relevant laws/decrees that introduced the electronic ID card were: The law N. 191 of Jun 16th,

[168] Ibid.

[169] Other relevant norms can be found in law of June 16, 1998; law of February 28, 2000, No. 26 (concerning INA-SAIA system); law of Mach 31, 2005, No. 43; the CDA; d.m. of August 2, 2005, No. 191 (decree of the Ministry of Internals). IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, country report Italy, April 2007, p. 18.

[170] Factsheet - Italy - Legal Framework; epractice.eu, June 2008.

1998 where, at Article 2, is written:

“The id card and any other identification document must contain the personal data of the holder and may contain the blood type and other options related to health care according to law”.

“The document, or its magnetic or other kind of data storage, may contain also other data, in order to rationalise and simplify the administrative action and the provision of services to citizens”.

- The official introduction of the electronic ID card – however – took place only in the year 2000, with a Ministry Decree dated July 2000. The Decree, at its Article 1, states that:

  *“As “service card” it is meant the set of identification data (excluding photo and hand signature) and of the administrative information cited at …[other Decree reference]”*171

Other legislation

- Decreto 8 novembre 2007 del Ministro dell’interno di concerto con il Ministro per le riforme e le innovazioni nella PA - “Regole tecniche della Carta d’identità elettronica”
- G.U. 9 novembre 2007 n. 229, S. O n. 261
- Decreto del Ministro dell’interno, del Ministro per l’innovazione e le tecnologie e del Ministro dell’economia e delle finanze 9 dicembre 2004 - “Le regole tecniche e di sicurezza relative alle tecnologie e ai materiali utilizzati per la produzione della Carta nazionale dei servizi.” G.U. 18 dicembre 2004, n. 296
- Decreto del Presidente della Repubblica 2 marzo 2004, n. 117 - “Regolamento concernente la diffusione della carta nazionale dei servizi, a norma dell’articolo 27, comma 8, lettera b), della Legge 16 gennaio 2003, n. 3.” G.U. 6 maggio 2004, n. 105
- Decreto del Presidente del Consiglio dei Ministri 1 aprile 2008
- Regole tecniche e di sicurezza per il funzionamento del Sistema pubblico di connettività previste dall’articolo 71, comma 1-bis del decreto legislativo 7 marzo 2005, n. 82, recante il «Codice dell’amministrazione digitale». G.U. 21 giugno 2008, n. 144.
- Decreto legislativo 30 giugno 2003, n. 196 - Codice in materia di protezione dei dati personali. GU n. 174 del 29 luglio 2003.
- Decreto legislativo 23 gennaio 2002, n. 10 - Attuazione della direttiva 1999/93/CE relativa ad un quadro comunitario per le firme elettroniche. G.U. n. 39 del 15 febbraio 2002

9.5 Analysis

eIDentity: CIE/CNS

Name

The two most important eID’s in Italy are the “Carta d’identitá elettronica”, the Electronic Identity Card (CIE) and the “Carta Nazionale dei Servizi”, the National Services Card (CNS).

To accelerate the implementation of eIDs, the CNS was launched to complement the CIE. The CNS has the same smart card characteristics as the CIE, but is meant for individuals not eligible to a CIE.[172]

[171] IDABC eID Interoperability for PEGS country report Italy, November 2007, p. 17-18.

[172] Modinis IDM Study, National IDM Profiles, Italian Profile, 2005.

The CIE is a hybrid card that is an instrument for authentication and identification in e-Government processes. The CIE is not solely intended for e-Government environments, but can also be used as a health insurance card, fidelity card or fiscal document.

The CNS lacks a number of the additional security elements of the CIE, such as the laser band, the holograms, etc. Therefore, CNS can not be used as a visual ID document (it also does not bear a photo of the holder). The CNS can be used to authenticate in ICT-based services and can be used to sign electronic documents with a qualified signature. The card contains an entity authentication certificate and a qualified signature certificate.[173]

Form

The eID is a set of attributes stored in a file-system in a Smart Card together with an X509 certificate.

CIE

Physically, the CIE is a ‘hybrid’ card made of polycarbonate. The Italian eID card comprises a microchip, an optical memory and an ICAO machine readable zone for the use of the card as a travel document.

It contains a set of personal data, including the holder's fiscal code and blood group, and fingerprint scans. The personal data, biometric key and digital signature are only stored on the card. In accordance with data protection legislation, this data is not kept on any central database and can only be released and used if the holder gives his/her permission by inserting a PIN code. The cardholder’s fingerprint template is stored in both the microchip and the optical memory and does not allow fingerprint reconstruction.

While the laser band provides security (since the data cannot be modified when attempting to make counterfeits) the microchip makes online identification possible and enables transactions between citizens and providers. The microchip can also store digital signature certificates.

A law adopted in March 2005 (no. 43/2005) provided for the demise of paper ID documents and their replacement by eID cards by the end of 2005. According to the initial plan, all new ID Documents issued as of 1 January 2006 should have been electronic. However, this initial objective had to be postponed. The ultimate goal is to substitute 40 million paper ID documents by 2011 at a pace of eight million cards a year.[174]

CNS

The CNS has an embedded microprocessor similar to that of the eID card as well as identical running software. The only difference is that the CNS lacks the additional security elements of the CIE, such as the laser band, the holograms, etc. Therefore, contrary to the CIE, the CNS **does not constitute a 'proof of identity'** and is not a legal identity document nor travel document. The CNS is only used in ICT -based services as an instrument of entity authentication. It can also be used to sign electronic documents with a qualified signature as it contains not only an entity authentication certificate but also a qualified signature certificate.[175]

Eligibility

The CIE can only be issued to Italians living in Italy and at least 15 years old. The CNS is issued to any citizen on request with no limits on age, under the condition that he/she doesn’t already own of a CIE.

[173] IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, country report Italy, April 2007, p. 19.

[174] Factsheet - Italy - National Infrastructure; epractice.eu, June 2008.

[175] Factsheet - Italy - National Infrastructure; epractice.eu, June 2008.

To enable the use of e-Government services for other people, the “Permission for Electronic Accommodation” (PSE), the Electronic Residence Permit, initiative has been started. The PSE is a hybrid card, has similar characteristics of the CIE and is compatible in regard to the used microprocessor (smart card). The legal basis for the PSE was established by the decree of 03/08/2004 defining the organisational and technical framework. At the moment the PSE project is in a first experimental phase and after finalisation it will be issued to non-Italians (EU citizens as well as non-EU citizens).[176]

Issuer

The CIE is issued by the municipalities through a system that is under the responsibility of the Ministry of Interior (National Center for Demographic Services) and that involves also the Istituto Poligrafico dello Stato (for the “preparation” of the cards).

The CNS can be issued by any Italian public administration.[177]

Public authorities can query, validate and update data from the INA. For each entry the INA holds a pointer to the local authority of the citizen in case more detailed information is needed. The INA can be used by all interested authorities for querying and validating a citizen’s personal data. The INA is also used in the issuing process of the CIE for validating the citizen’s personal data.[178]

The register of citizen data is kept on behalf of the Municipalities, while the central database contains only encrypted information. However, at least in the case of the CIE, it collects also the log of the issuing of each card and the keys needed by the municipalities to “open” the card for writing during its personalisation.[179]

The owner of the ID card is the Ministry of Interior, which has the overall responsibility of the project and manages the Trust Centre (including the PKI). However, the role of the national print-house (IPZS, Istituto Poligrafico e Zecca dello Stato) is very important, because it is in charge of the physical manufacturing of the cards and of their pre-personalisation. The responsibility of the issuing is up to the municipalities, which receive and process the citizen requests and physically consign the card.

The CNS has no single owner, so the organisation depends upon the particular administration adopting it. The most important CNS project is the one of Regione Lombardia. In this case, obviously the owner is the Regional Government and the card is delivered by a consortium and manufactured by its subcontractors. The trust centre is under direct control of the Region.[180]

Responsible authority

The responsible authority for the CIE is the municipality that issues it. The responsible authority for the CNS is the public administration that decides to issue it. [181]

Attributes

The attributes in the CIE are included in the file system of the cards and include the personal data of the holder (name, surname, sex, date of birth, place of birth, municipality of residence at the time of issuing) and the fiscal code (i.e., the unique identifier in Italy).

The data structure of the CNS is the same as for the CIE. [182]

The three types of authentication supported by the tokens are:

[176] Modinis IDM Study, National IDM Profiles, Italian Profile, 2005.

[177] Country Report Italy by Stefano Fuligni, Giovanni Manca and Roberto Pizzicannella for Italy.

[178] Factsheet - Italy - National Infrastructure; epractice.eu, June 2008.

[179] IDABC eID Interoperability for PEGS country report Italy, November 2007, p. 16.

[180] IDABC eID Interoperability for PEGS country report Italy, November 2007, p. 23.

[181] Country Report Italy by Stefano Fuligni, Giovanni Manca and Roberto Pizzicannella for Italy.

[182] Country Report Italy by Stefano Fuligni, Giovanni Manca and Roberto Pizzicannella for Italy.

- Visual identification
- Active authentication

The visual identification is a process that requires the traditional security means of previous documents, for example holograms, microprints, etc.

Finally, the active authentication requires computing process for a private key operation that has to occur within the token itself in response to a challenge sent by a server. In this case, only chip cards can be used. The active authentication is the only which guarantees a strong authentication over the network (i.e. when parties are not one in front of the other).[183]

The main information printed on the document is also present on the card body of the new electronic version and is the following:

- Municipality which issues the document
- Last (family) name
- First name
- Municipality of birth
- Date of birth
- Gender
- Number of birth certificate
- Height (cm)
- Number of the document
- Photo of the holder
- Official residence
- Address
- Date of issuing
- Date of expiration
- Citizenship
- Fiscal code
- Hand signature
- Indication about the validity of the document abroad[184]

However, each of these cards has (at least) one digital certificate on board (for authentication and/or attestation). Both the CIE and the CNS have – as an option left free to citizens – the possibility to install a second certificate (issued by one of the certification authorities in the trust list of CNIPA) for law enforced digital signature.[185]

One important issue deals with the management of biometric data. Templates are always used instead of full images. Particularly, for the CIE, templates are only stored on the card, so that the verification possible is only of the type “one to one”.[186]

One interesting feature of the CIE and CNS is the format of the authentication digital certificate, whose common name does not directly contain the name of the holder. Instead it contains the SHA-1 hash of the file “Dati Personali” (personal data), thus preventing anybody from accessing the personal information of the holders (for example, from the directory of certificates) without their explicit permission. In case of necessity, the file Dati Personali can be read too, its hash computed, and the result compared with that contained in the common name of the certificate.[187]

[183] IDABC eID Interoperability for PEGS country report Italy, November 2007, p. 18-19.

[184] IDABC eID Interoperability for PEGS country report Italy, November 2007, p. 13.

[185] IDABC eID Interoperability for PEGS country report Italy, November 2007, p. 19-20.

[186] IDABC eID Interoperability for PEGS country report Italy, November 2007, p. 23.

[187] IDABC eID Interoperability for PEGS country report Italy, November 2007, p. 16.

The process is strictly compliant with the SSL v3 standard, i.e. a challenge-response procedure is invoked between the server and the client and the holder is required to enter his/her (authentication) PIN number to unblock the private key operation run inside the chip. The private key operation is needed to correctly answer the challenge coming from the server. When the card also has a digital signature certificate on board, this can have a different PIN number to avoid misuse.

The information sent to the server during the authentication phase is that contained in the common name of the certificate that, as said before, hides the personal data of the holder.

Privacy has been considered an absolute must for the CIE; in this case, besides the hash of the personal data of the holder, the common name only contains the serial number of the card. Whenever personal data are strictly required, the server has then to send to the client an applet for reading also the personal data file, compute its hash and compare it to the one contained into the common name.

The CNS lowers this requirement a bit, by also including the Fiscal Code of the citizen in the common name, which allows a much bigger range of services to be delivered without the need for also reading the personal data file. It is not clear at the moment if the CIE will adopt the same measure in the future or not.[188]

Conditions for use

The eID (CIE or CNS) can be used by its holder to access any public service available on line, according to the "Code of Digital Administration" [189]

Creation and termination

The eID (CIE or CNS) is issued upon request of the citizen based on the physical recognition and identification of the owner.

The CIE expires after 10 years, while the validity of the CNS is determined by each public administration that issues it (issuing authority) and in any case cannot be longer than 6 years.

The CIE is terminated for theft, loss, or damage on request of the owner (through a toll-free number made available by the Ministry of Interior).

The termination procedures for the CNS are defined by the public administration that issues it (issuing authority) [190]

With the introduction of the electronic ID card, a central database was set up, but in it each record is encrypted with the public key of the issuing municipality, in order to preserve the privacy of citizens. In practice, this means that no real change in the way citizen data are used took place.[191]

The key generation procedure varies depending on the issuing scheme. In the case of the CIE, which is personalised (in a decentralised way) by the municipalities, the key generation occurs on-board of the card and the PKCS#10 certificate request is then sent to the trust centre for processing.

In all cases, however, when a digital signature key (also) has to be generated, this has to occur within the secure confines of the chip-card.[192]

[188] IDABC eID Interoperability for PEGS country report Italy, November 2007,, p. 16-17.

[189] Country Report Italy by Stefano Fuligni, Giovanni Manca and Roberto Pizzicannella for Italy.

[190] Country Report Italy by Stefano Fuligni, Giovanni Manca and Roberto Pizzicannella for Italy.

[191] IDABC eID Interoperability for PEGS country report Italy, November 2007, p. 13.

[192] IDABC eID Interoperability for PEGS country report Italy, November 2007, p. 19-20.

9.6 Authentication Authority

Name

The claimant can be authenticated by the middleware on the basis of the authentication certificate on the CIE/CNS. Validation of the certificates can be done by the Ministry of Interior (National Center for Demographic Services) for the CIE (Electronic Identification Card) and by the Italian Public Administration that issued the CNS (National Service Card), via the services provided by the accredited Certification Authorities.

What

Each AA can authenticate only the eIDs (x.509 certificates) that are issued by itself.

Responsible authority

The Ministry of Interior or the Public Administration issuer.

Input

The certificate's serial number or the certificate in case of an OCSP request; a “get CRL” request otherwise.

Output

An OCSP response or the entire CRL for the managed certificates.

These services are free to access.

For whom

An AA is used by relying parties (i.e. portal services, web sites, etc.) using OCSP query or scanning CRLs.

Process

A claimant uses his CIE/CNS through a smart card reader, the relying party ask the corresponding AA (via OCSP request or CRLs scan) about certificate validity and then authorise to access the service required if the eID is authenticated.

Assurance level

The assurance level is provided by the x.509 certificate itself.

Other

The CIE/CNS are strictly personnel and therefore is not possible any kind of delegation.

9.7 Conclusions

Italy recognizes two major eID's, the Carta d’identitá elettronica” (CIE) and the Carta Nazionale dei Servizi (CNS). These smart cards include two certificates, one for authentication and one for electronic signatures. The CIE is meant for Italian residents, the CNS can be obtained by anyone else residing in Italy. Authentication of the card holder can be done by the card middleware. Additional assurance can by obtained by an OCSP request or CRL scan directed at the CA that issued the card.

The CIE contains a SHA-1 hash of the Dati Personali file in the common name field on the card. The CNS contains includes both the SHA-1 hash and the holder's fiscal number as part of the common name field on the card. The fiscal code may only be used for identification and authentication and may only be stored by relying parties when mandated by law, or by consent of the claimant.

The CIE/CNS does contain personal data but this data can only be read when the holder gives his/her consent.

Additional data may be obtained from national authentic registers, such as the INA National Index of Registry Offices, held by the National Center of Demographic Services (CNSD) if a memorandum of understanding is signed with the Ministry of the Interior.

10 Country report: Iceland[193]

10.1 Structure of the Administration

Iceland is a republic, which has a parliamentary form of government. Most executive power rests with the Government. Iceland has 8 administrative regions and 79 municipalities.[194] Iceland is a member of the European Free Trade Association (EFTA) and the European Economic Area (EEA).

10.2 Debate (and history)

Iceland's initiative in the field of eGovernment dates from 1996, in which the Government published the 'Icelandic Government's Vision of the Information Society'. Several initiatives succeeded this policy document, like the 'Resources to Serve Everyone-policy' (2004), the launch of the information and service portal (island.is), and the drafting of the Icelandic Government Policy on the Information Society for 2008-2012[195].

The policy and strategy on eGovernment is determined by the Prime Minister's Office. The policy, which is defined centrally but implemented locally, is coordinated by a steering group called the "Information Society Taskforce". Another relevant actor in Iceland is "The eGovernment Taskforce".

10.3 eID model

Official ID documents are Passport and ID-card issued by The National Registry, and Driving Licence issued by the Police. Enrolment for all ID documents is in the provincial administrations (Syslumenn). These documents rely on information from the national registry of persons, where the key identifier is a unique ID-number.

The Icelandic eID model relies on the National Registry which contains information concerning domiciles, names, births, christenings, changes of address, marriages, cohabitation, divorces, deaths, etc. Moreover, persons in Iceland are identified with an ID-number. This number is issued at birth to all children born in Iceland and when persons register themselves if they take up residence. The ID number consists of 10 digits. Use of this unique identifier is bound by the general rule of having a 'just cause' to use the number.[196]

All residents in Iceland have a unique ID-number, which is used as the main identifier of persons by government and also in the private sector.[197]

These are the main eID schemes:

1. Today the Icelandic Governmental agencies use a variety of eIDM systems, most of which are username/password-based.
2. The Internal Revenue Directorate has established a general username/password scheme for all residents, which is also being used by a few other government organisations via SAML-token.
3. Some central governmental agencies have been using soft PKI X.509 certificates in eGovernment since 2003 for authentication and for electronic signature.
4. The internet banks have used username/password plus OTP-token for a couple of years.

[193] Based on analysis by the TILT team complemented by a country report written by Haraldur Bjarnason and Kári Ólafsson.

[194] ePractice.eu factsheet Iceland; IDABC interoperability for pegs country report.

[195] Source : ePractice.eu factsheet

[196] IDABC interoperability for PEGS report, profile Iceland, p.11

[197] Iceland country report by Bjarnason and Ólafsson.

5. Smart-card based PKI X.509 certificates will soon be rolled out, in co-operation between the government and banks, see below.

Today the government is implementing a central eIDM system in Iceland that is based on X.509 Client certificates and ETSI standards. The main objective of this project is to get mass distribution of electronic certificates to citizens and companies for authentication and electronic signature. One of the main building blocks for this is the creation of an open and standardized PKI environment in Iceland. Based on this structure eIDs will be distributed to all citizens in the country. Citizens will be able to use the eIDs in relations to both central and local government as well as any other business in Iceland. The Icelandic Government co-operates with the Federation of Icelandic Banks in building, implementing and maintaining this infrastructure. The Ministry of Finance has created a root certificate, named Iceland Root (Íslandsrót) that issues intermediate certificates to Identity providers (subordinate certificates authorities) in Iceland. An intermediate certificate has been issued to banks and it is planned that another certificate will be issued to the National registry for issuance of citizen cards. The banks have started to distribute certificates on debit cards to citizens. National registry is planning to start issuing certificates 2009. In the near future it is planned that certificates will be distributed to governmental employees for them to use in communication with citizens and companies. It is also likely that commercial companies will want some of their employees to use certificate in their work. The employees can then either use their certificates on the debit cards or on a citizen card. There is also a possibility that some large companies will use their own certificates issued by their company or some other commercial companies that are in the business of issuing employee certificates. The idea of creating an open and standardised PKI environment in Iceland is to support different certificate issuers to ensure efficiency for everybody that is involved or uses this infrastructure in Iceland and other countries.

Compliance of the smart card eIDs:

- The eID consists of two standard x509 client certificates, one for Authentication (standard SSL/TLS), and one for Non-Repudiation-Signatures. The certificates (and the corresponding private keys) are stored on smart-cards (ISO-7816 – PKCS#15).
- Certification policies fulfil the technical specification ETSI TS 101 456.
- End certificates for Non-Repudiation-Signatures are claimed to be qualified signatures on secure signature creation device that should fulfil the law on electronic signatures based on the EC Directive on electronic signature.
- Certificates for authentication fulfil the same requirements as the certificate for Non-Repudiation-Signatures but it is not claimed in the certificate that it fulfils the law since that is not required for Certificates for authentication.

10.4 Principal legislation and policy documents

Legislation:

- Amendment (no. 51/2003) to the Public Administration Act, no. 37/1993 comprising a chapter on the electronic handling of matters by public administration.
  Through this modification, general obstacles to the development of electronic administration were removed. While formulating the amendment, the committee in question was guided by the concept of equivalent value, and also emphasised the need to maintain technical impartiality. The alteration involved mere permission for the electronic handling of governmental administration cases, but not an obligation.

- Act No. 30/2002 on Electronic Commerce and other Electronic Services
- Administrative Procedures Act no. 37/1993
- The Act on the Protection of Privacy as regards the Processing of Personal Data, no. 77/2000 (came into effect in January 2001 and implements the EC Data Protection Directive)
- The act deals with how the protective principle relates to data quality and presented criteria for the legitimacy of data processing. The act applies to any automated processing of personal data and to manual processing of such data if it is, or is intended to become, a part of a file. It has been amended by Act No. 90/2001, Act No. 30/2002, Act No. 81/2002 and Act no. 46/2003.
- The Act on the National Registry, no. 54/1962

- The Act on the National ID card, no. 25/1965
- Act No. 28/2001 on electronic signatures. Based on the similar EC Directive, article 4 of the Act stipulates that fully qualified electronic signatures shall have the same force as hand written signatures. Furthermore, it is stipulated that other electronic signatures can be legally binding. Supporting legislation comes through the Electronic Commerce Act, 2002 and the Public Administration Act as amended in 2003.
- Service directive. The EC service Directive 2006/123/EC is in the implementation phase in Iceland.

Policy:

There are two main policies regarding e-government in Iceland. A policy that was implemented until 2007 (Resources to Serve Everyone – Policy of the Government of Iceland on the Information Society 2004-2007 (Prime Minister’s Office, 2004)) and a new one adopted in 2008 (The Icelandic Government Policy in the Information Society (‘Iceland, the e-Nation’, 30.6.2008)) for implementation in the coming years.

In the earlier policy, there are some goals that relate to identification. It says “The policy will be to aim for the general and widespread use of electronic certification so that any communicating partner may be positively identified...”

The goals related to electronic certification are on the responsibility of the ministry of finance.

The three goals are:

> *1. The policy will be to aim for the general and widespread use of electronic certification so that any communicating partner may be positively identified; electronic signatures and coding shall be introduced insofar as is deemed appropriate.*
>
> *2. An open but standardised market is Iceland's goal, through the use of electronic certificates and certifying services. The state's requirements shall be published with regard to the content, form and handling of electronic certificates for transactions with national institutions. Those requirements might become the model for a general Public Key Infrastructure (PKI) for industry and municipalities. A simple system, economic in operation, should be the object, so that cost may be distributed in proportion to user benefits.*
>
> *3. European and international standards shall be adhered to, aiming for integration with the Public Key Infrastructure of neighbouring countries when the time seems right.*

In the policy that was adopted in 2008 there are some goals that relate to eIDs. It says *“The e-nation shall adopt online payment, eIDs and e-procurement, in addition to working on other key tasks.”* There are also some activities stated in the policy like “Introducing eIDs in communications with public bodies” and “Services concerning eIDs and e-payments”.

Special policies regarding the use of eIDs have not been published but they are planned in 2009.

10.5 Analysis

eIDentity: PKI Certificates[198]

In Iceland, the first certificates were issued on May 27, 2003 as a part of a pilot project led by the Ministry of Finance. As a solution of this project there were two types of certificates: a public certificate for signing and encrypting e-mail etc. and a private certificate for accessing government systems. Currently, the Icelandic Ministry of Finance is implementing a central eIDM system, which is based on x.509 PKI certificates. The objective of the Government is to issue certificates that can be used for local and central government services, and for businesses as well.

[198] The information in this paragraph is mainly based on the IDABC interoperability for PEGS country report on Iceland.

Form

The Icelandic eID will be composed out of two x509 client certificates, one for Authentication (standard SSL/TLS), and one for Non-Repudiation-Signatures. The certificates (and the corresponding private keys) are stored on smart-cards (ISO-7816 – PKCS#15) that will be distributed on smart cards with the form of a bank card. It is not planned to make the use of an eID card mandatory.

Eligibility

The key for participating in a formal eIDM system in Iceland is to have the Icelandic ID number (SSN#). Hence also non-nationals can use the Icelandic eIDM system if they have an SSN# number. Everyone entitled to stay in Iceland can apply for an ID-number.

Issuer

The banks issue the eID on debit cards. The National registry is also planning to issue eIDs on citizen cards in the near future.

Responsible authority

The ministry of finance is responsible for the PKI structure in Iceland and is the issuer of the Icelanding Root certificate.

The Issuer is responsible for the eID and the issuance of the eIDs.

Attributes

Attributes that are directly linked to the holder of the eID are in the field Subject in the certificate.

> **Name:** Name of the subject (the field CN). Not unique and not necessarily exact or latest info.
>
> **Unique ID-Number of person:** The ID-number (kennitala) is a 10-digit number. The first six digits are the date of birth of the person. (DD day, MM month, YY last two digits in the year of birth). Persons are indentified with the ID-numbers in the National Register of Persons. (the field SERIALNUMBER)
>
> **Country:** Name of the country (IS) (the field C)

The only info on the eID is the date of birth and country of residence. Other information is not stored on the certificate. Other information is available from different parties in different ways. The National registry has for example information about legal address of resident, and organisations that have an access agreement with the National Registry can access this information via service providers.

Conditions for use

The holder of the eID can use the eID in communication with whom he wants. There are no restrictions on the uses. Both commercial and governmental parties can use the eID in communication. It is not recommended to use your personal eID for job-related transactions. Companies and government are expected to issue employee eIDs for this purpose.

Creation and termination

The eID is issued and terminated in accordance with the rules set in the certification policy of the issuer of the certificate. The certification policy is mainly based on ETSI TS 101 456.

10.6 Authentication Authority

Most of the eID schemes used in Iceland rely on verification by the issuing entity (many services use their own username/password scheme). The Internal Revenue Directorate scheme can be used by certain other organisations via SAML-token authenticated by The Internal Revenue Directorate.

10.7 Conclusions

- The Icelandic eID schemes rely mostly on national ID-number of person.
- Smartcard eIDs for signature fulfill the requirements of the EC Directive for qualified electronic signatures.

- Smartcard eIDs for authentication fulfill the same requirements although not intended for qualified signatures.
- A special agreement with the National Registry is needed to access additional data on the person. Data protection law limits the use of such data in other registers.
- Use of the ID-number as such is not so limited.
- The different types of eIDs can be issued to any resident, in some cases even to non-residents (short-term visitors that have obtained ID-numbers) and they do not distinguish between different citizenships.
- National systems rely on ID-number of persons and any person accessing services in Iceland will at some point need such a number. If they use a foreign eID to access a service, data from this eID will have to be stored together with the ID-number of person in the back-end system for that service.

11 Country report: Luxembourg[199]

11.1 Structure of the Administration

Luxembourg is a constitutional monarchy. Legislative power is in the hands of the unicameral Parliament. The Parliament approves bills put forward by itself or by the Government after consultations with the Council of State.

The Ministry of the Civil Service and Administrative Reform is responsible for eGovernment policy/strategy in Luxembourg and is assisted by a Coordination Committee for the Modernisation of the State (CCME). Other actors are the ‘eLuxembourg Service’ and the ‘Informatics Centre of the State’ (CIE).

A ‘Single centralised portal’ is active since 17 November 2008.

11.2 Debate (and history)

Luxembourg presented its eLuxembourg Action Plan in 2001, after a National Commission for the Information Society was created (2000), and after an Info 2000 Committee was created in 1995. Luxembourg has presented an eGovernment Master Plan in 2005. Recently (March 2008), the certified ‘Luxtrust’ signatures were introduced which should increase the role of electronic signatures in the country.

11.3 eID model

The current Luxembourg eGovernment strategy is built upon the eGovernment Master Plan that was drafted in 2005. A public/private partnership (LuxTrust) was created in 2003 to manage the development of a common Public Key Infrastructure (PKI) for eCommerce and eGovernment, which need to lead to a central eID infrastructure in the future.

The general identity infrastructure in Luxembourg comprises a general directory that is combined with a system of unique identifiers for the entities registered in the general directory (**repertoire general**), kept by the CIE. In accordance with the Act of 1979 on the numerical identification of natural and legal persons, all natural and legal persons mandated to reside in Luxembourg (natural persons), established there (legal persons), or registered in any administration get a unique identity number. The identity number is issued by the CIE and is protected by law. It may only be communicated to the person involved, and to public services, civil servants, and issuers of real estate documents or social security organisations.[200] Information in the directory is kept up to date by the communes. In effect, this makes the general directory a form of authentic source.

For natural persons, the general directory includes name, first name, gender, date and place of birth, civil status, date of death, official address, nationality, information regarding spouse, and identification numbers of the parents insofar as such numbers have been granted. In addition to this directory, civil servants at the commune level keep a number of separate civil status registers (such as registers of births, deaths and marriages), the information of which must be passed on to the general directory. The **identity number** is semantic. In the case of natural persons, it contains the date of birth, a sequence number indicating the order of birth of that day and the gender (odd number for men, even number for women), and a check digit. For legal persons the number indicates the year of establishment or first registration for non-national legal persons, legal form, sequence number and check digit.

For legal persons, the general directory includes name, legal form, place of establishment, year of establishment or of first activity within the Grand Duchy, principal activities, and date of dissolution.

[199] Based on analysis by the TILT team complemented by a country report written by Pierre Clausse.

[200] IDABC Luxembourg country report (PEGS), p. 14

Natural persons of the Luxembourg nationality over the age of 15 receive a mandatory identity card, issued by the communes since the entry into force of the Grand-Ducal Decree of 30 August 1939; or in the case of non-nationals mandated to reside in Luxembourg for more than three months, a foreigner's card. These cards include a basic set of identification information, including the identification number, a card number, the issuing commune number, a check digit, the name, first name, nationality, gender, date and place of birth of the bearer, and the issuing commune. This information must be filled out by the mayor or his representative, who signs the document and provides it with the commune seal. Married women may elect to include their husband's name. The card is in principle valid for 10 years, unless it must be revoked for other reasons (including e.g. change of domicile).

Information regarding legal entities and entrepreneurs is registered in the Register of Commerce and Enterprises of Luxembourg (Registre de Commerce et des Sociétés Luxembourg), held under the authority of the Ministry of Justice, at which point they receive a unique register number (RCS number). The information includes the official designation, RCS number, date of establishment, official address, legal form, persons authorised to represent the legal entity, capital and key events. The register can be publicly accessed on-line through https://www.rcsl.lu. There is only one register for all of Luxembourg, with offices in Luxembourg-Ville and Diekirch.

Enterprises must also acquire a fiscal number by registering separately at the Tax Administration (Administration des Contributions) and (if necessary) a VAT number. All of these must be done by paper; there is currently no electronic registration method.

Luxembourg has a centralised identity infrastructure in the form of a general directory (repertoire general) containing identity information for all natural and legal persons registered in Luxembourg, along with a system of unique identifiers for these entities. In addition to this, Luxembourg has had a system of mandatory ID cards for citizens over the age of 15 since 1939. However, there is no central e-ID infrastructure in Luxembourg yet, nor are there specific plans for the establishment of a national electronic ID card in the near future.

LuxTrust

From a policy perspective, the creation of LuxTrust S.A. as a public-private partnership involving i.e. the Luxembourg government and the Luxembourg Chambers of Commerce has been a major step. LuxTrust has been created in 2003 to manage the development of a common Public Key Infrastructure (PKI) in order to secure eCommerce and eGovernment in Luxembourg. LuxTrust has presented in July 2006 the consortium which was awarded the contract concerning the setting up of a PKI. It is expected to begin issuing smart cards to private persons in the course of 2007, and these cards are expected to become a frequently used authentication solution in eGovernment applications. Apart from LuxTrust, there are no other CSPs providing certification services which are used ineGovernment applications.

LuxTrust S.A. is a CA established on 18 November 2005 as a partnership between the Luxembourg Government and some of the biggest names in the Luxembourg private sector, mainly the financial sector.

LuxTrust aims to provide increased security for those in the e-commerce sector such as the Luxembourg Government, the financial sector and other sectors of the Luxembourg economy, as well as individuals. Although LuxTrust is focusing for the time being on how to improve Luxembourg e-commerce security, it is maintaining an international stance by adopting international standards in its solutions.

In July 2006 LuxTrust S.A. has selected a consortium called U-Trust which will provide the technical Infrastructure. LuxTrust offers a range of products and services, which will cover all needs in terms of e-commerce security and can be designed to suit particular requirements.

Certification Authorities

The Luxembourgish institute of Normalisation, Accreditation, Security and Quality (ILNAS) is competent to accredit and supervise Certification Services Providers which provide digital certificates or services related to electronic signatures in Luxembourg according to the eCommerce Act o 14 August 2000.

ILNAS is the unique accreditation body existing in Luxembourg. It is service provided by the Ministry of Economy and External Commerce and therefore provides guarantee of independency, impartiality, integrity and confidentiality.

11.4 Principal legislation and policy documents

Legislation:

- The Data Protection Act of 2 August 2002 (amended on 27th July 2007), governing the processing and use of personal data, and implementing Directive 95/46/EC.
  The 'Processing of Personal Data in the Electronic Communications Sector' Act (into force on 1 July 2005), transposes the EU Directive on privacy and electronic communications (2002/58/EC). The Data Protection Act of 2 August 2002, which was governing the processing and use of personal data in Luxembourg (implementation of the EU Data Protection Directive 95/46/EC) had to be adapted and complemented so as to transpose the EU Directive on privacy and electronic communications (2002/58/EC). So does the 'Processing of Personal Data in the Electronic Communications Sector' Act, adopted on 30 May 2005 and entered into force on 1 July 2005. This Act is also a part of Luxembourg's legislative '*Paquet Telecom*'. The data protection authority is the National Commission for Data Protection.[201]
- The eCommerce Act of 14 August 2000. This Act transposes Directive 99/93/EC and is complemented by a regulation of 1 June 2001 on electronic signatures and electronic payments.[202]
- The Act on the numerical identification of natural and legal persons (30 March 1979)[203]
  This law defines which identifiers and which information is kept on specific identities, but not how such information could/should be used for electronic authentication in general. The e-Signatures law of 9 July 2001 faithfully transposes the provisions of the e-Signatures Directive, but does not apply to authentication as such.
- The regulation of 1 June 2001 on electronic signatures, electronic payments and the creation of an electronic commerce committee.[204]
- The Act of 19 December 2002 concerning the Commercial Register, accounting and annual Accounts.[205]
- The Grand-Ducal Decree of 30 August 1939 introducing the mandatory ID card.[206]

[201] See http://www.legilux.public.lu/leg/a/archives/2002/0911308/0911308.pdf?SID=a3046e80bf0e2162a5b4e31f581ccd6e#page=2

[202] See http://www.legilux.public.lu/leg/a/archives/2000/0960809/0960809.pdf#page=2

[203] See http://www.legilux.lu/leg/a/archives/1979/0460706/1979A09641.html

[204] See http://www.legilux.public.lu/leg/a/archives/2001/0712206/0712206.pdf?SID=4646f8ac47e2886034bd21e7810183e6#page=17

[205] See https://www.rcsl.lu/mjrcs/webapp/data/mjrcs/static/pdf/loi_19_decembre.pdf

[206] See http://www.legilux.public.lu/leg/textescoordonnes/compilation/code_administratif/VOL_4/ORGANISATION/PIECES_IDENT.pdf

- The eCommunications Act(006). The new e-Communications Act of 30 May 2005 transposes the EU regulatory framework for electronic communications (Directives 2002/19/EC, 2002/20/EC, 2002/21/EC, 2002/22/EC). This act forms part of Luxembourg's legislative 'Paquet Telecom' which transposes the European Telecom Directives, and which also includes a specific law on the processing of personal data in the electronic communications sector.

Policy:

- The eGovernment Master Plan (2005)
- The eLuxembourg Action Plan (2001)

11.5 Analysis

eIDentity: The LuxTrust Smartcard

Name

The LuxTrust SmartCard is the key product for authentication from an eGovernment perspective.[207] They are expected to become the standard for on-line eGovernment applications.

Form

The certificates are stored either in a signing server, or a signing stick or a SmartCard which requires a PIN number.

Issuer

LuxTrust Registration Authorities (RA), currently 9 banking corporations and the Chamber of Commerce act as RA's for LuxTrust. Clients have to present themselves personally to a desk of a LuxTrust Registration Authority (RA) to be identified in a face-to-face procedure. The applicant must then submit an identity card (ID card or passport) on the basis of which he will be identified. Applicants must also submit an order form duly completed, signed and dated along with the required documents listed on the last page of the order form for the product of his choice.

Attributes

The card will hold two certificates of which one is destined for authentication, another is destined for electronic signatures.

11.6 Conclusions

Luxembourg has implemented a smart card solution for e-government and private sector services provided by LuxTrust which is the luxembourgish center of excellence in PKI. The smart card is a standard smart card (EAL4+ certified) with two certificates, one for authentication and one for qualified nonrepudiation signatures.

All natural and legal persons mandated to reside in Luxembourg (natural persons), established there (legal persons), or registered in any administration have a unique identity number. The identity number is issued by the CIE and is protected by law. It may only be communicated to the person involved, and to public services, civil servants, and issuers of real estate documents or social security organisations.[208]

[207] IDABC Luxembourg country report (PEGS), p. 13

[208] IDABC Luxembourg country report (PEGS), p. 14

12 Country report: the Netherlands[209]

12.1 Structure of the Administration

The structure of the Dutch administrative system has three main layers: central, provincial (12) and local (municipality, 467) level. Apart from these layers, the Dutch public sector comprises many functional organs and institutions responsible for administering governmental tasks, such providing student bursaries, social welfare, but also managing water levels (Water Boards).

Municipalities are the primary providers of government services[210] (including eGovernment services), they are responsible for hundreds of services. Other main (e)government services are provided by the tax authority (Belastingdienst), IB Groep (e.g. student grants), social insurance institute, and the unemployment service.

Formal identities are provided by the state and issued by the municipalities. Official ID documents are: identity card, passport and driver's license.[211] These documents are based on the information present in the Municipal Registry, which e.g. contains name, last name, address, gender, marital status, nationality, administration numbers and citizen service number, and information concerning parents, partner and children.

Electronic identities are provided/governed by DigiD, the common authentication system for government institutions, run by 'GBO.overheid'. GBO overheid is a division of the Ministry of Interior and Kingdom Relations. Next to the GBO.Overheid initiative, the Dutch eGovernment landscape comprises over 40 organisations and projects.[212]

12.2 Debate (and history)

In the Netherlands, eGovernment has been on the policy agenda since the mid 90s. Today the relevant core discussion is about the national authentication service (DigiD) established in 2004, which is aimed at harmonising and streamlining authentication schemes in the Netherlands. One of the topics of the current DigiD debate is, for instance, that people forget their DigiD login and passwords because these are used infrequently.[213] Another issue is that DigiD identities have been misused (i.e. exchanged amongst citizens) e.g. to file tax declarations.[214]

Another (long running) development in this area concerns the electronic Dutch identity card (eNIK), which needs to provide a high assurance level authentication within the DigiD scheme. The development of the eNIK started in 2004, but has been delayed significantly, because the development of the eNIK needs to be put up to tender according to a court judgement.[215]

The Netherlands was one of the early adopters of eGovernment in Europe. A first action programme was introduced in 1994, and has been succeeded by eight policy documents on electronic government.

[209] Based on analysis by the TILT team.

[210] Leenes, R.E., and Svensson, J.S. (2002), Size Matters - Electronic service delivery by municipalities? In R. Traunmüller, and K. Lenk (Eds.), Electronic Government - First International Conference, EGOV 2002, Aix-en-Provcence, France. Berlin/Heidelberg: Springer, pp. 150-156.

[211] Based on the 'Wet identificatieplicht 2005 (Identification Act)

[212] http://www.e-overheid.nl/e-overheid/projecten/projecten.html

[213] Cf. http://www.geldenrecht.nl/belastingen/aangifte2007/article2484245.ece, last accessed September 23, 2008

[214] Cf. http://www.nrc.nl/binnenland/article1785120.ece/Overheid_erkent_fout_met_DigiD, last accessed September 23, 2008

[215] Cf. http://www.e-overheid.nl/thema/basisvoorzieningen/domeinbeauthenticatie/enik/, last accessed 23-09-2008

One of the most recent policy documents is the document ‘Op weg naar de elektronische overheid’ (Road to an electronic government), which emphasized the needs for univocal identification, use of open standards, and a broad internet-mediated accessibility of public service delivery.[216] The document emphasises that new technologies can be utilised to increase efficiency, reduce administrative burden, and improve the Dutch competitive position. Moreover, the document notes that technologies can create new possibilities for openness, transparency, responsiveness, and accountability.[217]

12.3 eID model

The last policy document described above (Op weg naar elektronische overheid), has emphasised several components of the current ‘eID model’ for the Netherlands: the document inter alia notes that basis ICT-services like authentic registry, identification numbers, authentication mechanisms, and standards for data transport, are essential next to the development of the actual eGovernment services. Moreover, the policy document notes that, in line with parliamentary proceedings[218], it is necessary to make universal agreements with regard to authentic registry, the citizen service number, and electronic identification. In addition, the document mentions that parliament has requested the introduction of the principle of ‘one time provisioning of data’, to avoid citizens from providing the same personal data on multiple occasions.

In short, the Dutch eID model is based on:

- Three authentication levels inside a central authentication scheme (called DigiD);
- The existence of several authentic registries that contain personal data of the citizens (i.e. the Municipal Registry), and;
- A single unique ID number to be used between Dutch citizens and the government (the Citizen Service Number).[219]

12.4 Principal legislation and policy documents

The principal legislation and policy documents regulating the transfer of electronic personal data and subsequently affect the concepts of *digital personas*[220] and the use of electronic identities in The Netherlands, are:

Legislation:

- ‘Personal Data Protection Act 2000’ (‘Wet bescherming persoonsgegevens 2000’) implementing Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals regarding the free electronic transfer of personal data.[221]
- The ‘2003 Electronic Signature Act’ (Wet Elektronische Handtekeningen) was issued to implement Directive 93/99/EC and also to allow the use of biometrics in passports. Consequently, the

[216] http://www.e-overheid.nl/e-overheid/geschiedenis/geschiedenis.xml

[217] http://www.e-overheid.nl/e-overheid-2.0/live/binaries/e-overheid/beleid/opwegnaareoverheid.pdf

[218] Cf. Kamerstukken 29 362 (especially number 4, 8, 15)

[219] Cf. Buitelaar in Fidis 16.1

[220] CLARKE, R. (1994) – “Human identification in information systems: management challenges and public policy issues” - The Information Society, Vol. 7, No. 4, Canberra; pp 6-37

[221] OJ L 281/31, 23.11.1995. See also: Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, OJ L 201/37, 31.07.2002

usage of biometric identification schemes and digital identities in Dutch passports become embedded in Dutch law.[222]

- ‘Act on the Citizen Service Number’ (Wet algemene bepalingen burgerservicenummer)(Kamerstukken 30.312), as of April 2007 approved by the House of Representatives, discussed by the Senate and since November 2007 the law is put into practice through the Dutch municipalities.[223]
- Act on the use of the Citizen Service Number in Health Care (Wet gebruik burgerservicenummer in de zorg), and the Decision on the use of the Citizen Service Number in health Care (Besluit BSN in de Zorg). The Act will be implemented in phases, based on a Decision of May 23, 2008[224]. Some articles come into force on June 1, 2008 whereas others come into force on June 1, 2009.
- The ‘Act of 9 June 1994 on the Municipality Basic Administration’ (Wet gemeentelijke basisadministratie persoonsgegevens). This is one of the eight key registers that are used in the Netherlands. Three other key registers are planned. The development and use of key registers is a part of the project ‘streamlining of key data’.
- The ‘Act on Electronic Government Communications’ (implemented July 2004) (‘Wet elektronisch bestuurlijk verkeer) amending the General Administrative Law Act (Algemene Wet Bestuursrecht).
- The Archives Act 1995 (Archiefwet 1995). This act regulates the filing, storage, and destruction of public-sector records.
- Temporary decree on the use of numbers for government access facility, 2004 (Tijdelijk besluit nummergebruik overheidstoegangsvoorziening).[225]
- Royal decree on management of DigiD, 2006 (Besluit beheer DigiD).[226]
- Royal decree of 8 May 2003 defining the requirements for Certification Service Providers, entered into force on May 21, 2003 (Besluit elektronische handtekeningen)[227]
- The ‘Regulation on procurement rules for public contracts’[228] was introduced on 1 December 2005 (‘Besluit aanbestedingsregels voor overheidsopdrachten’), the one which implements Directive 2004/18/EC of the European Parliament and of the Council of 31 March 2004 on the co-

[222] Stb. 2003, 1999 (see http://overheid.nl/op). Aanpassing van Boek 3 en Boek 6 van het Burgerlijk Wetboek, de Telecommunicatiewet en de Wet op de economische delicten inzake elektronische handtekeningen ter uitvoering van richtlijn nr. 1999/93/EG van het Europees Parlement en de Raad van de Europese Unie van 13 december 1999 betreffende een gemeenschappelijk kader voor elektronische handtekeningen (PbEG L 13) (Wet elektronische handtekeningen).

[223] Wet algemene bepalingen burgerservicenummer; 2 november 2007, nr. 2007-0000442237,STAF/CZW/WVOB -<http://wetten.overheid.nl/cgi-bin/deeplink/law1/title=Wet%20algemene%20bepalingen%20burgerservicenummer>

[224] Besluit van 23 mei 2008 tot vaststelling van het tijdstip van inwerkingtreding van de Wet gebruik burgerservicenummer in de zorg en het Besluit gebruik burgerservicenummer in de zorg alsmede van het tijdstip van vervallen van het Tijdelijk besluit gebruik sofinummer experimenten informatietechnologie zorg (Stb. 186, 2008))

[225] Staatsbld 584,2004

[226] Staatscourant 18 August 2006.

[227] Stb. 2003, 200

[228] Stb. 2005. 408 16 July 2005

ordination of administrative procedures concerning public work contracts. This regulation also includes important implications on eProcurement services.

Policy:

- The '1998 Electronic Government Action Programme' (Actieprogramma Elektronische Overheid), which envisaged an active role of the government for an effective and efficient government.
- The 1998 document 'Legislation for the electronic highway' (nota wetgeving elektronische snelweg),deals with the use of biometrics, electronic identification, digital signatures and TTPs. The document points out that government legislation in the field of e.g. electronic identitfication and digital signatures is necessary, but also anticipates to self-regulation for Certification Service Providers (e.g.: TTPs that issue digital certificates for digital signing and encrypting).[229]
- The 2003 plan 'Modernising Government' (Andere Overheid): consisting of four objectives: improving public service delivery to the citizen, renewed relations between the government, povinces, and municipalities, a better organisation of the government, and a different and reserved approach to regulation.[230]
- The 2004 document 'Road to the electronic government' ('Op weg naar de elektronische overheid'), emphasising uniform authentication, standardisation, and broad adoption of electronic public service delivery.
- The 'Guidelines of the Ministry of Economic Affairs on Certification Service Providers', entered into force on May 21, 2003.[231]

12.5 Analysis

Three species of eIDs are distinguished within the Netherlands. They are all part of the DigiD concept. DigiD is part of a federated identity management scheme. Associated relying parties, typically public administrations such as municipalities, redirect users for authentication to GBO.overheid which authenticates the claimant and on successful authentication returns a BurgerServiceNummer ('Citizen Service Number' or BSN) to the relying party.

Apart from the DigiD, the government also recognises commercial ca certificates for a number of eGovernment applications.[232] These ca certificates are based on prior physical identification, i.e. the applicant has to appear in person before the CA to receive his credentials. Currently, four private certification authorities are recognised that comply with the required standards regarding qualified certificates defined in the Dutch eSignatures Act and which can be used for certain eGovernment applications. As trusted third parties they can deliver PKI based digital certificates for the generation of secure electronic signatures in eGovernment applications.

[229] Cf. Kamerstukken 25 880, number 2 and; HOF, S. v. d. (2007) – "The status of e-government in the Netherlands" in PRINS, J. E. J. (ed) Designing e-government pp 1-281; Kluwer Law International; pp 245-261 (pp 246)

[230] HOF, S. v. d. (2007) – "The status of e-government in the Netherlands" in PRINS, J. E. J. (ed) Designing e-government pp 1-281; Kluwer Law International; pp 245-261 (pp 246)

[231] Stcr. 8 mei 2003, p. 10, (see http://www.sdu.nl/staatscourant/) Beleidsregel van de Staatssecretaris van Economische Zaken met betrekking tot de aanwijzing van organisaties die certificatiedienstverleners toetsen op de overeenstemming met de bij of krachtens de Telecommunicatiewet gestelde eisen, op grond van artikel 18.16 van de Telecommunicatiewet.

[232] IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications: NATIONAL PROFILE NETHERLANDS.

According to the ENTR/05/58-SECURITY/SC1/NL_Profile, the four Dutch recognised certification authorities can also offer their certificates to foreign entities, and that no generic standards have been put in place to accept certificates issued by other entities. From an interoperability perspective, this means that any user of an application requiring commercial ca certificates is limited to these providers; no other certification service providers qualify. The four certification authorities are: Getronics PinkRoccade Nederland BV, Diginotar BV, CIBG, ESG De electronische signatuur BV.

eIDentity: DigiD

The current eIDs are provided through DigiD. Claimants that want to obtain an electronic identity, apply for this identity at DigiD, which is a service managed by a department of the Ministry of the Interior and Kingdom Relations, called 'GBO.overheid'.

The DigiD service comprises three assurance levels and hence three different kinds of DigiD's can be obtained by the claimant. The first and second assurance levels are called 'DigiD basis' and 'DigiD middle'. The third level, 'DigiD high', will be filled in by the Dutch electronic Identity Card, called 'eNIK', which is currently under construction.

A model of the DigiD scheme is provided in figure 3.

The DigiD basis level grants a claimant access on the basis of only a password and username. For most electronic services this assurance level is regarded sufficient. The middle level provides a higher assurance and currently consists of session-specific login codes that are provided to the claimant by means of text messages on their mobile phone (SMS, Short Message Service). The high level of authentication (the eNIK card) will be based on PKI, but is still under development (see above under 'debate and history').

DigiD is not governed by a specific Act, but primarily governed by contracts (terms and conditions) to which both claimants and relying parties are bound on registration, and several Royal Decrees. Because of this, the authentication levels of the DigiD scheme are not laid down in formal regulation. However, DigiD can be regarded to be an electronic Signature according to the 2004 Electronic Signature Act.

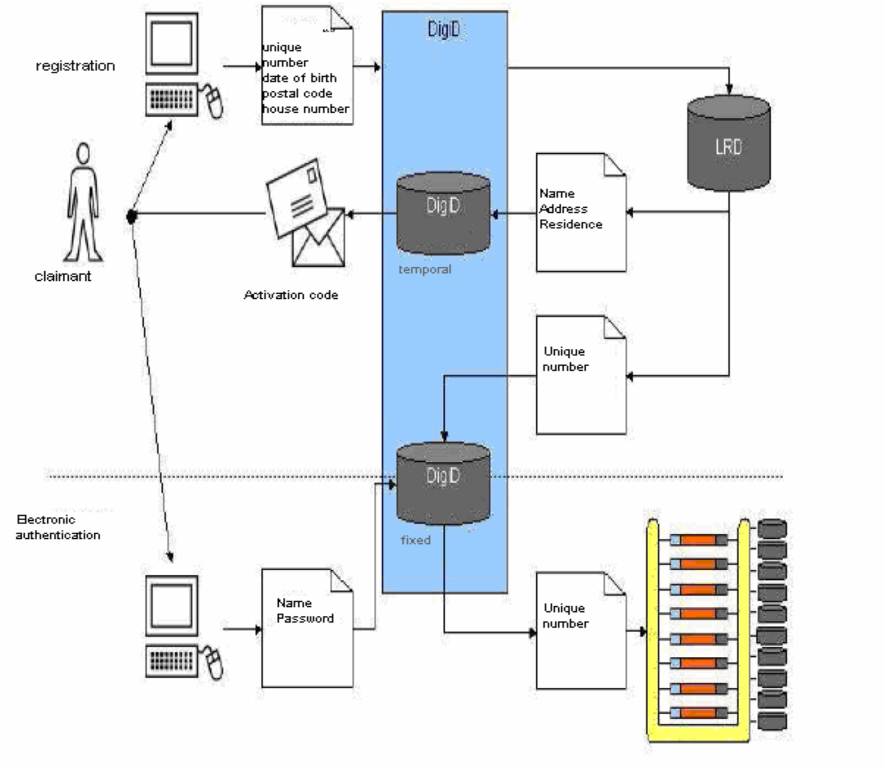

Figure 3: the DigiD scheme (www.DigiD.nl)

Form

The eID in the case of DigiD base level and DigiD medium level of authentication only consist of the BurgerServiceNummer and contains no additional data. In the Dutch context the eID does not need to contain additional data because all relying parties eligible for using the DigiD can obtain additional data pertaining to the client from the authentic registries on the basis of the BurgerServiceNummer. The BSN is released to a relying party when username and password of the claimant match. The middle level authentication is based on the use of the same username and password, but additionally the individual must submit a onetime transaction code that is forwarded to the mobile phone of the claimant.

The form of the eNik is not clear yet. The eNIK will consist of a chip card that holds a number of certificates and signatures. The content of the certificates is unknown.

Eligibility

A DigiD level base and medium can only be obtained by individuals that are registered in the Municipal Registry. One of the reasons for this limitation is that the information in the Municipal Registry is used to verify the individual's claims and to obtain the physical address to which the DigiD activation code will be sent (by ordinary mail).

Applicants provide their BurgerServiceNummer, their postal code, date of birth, and house number when applying for a DigiD on the GBO.overheid website (http://www.digid.nl). For application of a DigiD middle level-identity also a mobile phone number needs to be provided to GBO.overheid. Claimants have to agree to the terms and conditions regarding DigiD use on the registration website.

As the Municipal Registry plays a pivotal role in the registration process any resident in the Netherlands registered in the Municipal Registry can obtain a DigiD. This includes foreigners that have a relation with the Dutch government, like people that live in the Netherlands for a period longer than 4 months.[233] Non residents can not yet obtain a basis and middle level DigiD. However, a 'non-inhabitants registry' is under construction which, according to GBO.overheid, will provide non residents a possibility to obtain DigiDs as well.[234] Thus, the DigiD does not distinguish between Dutch nationals and foreigners.

It is unknown whether foreigners will be able to apply for a high level DigiD authentication in the form of a Dutch electronic identity card (eNIK).

Responsible Authority

GBO.Overheid and DigiD are the responsibility of the Dutch Ministry of Interior and Kingdom Relations. The responsibility for the Municipal Registry lies at the municipal college of burgomaster and alderman.

Issuer

The base and middle level DigiDs are issued by GBO.overheid, a department of the Dutch Ministry of the Interior and Kingdom Relations. DigiD and GBO.overheid are instituted by the temporary decree on the use of numbers for government access facility 2004 (Tijdelijk besluit nummergebruik overheidstoegangsvoorziening), the Royal decree on the administration of DigiD (Besluit beheer DigiD), and the Organisational decree directorate-general Administration (Organisatiebesluit directoraat-generaal Bestuur). The latter decree comprises the creation of GBO.Overheid, including a department responsible for Identification and Authentication which manages and develops DigiD (including PKI) and supervises certificate providers.

Attributes

The base and medium levels of DigiD consists of the BurgerServiceNummer (BSN), which is a unique identifying number for citizens registered in the Municipal Registry. The BSN is used as a key to re-

[233] Cf. S. 65 Act on the Municipal Registry

[234] Cf. http://www.digid.nl/burger/vraag-en-antwoord/aanvragen/#irfaq1

cords pertaining to individuals in other Dutch Authentic Registries (currently there are ten registries). One of these registries is the Municipal Registry, which contains information about residents in a municipality, such as name, last name, marital status, address, residence, and parents and children. The Municipal Registry is governed by the Act of 9 June 1994 on the Municipality Basic Administration. Other authentic registries are for instance, the Land Registry (Kadaster), Commercial registry, license plate registry. Three new registries are planned (e.g. underground registry, registry of non-residents).

Everyone who engages in relations with the Dutch government (and thus also persons that stay in the Netherlands for a longer time or work in the Netherlands) are granted a BurgerServiceNummer. This number, which replaced the Dutch Social-Fiscal (‘SoFI’) number in November 2007, is the single identifying number used in the citizen-government relations. Traditionally, public sector institutions use/used their own identifiers, such as a healthcare number, a student number, a social-fiscal number, and an ‘A-number’ (the identifier used in the administration). Many of these are replaced by the BurgerServiceNummer.

The BSN (9-digits) does not contain any personal information.[235] Section 8 of the Act on the BurgerServiceNummer states that the body of burgomaster and alderman assigns the BurgerServiceNummer to an individual immediately after registration in the Municipal Register. The Act on the Citizen Service number defines that only ‘users’ are allowed to use the Citizen Service Number. ‘Users’ are defined as administrative bodies (Article 1d(1) Act on the Citizen Service Number), or any other to which the use of a Citizen Service Number is prescribed by law (Article 1s(2)). For example, an employer may use of the number for limited purposes, for instance for tax purposes, but not as a general employee number. The use of the BurgerServiceNummer in the health care domain is regulated in the ‘Act on the use of the Citizen Service Number in Health Care’. The use of the BurgerServiceNummer is therefore restricted.

The eNIK will likely contain additional attributes, such as name and date of birth.

Conditions for use

The claimant, who has registered for a DigiD, has to accept the terms and conditions for the use (‘gebruiksvoorwaarden DigiD’) of this eID. According to the conditions for use, a claimant is ‘an organisation or a legal entity that is registered at the commercial registry or a natural person that is registered at the Municipal Registry of personal data, in possession of a sofi-number, BurgerServiceNummer, or any other number assigned by the government, and who has applied for a DigiD or for which a DigiD has been requested (article 1.5 DigiD Terms and Conditions)

The user is required to keep the DigiD strictly personal, and that the DigiD cannot be handed over (articles 2.8 and 2.9 of the conditions). Moreover, the user should immediately inform GBO.Overheid if (s)he knows that the eID has been abused or stolen.

Because the relation between GBO.overheid and the claimant is governed by an agreement, it can be difficult to impose sanctions to the claimant when a claimant does not adhere to these conditions.[236]

Claimants are not obliged to use the DigiD for government services, even though some government services are only available as eGovernment services, e.g. filing VAT tax returns. However, in general the principle of parataxis (nevenschikking) applies to government services, meaning that citizens should be able to choose to communicate with the government between: physical access, access in writing, access with telephone, or electronic access.[237]

[235] S. 2, Act on the Citizen Service Number

[236] Rapport nut of noodzaak regelgeving MijnOverheid.nl en DigiD, p. 22. Breaching the terms and conditions will result in default, but damages on the part of the government will usually be difficult to establish.

[237] See MvT Wet elektronisch bestuurlijk verkeer

The DigiD base level and medium level identities can only be used for services/parties that have a contractual relationship with GBO.overheid. This contractual relation is only accessible for institutions that are authorised to use the BurgerServiceNummer or another unique identifier. This rules out foreign relying parties (as well as private sector entities).

Creation and termination

The eID is issued upon verification of the information provided by the application a web-form, against the information that is recorded in the Municipal Registry. After verification, the applicant will receive an activation code by regular mail on the address associated to their BurgerServiceNummer according to the Municipal Registry. The applicant subsequently has to activate his DigiD by entering the activation code on the DigiD website.

Termination of the Digital Identity can be done by the identity provider (GBO.overheid), at all times.[238] A claimant can, at all times, delete his or her DigiD at the DigiD website.[239]

GBO.overheid not only issues the eIDs in the Netherlands, it also functions as the Authentication Authority.

12.6 Authentication Authority

Name:

The Dutch Authentication Authority is the same authority that issues the DigiD eID's. Thus, GBO.overheid both issues as verifies the eIDs.

What

The current eIDs that can be authenticated by GBO.Overheid are the DigiD base level and the DigiD medium level identities.

Input

When an applicant needs to be authenticated for an eGovernment service, the eGovernment service (relying party) will redirect the applicant to the Digid website. Upon completion of the authentication process, the claimant is redirected to the eGovernment service with either success (in which case the service will receive the claimant's BurgerServiceNummer) or failure.

The Authentication Authority requires the claimant to provide his username and password (base level authentication) or username, password and a session SMS token (medium level authentication).

Output

Output of the authentication process for DigiD-basis and DigiD-middle is the claimant's BurgerServiceNummer, which contains no information about the claimant. The legal conditions for the use of this output are defined by the Act on the Citizen Service Number and the Data Protection Act. Only government or other organisations that are authorised by law can use the BSN.[240]

For whom is the Authentication Authority?

The Authentication Authority can authenticate any base and medium level DigiD in the Netherlands.

The Authentication Authority can authenticate for any entity that has subscribed to its services. Only organisations that are authorised to use BurgerServiceNumbers can subscribe to DigiD and they have to accept the service's terms of use and terms of connection.

[238] S. 8 general terms of use DigiD, see. http://www.digid.nl/privacy/

[239] S. 2 (17) general terms of use DigiD

[240] Article 1d Act on the Citizen Service Number

Process

The eGovernment service (relying party) that requires claimants to authenticate redirect the user to the Authentication Authority which asks the user for username and password (and SMS token for medium level authentication) and returns either BurgerServiceNummer of an error message to the relying party.

Assurance level

Currently, GBO.Overheid can only provide authentication for base level authentication and for medium level authentication. The applicants' application is checked against data in the Municipal Registry and the activation details are sent to the applicant's home address (according to the Municipal Registry). Because the mail can be intercepted, non eligible individuals can obtain a DigiD on behalf of others. The assurance level of the DigiD therefore is low.

Other

Currently, the Dutch authentication scheme does not incorporate mechanisms for citizens to mandate others to act on their behalf. Hence, the requirements regarding intermediaries management and delegation outlined in the European eID framework are not met in the Netherlands at present. However, the Dutch Ministry of Economic Affairs and the Ministry of the Interior and Kingdom Relations have initiated a joint program aiming at establishing a common authorisation- and delegation facility ('Gemeenschappelijke Machtigings- en Vertegenwoordigingsvoorziening', GMV). The 'launching customer' for this facility will be the Dutch Tax Administration.

12.7 Conclusions

The Dutch electronic identity currently consists of the DigiD (base and medium level), which consists only of the BurgerServiceNummer. This renders the DigiD relatively useless in other member states: the BSN is just a number and does not contain any other data.

The BurgerServiceNummer may only be used by the government and other institutions that are authorised by law to use the number. The list of users is conclusive and does not contain foreign institutions. This is a barrier for cross-border authentication (at least for the current authentication levels in use).

Acquiring a Dutch eID (base and medium level) is currently only possible for Dutch residents registered in the Municipal Registry. The DigiD does not distinguish between Dutch nationals and foreigners.

Both claimants and relying parties are bound by the general terms and conditions for the use of Dutch eIDs.

13 Country report: Portugal[241]

13.1 Structure of the Administration

The structure of the Portuguese Administrative System has two main layers: Central and Local. It is a parliamentary republic of which the legislative power is assigned to a unicameral Parliament. The country is organised in Regions, Districts, Municipalities, and Localities.[242]

13.2 Debate (and history)

In Portugal, the development of e-ID started with the transcription of EU directives. But the main driver to the future spread of e-ID´s to the society in general, started with Technological Plan, that has the objective of developing of the Portuguese Information Society and improve the country's competitiveness. The plan, presented publicly in November 2005, is often referred to as the 'Technological Shock' and constitutes the central piece of the Government's economic policy. It consists in a series of articulated transversal measures aimed among other things at stimulating innovation by Portuguese companies, fostering research & development activities, improving education and training, and modernising the Public Administration.

The public programs for the promotion of information and communication technologies and the introduction of new relationship processes in society, between citizens, companies, non-governmental organisations and the State, with the purpose of strengthening the information society and of the electronic government (eGovernment), involve, for certain specific purposes, strong digital authentication mechanisms of identities and electronic signatures that can be substantiated through the use of the so called public key structures (PKI).

Examples of projects within the scope of the information society and of the electronic government are those regarding the Citizen's Card[243], the Portuguese electronic passport[244], the availability of the Public Administration services through the Internet which require strong digital authentication of identities and of electronic signatures and the dematerialisation of the intra and inter State organisations that require that type of authentication. [245]

13.3 eID model

Formal identities are provided by the state, and issued by central government related Organisations. In Portugal, IRN is the responsible Organisation.[246] This entity issues the official ID´s "Bilhete de Identidade" and the recent "Cartão de Cidadão", from now on, Citizen Card. These documents are issued based on the information IRN (under the Ministry of Justice) has of the citizen. For example, name, surname, address, gender. Nationality, information concerning relatives, etc. The Citizen Card, like its predecessor, aggregates basic Civil Information of the citizen, and is issued centrally by INCM.[247]

[241] Based on analysis by the TILT team and a country report written by André Vasconcelos and Fátima Carrão.

[242] www.epractice.eu portugal factsheet

[243] www.cartaodocidadao.pt/

[244] www.pep.pt

[245] Country report Portugal by André Vasconcelos and Fátima Carrão, Portugal.

[246] www.irn.mj.pt

[247] Country report Portugal by André Vasconcelos and Fátima Carrão, Portugal.

The Citizen Card, is also an eID Card that comprises electronic identities to its owner. In Portugal, electronic identities are provided/governed by the Electronic Certification System of the State (SCEE)[248].

Several citizen-oriented services (+800) are being offered to the citizen through the Citizen's Portal, which is the Portuguese central digital channel for public services. The Portugese eID, the Citizen Card (Cartao de Cidadao), needs to enhance the possibilities of the Citizen's Portal.[249]

The Citizen's Card is a smart card that needs to replace several existing identity cards. These are the Identification Document, the Tax payer's Card, the Social Security Card, the Voter's Card, and the Health System Card. It allows authentication by means of the telephone, the internet, and through personal contact.

The Citizen's Card holds several numbers, a chip for authentication purposes and a chip for qualified signatures. Attributes stored in the authentication certificate are obtained from the Instituto da Tecnologia da Informação na Justiça, which collects these data from several other institutes. [250]

The Portuguese eID model does not rely on one unique number, due to constitutional restraints.[251]

13.4 Principal legislation and policy documents

Legislation:
About the Citizen Card, the legislation is:

- The Law n.º 7, of 5 February 2007, governs the Citizen Card, and the relations between all parts of the scheme.

About Digital Certificates and eGovernment, the core legislation is:

- Article 268.º n.º 2 of the Portuguese Constitution establishes the fundamental right of access to administrative archives and registries, except for information related to state security, criminal investigation and personal privacy. A further law regulates the right of access to public documents (Law n.º 65/93, of 26 August, republished by Law n.º 94/99, of 16 July). On 7 September 2007 Portugal notified full transposition of the European Directive 2003/98/EC of 17 November 2003 on the reuse of public sector information, accomplished by Law n.º 46/2007.
- The Decree-Law nº 116-A, of 16 June 2006, governs the creation of the Electronic Certification System of the State (SCEE) – Private Key Infrastructure.
- The Decree-Law on Electronic Signatures n.º 62, of 3 April 2003, aims to align the legal regime for digital signatures established in a previous Decree-Law (Decree-Law n.º 290-D/99, of 2 August 1999) to Directive 1999/93/EC of the European Parliament and the Council of 13 December 1999, on a Community framework for electronic signatures. The Decree-Law nº. 165/2004, of 6 July and the Regulatory Decree n.º 25/2004, of 15 July constitute further legislation in this area.
- Published on 10 February 2004, Portugal's Law on Electronic Communications n.º 5/2004 transposes most of the EU new regulatory package on electronic communications. In particular, the law transposes directives 2002/19/EC, 2002/20/EC, 2002/21/EC and 2002/22/EC, all of the European Parliament and of the Council of 7 March 2002, and in addition the directive 2002/77/EC of the Council of 16 September. The European Directive 2002/58/EC on privacy and electronic communications is transposed by Law n.º 41/2004, of 18 of August.

[248] www.scee.gov.pt/ecee/en/

[249] ePractice.eu factsheet Portugal.

[250] IDABC interoperability country report

[251] IDABC Interoperability for PEGS Country report Portugal, p.9

- The Decree-Law on Electronic Commerce no. 7/2004, of 7 January and the Joint Order n.º 357/2006 of 28 April transposed into national law the EU Directive on electronic commerce (Directive 2000/31/EC).
- Law on the Protection of Personal Data was adopted on 26 October 1998. It governs the collection and processing of personal data and allows any person to access and correct their personal information held by a public or private body. The law transposes the Directive 95/46/EC of the European Parliament and the Council, of 24th October 1995, dealing with the treatment and circulation of personal data and is enforced by the National Data Protection Commission.
- The Law of Access to Administrative Documents n.º 65/93 was adopted in August 1993 and amended by law n.º 8/95, of 29 March, by law n.º 94/99, of 16 July, and by law n.º 19/2006, of 12 June. It allows any person to demand access to administrative documents held by state authorities, public institutions, and local authorities in any form. [252]

Policy:

- The Green Book for the Information Society (Livro Verde Para a Sociedade da Informaçao, 1997)
- The '2003 Plan of Action for Electronic Government', which was defined as an instrument of strategic and operational co-ordination, for the development of electronic government in Portugal. A development supported by the improvement of information technologies that put citizens and organisation, in the center of public service providers, contributing to State modernisation, leveraging efficiency and reducing costs. Examples of fundamental projects: Citizen Portal, Interoperability Norms Definition.
- The '2005 Technological Plan[253]' is an action agenda for all the Portuguese society, which aims at mobilising enterprises, families and institutions for surpassing the modernisation challenges the country has been facing during the last years. Within this context, the Portuguese Government has assumed the Technological Plan as a priority in the implementation of its public policies. Besides, the measures aggregated in the Technological Plan constitute the pillar for Growth and Competitiveness of the Portuguese National Reform Plan, designated National Action Programme for Growth and Jobs 2005-2008. Examples of fundamental projects: creation of the Citizen Card, creation of the Portuguese Electronic Passport, and the possibility of creation a Company in One Hour.
- The Simplex Programme (2006), aiming at the public administration's efficiency, transparency, and the improvement of the relation with citizens.[254]

13.5 Analysis

eIDentity: Citizen Card

Currently, an electronic identity is available to any citizen, when he applies for its Citizen Card – the new Portuguese ID. This is a service managed by IRN.

Name:

Citizen Card (Cartão do Cidadão).

Form

The Portuguese Citizen Card has the form of a smart card with an incorporated microchip for information storage. The card has the form of a physical document that identifies the citizen physically, and of a digital document for electronic authentication. Apart from the basic information of the citizen and other functions the eID includes two digital certificates (authentication and digital signature certificate). The card can be used in combination with a range of card readers. The front of the Citizen's

[252] Country report Portugal by André Vasconcelos and Fátima Carrão, Portugal.

[253] http://www.planotecnologico.pt/en/technological-plan/about-the-plan/list.aspx

[254] Country report Portugal by André Vasconcelos and Fátima Carrão, Portugal.

Card will have the holder's photograph and personal details. On the back there will be the identification numbers for the different public bodies, an optical reader area and the chip.[255]

Eligibility

The Portuguese Citizen Card can be obtained by any Portuguese Citizen or a Brazilian, as long as he is eligible by the Porto Seguro Treaty (agreement signed by Portuguese and Brazilian Governments).

The Card can be requested in any IRN office, and there is no territorial restriction. After the identity has been confirmed in all Organisms of the initiative, and the information to personalisation of the Card is gathered by the system that controls the Citizen Card Life Cycle (including the two digital certificates), the Card is sent to INCM for personalisation.

The citizen can only pick-up his Card, when he is in the possession of the "address confirmation letter", which is a letter sent to the citizens address, to confirm that the citizen is reachable in the address given in the Card request – this is required, since all Organisations of the initiative confer great importance to the citizens address.

Apart from this reason, this letter also contains critical information for the citizen to obtain is Card:

- PINs for the use of the digital certificates (authentication and digital signature), and the access to the address (the address, for security reasons, is only accessed by PIN);
- PUK for digital signature certificate "activation" – it is optional for the citizen to "activate" the use the digital signature certificate (and only allowed for activation if the citizen is more then 16 years old);
- Other information, like Card Activation Code, Cancellation Code, codes for unblock PINs.

The process to deliver the Card to the citizen follows strict rules. For example, it is used a functionality of the Card – the Match-On-Card, where citizen fingerprints are matched to the ones in the Card, obtained in the process of Card Request, and validated.[256]

The card is mandatory, and is issued to any child in the population register from the age of 6.[257]

Issuer

The issuer of the Portuguese Citizen Card is the Portuguese Government.[258]

The card will be distributed by the same location where the ID hard copy document is provided: the Local Civil Registry and Citizen's Shops ("Lojas do Cidadão").[259]

Responsible authority

The entity responsible for the registration process and other phases of the Card Lifecycle is IRN, institute of the Ministry of Justice. The SCEE manages the PKI and supervises certificate providers. [260]

Attributes

The physical part of the eCard contains the same information as the traditional ID-Card: Name, date and place of birth, date and place of issuance of the card, validity period of the card, parents, marital status, title and number of the card, picture and handwritten signature, residence, and National register number.[261] The chip of the eCard contains, besides the information that can be seen on the Card, the holder's address and two digital certificates, one for identification and authentication and one for a

[255] IDABC interoperability country report

[256] Country report Portugal by André Vasconcelos and Fátima Carrão, Portugal.

[257] IDABC interoperability country report

[258] Country report Portugal by André Vasconcelos and Fátima Carrão, Portugal.

[259] STORK D2.1., p. 35 ; IDABC interoperability report Portugal p. 9

[260] Country report Portugal by André Vasconcelos and Fátima Carrão, Portugal.

[261] IDABC interoperability country report

qualified electronic signature. The Citizen's Card will not contain data on its holder's tax, health or social security situation.[262] The contact circuit on the ID card also includes biometrical data in the form of photo and finger prints.[263]

The card is an exclusive authentication document and does not contain any information of the services that may access the card. Complementary information about the holder will continue to be held separately.[264]

The ID number(s) included on the card (civil number, fiscal identification number, health identification number, social security number) may not be processed or stored unless authorised by law or by permission of the Data Protection Authority.[265]

Conditions for use

The conditions of use the Portuguese Citizen Card, are regulated in Law n.º 7, of 5 February 2007. The citizen is not obliged to use the electronic features of the Card, but it is encouraged to do so. For example, when the citizen gets its Card, the authentication certificate is ready to use, like the digital signature certificate, but only if he opted to "activate" it.[266]

Creation and termination

The starting point is the Citizen Card request. The request respects strict procedures for guaranteeing the identity of the requester, and the identification of the citizen – this includes, amongst other validations, AFIS validation. Then, the request goes to the other State Agencies (Tax, Social Insurance, and Health Care) for identification of the citizen. The Portuguese Constitution prohibits the use of a Unique Identification Number amongst State Agencies. So, the functional and technological processes installed guarantees that each agency receives and stores its information. This is possible due to entities federation mechanism put in practice.

The Citizen Card is a smart card, and on its *chip*, apart from the information of the citizen, it includes two digital certificates for citizen usage (authentication certificate and digital signature certificate). The system responsible for the management of the Citizen Card lifecycle is responsible for aggregating the information, including the electronic certificates that go to the card, and sending it to the Organisation responsible for its personalisation (Central Card Personalisation) - INCM.

The identification of the Citizen in the various Agencies part of the initiative is automatic for the majority of the Citizen Card requests. This is due to the implementation of automated schemes for identifying the citizen in the systems of all agencies involved.

This allows that the Citizen Card is available for delivery to the citizen in 5 days after the request.[267]

The Card is valid for a period of five years, and is mandatory for all people registered in the population register.

[262] http://www.cartaodecidadao.pt/index.php?option=com_content&task=view&id=8&Itemid=35&lang=en

[263] IDABC Country report interoperability, p. 14; https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/bin/view.cgi/Main/PortugueseProfile

[264] http://www.cartaodecidadao.pt/index.php?option=com_content&task=view&id=8&Itemid=35&lang=en

[265] Article 16, Lei n.o 7/2007 Cria o cartão de cidadão e rege a sua emissão e utilização

[266] Country report Portugal by André Vasconcelos and Fátima Carrão, Portugal.

[267] Country report Portugal by André Vasconcelos and Fátima Carrão, Portugal.

13.6 Authentication Authority

Name

Electronic Certification System of the State (SCEE)

What

The claimant can be authenticated by the middleware. It is responsibility of all service providers, to validate the certificate used against the CRL (Certificate Revocation List).[268] The eIDs are validated against a PKI Infrastructure. Under SCEE hierarchy, there is a CA for the Citizen Card, amongst others recognised by SCEE.[269] Under Citizen Card CA, we find the CA for the Authentication and Digital Signature.[270]

Input

When the citizen needs to be authenticated for an eGovernment service or any other service provided by Private Sector (if the website is ready for authentication with certificates), he/she uses its eID (digital certificate from Citizen Card). The certificate is accessible though Portuguese Citizen Card Middleware (software available in www.cartaodecidadao.pt). For its use, the citizen needs additionally to have its Card inserted in a compatible smartcard reader. The Card, and the digital signature certificate, also allows the citizen to digitally sign e-mails, documents, etc.

Output

The outputs are: Citizen Authenticated in a website using the authentication certificate of the Card. The SCEE operates independently from other public key infrastructures of a private or foreign nature, but allows the interoperability with the infrastructures that fulfil the necessary authentication rigour requirements in line with the EU signature regulation.[271]

For whom

Any citizen or entity can validate the certificates on the Cartão de Cidadão. [272]

Assurance level

The assurance level is high, since the use of the certificates is dependent of two factors: the Card possession, and the PIN knowledge that allows its use

13.7 Conclusions

Portugal implements a smart card, the Cartão de Cidadão, including an authentication certificate and a certificate for non-repudiation digital signatures.

The card contains: Name, date and place of birth, date and place of issuance of the card, validity period of the card, parents, marital status, title and number of the card, picture and hand written signature, residence, and National register number, the holder’s address and two digital certificates, one for identification and authentication and one for a qualified electronic signature.

The ID number(s) (civil number, fiscal identification number, health identification number, social security number) included on the card may not be processed or stored unless authorised by law or by permission of the Data Protection Authority.[273]

[268] Country report Portugal by André Vasconcelos and Fátima Carrão, Portugal.

[269] www.scee.gov.pt/ecee/en

[270] Country report Portugal by André Vasconcelos and Fátima Carrão, Portugal.

[271] Country report Portugal by André Vasconcelos and Fátima Carrão, Portugal.

[272] Country report Portugal by André Vasconcelos and Fátima Carrão, Portugal.

[273] Article 16, Lei n.o 7/2007 Cria o cartão de cidadão e rege a sua emissão e utilização

14 Country report: Slovenia[274]

14.1 Structure of the Administration

The Slovenian constitutional system is a parliamentary republic. The state's authority is based on the principle of separation of the legislative, executive and judicial powers, and a parliamentary system of government.

Legislative power is held by a unicameral parliament, the National Assembly, which has exclusive jurisdiction over the passing of laws. The National Council is mainly an advisory body without full lawmaking powers. The Head of State is the President of the Republic. Executive power is exercised by the Government, which consists of the Prime Minister and other Ministers. The Government and the ministers are independent within the framework of their jurisdiction, and responsible to the National Assembly.

Slovenia has a single-level system of local self-government; a municipality regulates only local tasks.[275]

The highest decision-making authority for eGovernment projects at the national level is the Coordinating Body for Better Public Administration. The Ministry in charge for the development of eGovernment in Slovenia is the Ministry of Public Administration. At the local level the major responsibility is in the hands of the Government Office for Local Self Government and Regional Policy.[276]

The Ministry's 'Directorate for e-Government and Administrative Processes' is the body in charge of reforming administrative processes and developing eGovernment in order to bring services closer to citizens and businesses. The Directorate provides infrastructure which represents a solid platform for electronic application and e-service provision. This includes for example: a national telecommunication network (HKOM) which connects all central departments; a data centre; a system of central administration registers (e.g. Central Register of Population, the Business Register), back-office automation (electronic accounting system, human resources system and archiving system); single access points for services to citizens and businesses (e.g. e-government State Portal e-Uprava, and the business portal e-VEM); public-key infrastructure for secure authentication. Slovenia is currently working on the development of a national interoperability framework which will include a common set of standards, guidelines, solutions and architectures which can be used to link databases, applications and information systems.

14.2 Debate (and history)

There are four Certificate Service Providers in Slovenia (see below). The certificates are either software certificates of they can be stored on the smart card depending on users' choice. In Slovenia there were several attempts to introduce national eID card (smart card) which raised social debate.

The Slovenian national eID card project officially started in February 2003 with the establishment of a dedicated project group. The Identity card Act was amended in April 2008 and now presents new legal grounds for the introduction of electronic ID card. According to the proposals put forward by the Slovenian Government the future eID card would incorporate several functions by combining several sensitive datasets on just one card. The cards will include on the chip, the holders' name and address, their Personal Tax Number, their unique Personal Registration Number (PRN), their Healthcare Insurance Number. Personal identification number and tax number are to be stored in encrypted form preventing unauthorised access without the citizen consent. The card will possibly contain two digital Qualified Certificates: one providing access to eGovernment services, the other for confirming healthcare insurance rights. The Slovenian ID card is to be authentic instrument, used by citizen to prove

[274] Based on analysis by the TILT team and a country report written by Davorka Šel, Aleš Pelan, Brane Kren and Katarina Čepon.

[275] Factsheet – Slovenia - Country Profile; epractice.eu, June 2008.

[276] IDABC interoperability for PEGS country report Slovenia, November 2007, p. 14-15.

his/her identity and citizenship and for crossing the Slovenian border. In the summer 2008 the eID card project was put on hold. The new government which is to be constituted after elections in September 2008 is to decide about the future of the eID card project.[277]

14.3 eID model

There are four Certificate Service Providers (CSPs) delivering certificates to the public in Slovenia that are registered at the Ministry of Higher Education, Science and Technology. All of them issue qualified certificates that form in a sense the »de facto« standard in e-services in Slovenia and e-government applications follow it by putting this demand into the Decree on administrative operations. According the Decree on Administrative Operations, which resides under the General Administrative Procedure Act, the eGovernment services operations for citizens and businesses can be performed by any qualified certificate. The certificates, issued by Slovenian CSPs, are widely used in different eGovernment applications.[278]

Every citizen in Slovenia has 3 national identifiers being:[279]

- Personal Registration Number

  Every Slovenian citizen is registered with the Slovenian Central Register of Population (CRP) and receives a unique Personal Registration Number (PRN – Slovenian abbreviation: EMŠO) as defined in the Central Population Register Act. Citizens usually become registered with the CRP at birth or immigration. Other individuals who have no PRN but have to exercise some rights or duties in Slovenia become registered with the CRP as well. For instance, even foreigners become registered with the CRP thus receive a PRN in the event of buying a Slovenian property or other events.[280] The PRN is a thirteen-digit number containing date of birth, label of the register, gender and a control number.[281]

- Personal Tax Number

  The tax number in Slovenia is defined by the Tax Administration Act. The tax number is the identification sign which defines the taxpayer (individuals and legal entities), and it is used for uniform specification and connection of data in tax records about the taxpayer, which are managed by the Tax Administration. The tax number is a random eight-digit number used for all taxes.

- Health Insurance Number.

  Health insurance identification: the identifier is the “unique identification insurance number” (HIIS number, in Slovene “*številka ZZZS*”).

Every legal person has the following identifiers:

- Identification Number

  Every entity holds a uniform 7-digit Identification Number that is assigned to the entity when it gets registered in the primary register. Identification Number is intended to be used in data exchange between business entities themselves and registration offices.[282]

[277] Country report Slovenia by Davorka Šel, Aleš Pelan, Brane Kren and Katarina Čepon, Slovenia.

[278] Country report Slovenia by Davorka Šel, Aleš Pelan, Brane Kren and Katarina Čepon, Slovenia.

[279] IDABC interoperability for PEGS country report Slovenia, November 2007, p. 10.

[280] Modinis IDM country report Slovenian, July 2006.

[281] IDABC interoperability for PEGS country report Slovenia, November 2007, p. 17.

[282] IDABC interoperability for PEGS country report Slovenia, November 2007, p. 18.

- VAT Number.

  See ‘Tax Number’ above. When Slovenia joined the EU, the Tax number got the prefix SI (code for Slovenia) for VAT purposes.

The identity card is defined in the Identity Card Act and is not obligatory in Slovenia. Every Slovene citizen with permanent residence in Slovenia is entitled to posses an identity card, which can be issued also to an underage person if his/her parents or legal representative apply for it. A Slovene citizen with temporary residence in Slovenia can obtain an identity card if he/she is 18 years old and doesn’t posses a valid official identification document. The identity card can be also used as a travel document in EU Member States, Croatia, Iceland, Liechtenstein, Norway and Switzerland.[283]

The legal basis for the introduction of digital certificates and electronic signatures in eGovernment applications for administrative operations can be found in the Decree on administrative operations. According to the decree the e-government applications for citizens and private sector can be performed by any qualified certificates issued by registered CSPs, governmental CAs and other commercial certification authorities.

14.4 Principal legislation and policy documents

Legislation:

The e-ID systems are built according to the Slovenian Data Protection Act but the question of authentication is not especially emphasised by law [284] and there is currently no overall eGovernment legislation in Slovenia.

General Administrative Procedure Act (Official Gazette of the Republic of Slovenia, no. 105/2006-ZUP-UPB2), which was addopted in 1999 and several times amended, where the last amendment was in 2006, provides the general legal basis for all administrative proceedings; i.e. all Administration to Citizen (A2C) and Administration to Business (A2B) and a major part of Administration to Administration (A2A) relations. Among the main provisions of the Act is one allowing for two-ways and full electronic communications between administration and citizens. Before the entry into force of this text, citizens could post their eDocuments through the eServices of the eGovernment state portal by using the web application and digital signature, but the answer from the administration could be expressed by classical mail only. This Act thus legalised what is qualified as “eDelivery”.

Decree on Administrative Operations This decree was adopted in 2005 and amended several times since then. It forms the legal basis for the introduction of eSignatures in eGovernment services and applications (administrative operations). According to the decree, the eGovernment services operations for citizens and businesses can be performed by any qualified certificates issued by registered Certificate Service Providers (CSPs), governmental CAs and other commercial certification authorities.

Act amending the Electronic Commerce and Electronic Signature Act The initial version of the Electronic Commerce and Electronic Signature Act (ECESA) was adopted by the Slovenian Parliament on 13 June 2000 and came into force on 22 August 2000. It provides the legal basis for using eSignatures and developing eServices in Slovenia.

The Act amending the Electronic Commerce and Electronic Signature Act, adopted in April 2004, defines more precisely the responsibilities of providers of Information Society services and sets the conditions for the realisation of the electronic identity card project.

[283] IDABC interoperability for PEGS country report Slovenia, November 2007, p. 16.

[284] Modinis IDM country report Slovenian, July 2006.

Slovenian legislation literally translated the definitions of “advanced” and “qualified” electronic signature of the Directive 1999/93/EC of 13 December 1999 on a Community framework for electronic signatures. However, the word “secure” is used for referring to an advanced signature. As defined in the Act, the devices for secure electronic signing should comply with special conditions regarding security and reliability. Those conditions should be more detailed in a Decree that is still to be adopted. In accordance with the Directive, electronic signatures for internal governmental applications must be secured by qualified certificates issued by one of the Certification Authorities at the Ministry of Public Administration.

Access to Public Information Act The initial version of the Access to Public Information Act was adopted and came into force in 2003. The Act was amended lastly in March 2006.

The current version of the Act provides everyone with a right to access information of public character held by state bodies, Local Government agencies, public agencies, public contractors and other entities of public law. The bodies must respond within 20 days.

There are exemptions for: classified data; business secrets; personal information that would infringe privacy; confidentiality of statistics information; public archives; tax procedure; criminal prosecutions; administrative or civil procedures; pre-decisional materials that would lead to a misunderstanding; nature conservation; and internal operations. Amendment passed in July 2005 introduced the public interest test, which can reveal even the most hidden faults and irregularities taking place in the public sector and thus greatly enhance public sector transparency and public trust in Government institutions.

The original Act also established an independent body; the Commissioner for access to public sector information, competent for deciding on an appeal against the decision by which the body dismissed the request or refused the access to public information. Since January 2006, this responsibility has been taken over by the Information Commissioner. Fines can be imposed for destruction of information or failure to disclose without authorisation.

With the Act on Access to Public Information, the Directive 2003/4/EC of 28 January 2003 on public access to environmental information was transposed into Slovenian Law.

Personal Data Protection Act The Personal Data Protection Act currently applicable was adopted in July 2004, came into force on 1 January 2005 and was amended in July 2007. It replaced a previous version of the Act adopted in 1999, and transposed the EU Directive 95/46/EC on Data Protection into Slovenian law.

The main goal of the Act is to prevent illegal and unwarranted violations of personal privacy in the course of data-processing, and to ensure the security of personal databases and of their use. Until 1 January 2006, the Inspectorate for Personal Data Protection was in charge of overseeing the application of the Act. Since that date, such responsibility has been transferred to the Information Commissioner (Information Commissioner Act, adopted in December 2005).

Electronic Communications Act The Electronic Communications Act was adopted in March 2004 and came into force on 1 May 2004. It was lastly amended in 2006. The Act aims to establish effective competition in the electronic communications market, maintain effective use of the radio frequency spectrum and of the number space, ensure universal services and protect user’s rights. This Act encompasses all relevant issues that are separately dealt with by the EU directives forming the so-called EU Regulatory Framework for Electronic Communications, namely: Directive 2002/21/EC (‘Framework’ Directive); 2002/20/EC (‘Authorisation’ Directive); 2002/19/EC (Access and interconnection Directive); 2002/22/EC (‘Universal service and user’s rights Directive); and 2002/58/EC (‘ePrivacy’ Directive).

eArchiving Legislation The Protection of Documents and Archives and Archival Institutions Act and the Regulation on documentary and archival material custody were both passed in 2006 with the aim to regulate electronic content management.

All electronic records, including digitalised documents have full legal effect provided they comply with technical conditions. The regulation governs the activities and internal rules for individuals to keep documents and/or archives, the storage of such materials in physical and digital form, the general conditions, registration and accreditation of digital storage equipment and services, the selection and transfer of archives to public archival institutions, the processing and the keeping of registers of archives, the protection of film and private archives, the use of archives in archival institutions and the work of the Archival Commission.

Both acts also contain provisions regarding the long-term validity of eSignature. [285]

Policy:

The strategic objectives for e-government development in Slovenia are outlined in the Slovenian e-Government Strategy 2006-2010 (SEP-2010) and are aligned with the objectives of the Development Strategy of Slovenia. They focus both on the back-office (e.g. to improve overall government efficiency) and front-office dimensions of the use of ICTs in government (e.g. to improve user satisfaction, service delivery and quality, and to promote citizen access to information and participation in government). The strategy for e-government development in Slovenia is well articulated and includes a vision statement and strategic orientations illustrating the key principles supporting e-government development (e.g. user centricity, simplicity, transparency). Based on the strategic orientations, the strategy also sets out targets for 2010 and identifies projects/activities to implement them. A management model for the implementation of the e-government projects has been established.

The vision and strategy for e-government are accompanied by an action plan (Action Plan for E-government 2006-2010) which details the measures to be carried out to implement the strategy. Progress made in implementing the action plan is measured according to a series of indicators (e.g. number of services provided, use of services, user satisfaction). While the SEP-2010 covers aspects that are common to local government (e.g. e-government communication infrastructure and networks), a specific E-government Strategy for Local Self-Government provides the frameworks for e-government development at the local level.

The Strategy lists amongst information solutions to be completed within its time frame:

- Identification and authentication: it will be necessary to establish a system (module) which will enable simple and user-friendly identification (electronic identity) and authentication for all eGovernment services. [286]

14.5 Analysis

eIDentity: username/password[287]

Form

For the lowest trust level (out of the four distinguished in Slovenia), the citizen can make use of username/password:

- Where the registration is performed on-line by send-out of confirmation e-mail with username, initial password defined by the system and active URL to an address indicated by citizen

[285] Country report Slovenia by Davorka Šel, Aleš Pelan, Brane Kren and Katarina Čepon, Slovenia.

[286] Country report Slovenia by Davorka Šel, Aleš Pelan, Brane Kren and Katarina Čepon, Slovenia.

[287] IDABC interoperability for PEGS country report Slovenia, November 2007, p. 23 and Country report Slovenia by Davorka Šel, Aleš Pelan, Brane Kren and Katarina Čepon, Slovenia.

- While the authentication is carried out by assigned combination of a username and password chosen by user. However the initial password is determined by the system and the user can change the initial password upon registration with the initial password.

eIDentity: soft certificates

Since the national eID cards have not been introduced yet currently most eGovernment applications use authentication and digital signature capabilities based on qualified certificates from certain registered certification authorities, governmental as well as commercial:[288]

1. Certification authority at the Ministry of Public Administration (in Slovene "*Overitelj na Ministrstvu za javno upravo*"), Tržaška cest 21, SI-1000 Ljubljana, Web: http://www.ca.gov.si.
2. HALCOM informatika d.o.o., HALCOM informatika d.o.o., Tržaška cesta 118, SI-1000 Ljubljana, Web: http://www.halcom.si
3. AC NLB (Certification Authority at the bank "*Nova ljubljanska banka*"), Šmartinska 132, SI-1520 Ljubljana, Web: http://www.nlb.si/acnlb.
4. POŠTA®CA (Pošta Slovenije), Slomškov trg 10, SI-2500 Maribor Web: http://postarca.posta.si.

The certificates are software certificates, but can also be stored on smart cards, which is foreseen for the Slovenian e-ID card.

All of them are based on prior physical identification, i.e. the requesting party needs to appear personally before the CA to receive his credentials. As trusted third parties they can deliver PKI based digital certificates for the generation of secure electronic signatures in eGovernment applications. Such certificates are widely used in different eGovernment applications.

Attributes

Certification Authorities in Slovenia use different approaches in mapping single certificates with its holder's identifiers (e.g. personal tax number or Personal identification Number) but all of them manage some connection between the user and his certificate. Some Certification Authorities simply add the personal tax number in certificates, while others add a unique certificate identification (serial number) to a certificate and keep all the data in a stand-alone database (like the Certification authority at the Ministry of Public Administration). Personal data in this database can only be used under conditions regulated in Personal Data Protection Act (Official Gazette of the Republic of Slovenia, No. 86/2004, 113/2005-ZInfP).

eIDentity: Slovenian eID card

Name

The Slovenian e-ID card is not introduced yet but will contain the, already existing, qualified digital certificates.

Form

The eID cards had still not been introduced. In April 2008 the Identity card Act was amended, thus providing new legal grounds for the introduction of the electronic ID card.

Eligibility

The Slovenian ID card with microchip holding qualified digital certificate issued by governmental Certification Authority will be issued to citizen older than 14 years. Foreigners can not apply for the eID card. The condition to obtain a certificate is to have a PRN and a Tax number in Slovenia.

[288] IDABC interoperability for PEGS country report Slovenia, November 2007, p. 28.

Issuer

Individuals will be required to request for a Slovenian e-ID card at a registration authority at an administrative office.[289] The individual must be registered with the Central Register of Population (CRP) thus the individual has got her personal registration number (PRN) already. Based on the personal data the e-ID card will be personalised. The governmental certification authority SIGEN-CA issues qualified certificates for the individual which will be stored on the e-ID card. Certificate serial number (SN) is stored in a special database along with the PRN.[290]

Responsible authority

Ministry of the Interior

Attributes

According to the latest proposals the eID card would incorporate several functions by combining several sensitive datasets on just one card. In addition to their holders' name and address, their Personal Tax Number, their unique Personal Registration Number (PRN), their Healthcare Insurance Number, the serial and register number of the personal ID, and possibly two key-pairs thus two electronic certificates: one certificate/key-pair for authentication and encryption purposes, a second certificate for creation of electronic signatures. Both the Personal Registration Number and the Personal Tax Number will be stored in encrypted form so as to prevent unauthorised access without the citizen's consent.[291]

Besides providing an electronic identity the Slovenian e-ID card shall be used as conventional ID card as well. Therefore, the layout of the front side is to contain the cardholder's personal data and her/his image. Upon latter decision the card should be ready to upload additional biometric data.

Persons are authenticated by password (PIN) and electronic signatures are used.

Conditions for use

The e-ID system is not limited to e-government applications only; it can be used for other applications as well.[292]

14.6 Authentication Authority

The e-ID system is driven by central authorities: the Ministry of Public Administration. The register of Tax numbers is driven by the Slovenian Tax Authority; the Central Register of Population resides under the authority of the Ministry of Interior.[293]

All above mentioned CSPs began issuing digital certificates with clear intentions and expectations about their users. The CSP at the Ministry of Public Administration started issuing certificates to the public to promote e-government applications, CSPs HALCOM-CA and AC NLB focused primarily on issuing certificates for e-banking, while CSP POŠTA®CA started issuing digital certificates as a part of a service called »Secure mailbox« (eDelivery) which is also offered by the Slovene Post.

E-service providers take different approaches in selecting supported CSPs – some rely only on certificates issued by a specific CSP, others define groups of CSPs – but the most frequent solution is to support all qualified digital certificates issued by registered CSPs.

[289] According to the IDABC interoperability for PEGS country report Slovenia, November 2007, p. 16, an application form for an identity card can be filed in every administrative unit information office.

[290] Modinis IDM country report Slovenian, July 2006.

[291] Factsheet – Slovenia – National Infrastructure; epractice.eu, June 2008 and Modinis IDM country report Slovenian, July 2006.

[292] Modinis IDM country report Slovenian, July 2006.

[293] Modinis IDM country report Slovenian, July 2006.

Certification Authorities keep different kinds of user data:

- Personal Registration Number and/or Tax Number for citizen,
- Identification Number and/or VAT number for legal person.

Certification Authorities that keep data in stand-alone database offer different interfaces for applications to connect to the database; usually there is a web-service (SOAP) or some other kind of interface (ODBC, JDBC) available.

14.7 Conclusions

Slovenia is planning to introduce smart card based e-ID cards. Currently citizens can obtain e-government services by means of username/password for low sensitivity services and qualified digital certificates for higher levels of assurance.

Slovenes have three identifiers: Personal Registration Number (EMŠO), Personal Tax Number and Health Insurance Number.

Slovenia has an extensive set of authentic registries. Because of the nature of the data kept in the CRP all its users are required to have proper legal basis.

15 Country report: Spain[294]

15.1 Structure of the Administration

Spain is today a regional state with seventeen autonomous communities (regions). This makes the central and regional eGovernment differ on level, speed of development, level of implementation and extent of the eGovernment applications.

The efforts of all Administrations on electronic information sharing, is leading to the so-called "unique counter" (*ventanilla única*). This objective means that all citizens will be able to do any official interaction with the administrations at any official Registry (state/regional/local) without presenting physical, and officially registered, documents or data. This will be possible because all Administration bodies will share information.

However, this horizontal integration between eGovernments should be driven by the services described below.

State eGovernment

eGovernment initiatives and applications are developed independently in every Ministry, and the Ministry of Public Administrations – MAP –is responsible for steering the development and implementation of eGovernment in Spain's central state administration. These tasks are co-ordinated at state level by the Directorate General of Impulse of the Electronic Administration (*DG para el impulso de la administración electrónica*) in the Ministry's General Secretariat for Public Administrations.

In addition, the Higher Council for Electronic Administration is in charge of leading, co-ordinating and monitoring the implementation of eGovernment across central government and participates in the Sectorial Committee of eGovernment, which is the technical organ in charge of eGovernment cooperation among the three levels of Spanish Administration: state, regional (autonomous communities) and local (municipalities).

In Spain, the Law for Electronic Access by Citizens to Public Administrations (LAECSP)[295] obliges that all public administration services will be offered online. In this way it requires the use of different channels for eServices, and the right of citizens to choose between them without restrictions; including an Internet access point in public offices on the street. Up to now, the single multi-channel access point for all the current services; using or not electronic certificates is made via the 060 network: www.060.es with 24x7 availability. It provides a full co-ordination of all services offered by the national, regional and local administrations, without requiring the users to know which administration is providing them.

The main effort of state government is aimed to the use of the DNIe card[296], which is horizontally coordinated by the "Oficina Técnica del DNI electrónico" (DNIe card Technical Office).

Regional Government

Regional (Autonomous Communities) eGovernment initiatives using electronic authentication systems are lead and co-ordinated by their respective regional Administrations. Although usually a specific

[294] Based on a country report written by Jose Fernando Carvajal Vión complemented by an analysis by the TILT team.

[295] LAECSP Ley Para el Acceso Electrónico de los Ciudadanos a los Servicios Públicos. BOE 23-06-07 http://www.map.es/iniciativas/mejora_de_la_administracion_general_del_estado/moderniza/Administracion_Electronica/parrafo/05/document_es/A27150-27166.pdf

[296] DNIe Royal Decree 1553/2005, of December 23, ruling the national identity card and its eSignature certificates.http://www.dnielectronico.es/marco_legal/RD_1553_2005.html

Public Body, department or entity is in charge of its coordination, the information about eGovernment is dispersed and not clearly available.

It is important to note here, in order to facilitate a proper comparison with other Member States, that management of specific matters such as education or health have been transferred to the Spanish Regions and only residual competencies are kept by the State Government.

A good example is the *Gencat.cat*, the website of the Catalan Regional Government. It is an example of a radical redefinition of the eGovernment portal concept, and a mass-scale deployment based on transparency and Web 2.0 philosophy in public administration, fully backed by a policy driven strategy focused on an integrated citizen-centric approach. However, not all regions have the same maturity state.

Local eGovernment

Local eGovernment initiatives are lead and coordinated by local authorities, mostly municipalities. Unfortunately, the development degree for municipalities is even less than that for regional eGovernment initiatives. Even so, there are also good examples as the Madrid City's homepage, which is in the top five places on the report "Digital Governance in Municipalities"[297].

In Spain, the Plan Avanz@'s policy is to connect electronically all Spanish municipalities (more than 8.000), most of which do not yet have broadband access or public offices. This includes the eModel Programme that finances projects in order to ensure that about 2010, all citizens will be able to communicate electronically with the administrations, without discrimination due to geographic (or other) reasons.

Most of the Spanish Municipalities are developing and testing projects for "Ciudades Digitales" (Digital Cities) in order to transform fully their Local Governments to permit the citizens to have access to all public services by using the municipalities' web pages, with different sections addressed to citizens (A2C), enterprises (A2B) and public officers (A2A) by means of their intranet.

The Higher Council for Electronic Administration takes care, among others, of computer co-operation among Administrations and others entities like local ones. It promotes the collaboration and co-operation among the Spanish Regions and municipalities, the use of telecommunications in the Administration, the Security Policy and the improvements in quality and productivity in the information services development.

15.2 Debate (and history)

The National Identity Card (commonly known in Spain as DNI) was created by "Decreto de la Presidencia del Gobierno de 2-3-1944 (B.O.E 81)" and it substituted the olds mid's s. XIX "personal identification cards"[298]. Through the years 1951 to 1992 the DNI card has been issued on up to seven different cards supports, and this last support is being substituted since 2006 by the DNIe[299]) with a tendency to putting down less personal data on in.

Now the data printed on card and their electronic form have been merged on the DNIe card, to facilitate both physical and electronic identification. This card is compulsory for persons over 14 years.

[297] S.K. Marc Holzer, "Digital Governance in Municipalities Worldwide (2007)"; http://andromeda.rutgers.edu/~egovinst/Website/PDFs/100%20City%20Survey%202007%20(Full%20Report).pdf.

[298] Pablo Sanjuán García, "Dni–history"; http://www.lexnova.es/pub_ln/revistas/revista_ln/Revista42/10_Cronica.pdf.

[299] DNIe Royal Decree 1553/2005, of December 23, ruling the national identity card and its eSignature certificates.http://www.dnielectronico.es/marco_legal/RD_1553_2005.html

The issuance of the DNIe card began in 2006, and therefore a certain period of time will elapse before all Spanish citizens have the DNIe card due to the underlying renovation process.

The Organic Law 1/1992 of February 21st on Citizen Security Protection regulates the issuance of the National Identity Card and who can issue it, and lately, the DNIe Royal Decree 1553/2005, of December 23rd, rules the national identity card and its eSignature certificates.

In Spain, three types of "persons" need identification to interact with Public Administration services:

Nationals

As DNIe is compulsory, when requested for the first time, the physical presence of the person is required, as well as the presentation of a birth certificate granted by the corresponding Civil Registry[300] [5, 6].

The Civil Registry stores date of birth, parents, name and surnames and any changes of these data, the judicial modifications of the persons' capacity, if he/she is insolvent, in bankruptcy or suspension of payments; declarations of absence or death, nationality and neighbourhood, parental rights and duties, guardianship and other legal representations, marriage and death.

The use of the DNI is a habit in Spanish society, but there is much ignorance regarding the possibilities offered by the electronic identification of the DNIe.

Non-Nationals

Non-national residents have a legal framework that regulates[301] their identification and other issues. They are identified by a resident card with a number "Número de Identificación de Extranjeros", commonly known as "NIE" on an identification card "Tarjeta de Residente". This card attests the legal residence of foreigners in Spain, their identity and that they have been granted the corresponding authorisation or the recognised right to stay in Spanish territory for more than three months. An exception is made for E.U. nationals, as no previous administrative resolution is required for them when applying for their resident card. EU-foreigners staying in Spanish territory have this right, but also have the obligation to bear a document that proves their identity, issued by the competent authorities of their country of origin or the country where they come from.

At present, foreign citizens, holders of a NIE card can obtain an electronic certificate as an authentication means in order to make on-line transactions with the Spanish Administration. The foreigner's identity card requires prior identification before a Certification Service Provider can issue the qualified

[300] CRO The Civil Registry Office is regulated in the Law of June 8, 1957, in Decree of November 14, 1958. "Real Decreto 644/1990, de 18 de mayo, por el que se dictan normas relativas al Registro civil Central. - BOE. Boletín Oficial del Estado - vLex"; http://vlex.com/vid/18142232.

Ruling of the Law on Civil Registries, Royal Decree 644/1990 of May 18 on the rules regarding the Central Civil Registry Office. "Ley de 8 de junio de 1957, sobre el Registro Civil."; http://noticias.juridicas.com/base_datos/Privado/lrc.html

[301] Ruling of the Law on Civil Registries, Royal Decree 644/1990 of May 18 on the rules regarding the Central Civil Registry Office. "Ley de 8 de junio de 1957, sobre el Registro Civil."; http://noticias.juridicas.com/base_datos/Privado/lrc.html

Royal Decree for Ruling the execution of Organic Law 4/2000 of January ."REAL DECRETO 864/2001, de 20 de julio, por el que se aprueba el Reglamento de ejecución de la Ley Orgánica 4/2000, de 11 de enero, sobre derechos y libertades de los extranjeros en España y su integración social, reformada por Ley Orgánica 8/2000, de 22 de diciembre."; http://www.boe.es/boe/dias/2001/07/21/pdfs/A26552-26603.pdf. Article 60 lists the actions that may be inscribed in the Foreign Registry Office

EX1 On rights and liberties of foreigners in Spain and their social integration, modified "Ley Orgánica 8/2000, de 22 de diciembre, de reforma de la Ley Orgánica 4/2000, de 11 de enero, sobre derechos y libertades de los extranjeros en España y su integración social."; http://noticias.juridicas.com/base_datos/Admin/lo8-2000.html.

certificates (so called "certificado reconocido"), based on a PKI solution. Such electronic certificates are issued by the FNMT and others, for purposes of tax declarations. Another example of this type of certificate is the idCAT, that can be issued to foreign citizens This is a qualified certificate based on software issued by CATCert that can be used for different kinds of procedures within the public administrations.

More information on regulations about non-nationals can be obtained at Interior Ministry http://www.mir.es/SGACAVT/extranje/normativa_basica.html

Entrepreneurs / Corporations

In Spain, establishing a company requires the granting of a public statement witnessed by a Notary, which determines the moment of its constitution, and therefore, its capacity to operate legally in trade.[302] Afterwards, its inscription in the Companies Registry[303] is mandatory and after having paid the respective taxes, the company should obtain a Tax Identification Number (called "Código de Identificación Fiscal", commonly known as "CIF", similar to the VAT no.), with identifying nature. At this moment, after being registered this way, companies are from that moment ***legal persons***

The purpose of the Companies Registry is to obtain full security and transparency in mercantile business, so that it is possible to know the legal situation of entrepreneurs. In this file, both individual entrepreneurs and society companies (mostly Limited and Anonymous Societies) are inscribed. It is a public registry and therefore, it may be consulted by citizens or individual entrepreneurs interested in any information relating to the situation of a company: its partners, managers or legal representatives, bylaws, etc.

- Concerning individual entrepreneurs, the entrepreneur's identity and his company and the ***general powers granted*** to specific persons to act on behalf of the company are inscribed, as well as their modification, annulations and substitution. Sometimes other details regarding transactions are inscribed.
- In the case of companies, the incorporation, designation and termination of administrators/managers, liquidators and auditors, general powers and delegation of faculties must be inscribed, as well as their modification, revocation and substitution.

Concerning the authorisation and delegation processes, at present in Spain there is no specific generalised formal policy or infrastructure yet. However, there are certain cases where this delegation is formalised, such as the one developed and used for the presentation and on-line payment of taxes. Indeed, the Tax Agency recognises certain persons called “collaborators”[304], who may belong to other public administrations or private entities, institutions or organisations that represent specific sectors or social, labours, entrepreneurs or professional interests. This collaboration fundamentally refers to the following aspects: simplification in the fulfilment of taxing obligations, assistance and verification of correct tax declaration. The collaboration also includes, after authorisation by the represented persons, to electronically present to the Tax Administration tax declarations, communications or any other document with taxing transcendence, correction of errors, information on the status of the procedures for returns and reimbursements, and requests and obtainment of tax certificates.

[302] Declarations on census of entrepreneurs and professionals “Real Decreto 1041/1990, de 27 de julio, por el cual se regulan las declaraciones censales que han de presentar a efectos fiscales los empresarios, los profesionales y otros obligados tributarios. (Vigente hasta el 1 de septiembre de 2003)”; http://noticias.juridicas.com/base_datos/Derogadas/r2-rd1041- 1990.html.

[303] Rules for Companies Registries “Real Decreto 1784/1996, de 19 de julio, por el que se aprueba el Reglamento del Registro Mercantil.”; http://noticias.juridicas.com/base_datos/Privado/rd1784- 1996.html.

[304] “Orden HAC/1181/2003, de 12 de mayo, por la que se establecen normas específicas sobre el uso de la firma electrónica en las relaciones tributarias por medios electrónicos, informáticos y telemáticos con la Agencia Estatal de Administración Tributaria.”; http://noticias.juridicas.com/base_datos/Admin/o1181-2003-hac.html.

In order to act on behalf of third parties with their own certificate, a collaborator requires a specific authorisation from the citizen, who may grant it by personally appearing at the Tax Agency offices, or by means of a public or private document.

Certificates issued for representatives of companies require the inclusion of more data, like the company represented and a new extension[305] with a unique OID, established by IANA for the Spanish Tax Agency.

The LFE allows Administrations and CSPs to include some additional requirements on the certificates extension, which do not affect interoperability. Thus, this type of certificates, its extensions, and how data is stored is going to be standardised and endorsed with the development of the “Additional Conditions” foreseen in the law.

The DNIe will not be able to certify companies and persons in relation to their role in the company. Camerfirma, a subsidiary of the Chamber of commerce, acts as a CSP for companies, issues certificates that identify natural and legal persons, allowing them to access to online applications and public administrations services, as well as electronic signatures.

Although this certificate validity is for 2 years, it is important to mention that the maximum period of validity allowed by LFE for qualified certificates is 4 years. This type of certificate is normally emitted on software or smartcards, and will be able to certify companies’ managers on the following points:

- Ownership of the company
- Representation
- As legal Person
- Electronic invoicing

In addition to legal person certificates, Public Administrations will have to admit the electronic certificates issued to ***entities without legal personality***, as foreseen in LFE, in the terms that will be determined later on.

15.3 Principal legislation and policy documents

Legislation Framework

The Electronic Administration is having its biggest impulse in the last years, motivated partly by a legal framework that had taken the real world’s legal guarantees into the virtual one and by the evolution of the related technologies and the development of leading projects like the DNIe. The most interesting, in this sense, is the LFE that settles down, among many other things, the concept of advanced and recognised (qualified) signatures, being the last one endowed full legal validity for the public and private electronic transactions.

On the other hand, the LOPD (Law for Protection of Personal Data) and its recently developed regulation guarantee the security and confidentiality of the personal data provided by citizens in these transactions.

Lastly it is necessary to mention, and in a very outstanding place, the recent LAECSP (Law for Electronic access of the citizens to Public Services) that established the citizens' right to access any public administration using electronic means.

It is worth mention a very important change on the evolution from traditional DNI card to DNIe refers to its *identification quality effects* as is recognised on article 15.2 of LFE.[306] Now, it attests the iden-

[305] ESI “Electronic Signatures and Infrastructures (ESI); Requirements for role and attribute certificates ETSI TR 102 044 V1.1.1 (2002-12)”; http://portal.etsi.org/docbox/EC_Files/EC_Files/tr_102044v010101p.pdf.

tity, physical and electronic, towards all (“erga omnes”), not only to public administrations. Therefore, it obliges third parties to recognise electronic signature made with it.

The current legal Framework is shown below. It has references that spread through the text.

- **LAECSP**: Ley Para el Acceso Electrónico de los Ciudadanos a los Servicios Públicos. BOE 23-06-07 http://www.map.es/iniciativas/mejora_de_la_administracion_general_del_estado/moderniza/Administracion_Electronica/parrafo/05/document_es/A27150-27166.pdf.

  The LAECSP Law of Electronic Access of the Citizens to the Public Services promotes the use of Information Technologies and Communications in the relationships between Public Administrations and citizens, thus improving the services and reducing the digital breach.

- **DNIe:** Royal Decree 1553/2005, of December 23, ruling the national identity card and its eSignature certificates. http://www.dnielectronico.es/marco_legal/RD_1553_2005.html

  It regulates the expedition of the National Document of Identity and their electronic certificates for authentication and signature.

- **LFE.** “Ley 59/2003, de 19 de diciembre, de firma electrónica.” http://noticias.juridicas.com/base_datos/Admin/l59-2003.html.

  The LFE signature law affects Identity providers which reside in Spain or that gives services from abroad, but has a permanent establishment in Spain, which implies being registered at Companies Registries.

- **LOPD** “Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.”; http://noticias.juridicas.com/base_datos/Admin/lo15-1999.html.

  This Law established the conditions derive from the Directive 95/46/EC - The Data Protection Directive.

- **REGLAMENTO LOPD:** Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.”; http://noticias.juridicas.com/base_datos/Admin/rd1720-2007.html.

  This Decree develops rules for the implementation of the LOPD and defines security level and measures that a service provider must establish in order to protect data.

Additionally, although it is not a law, we must mention the following initiative document that establishes the validation practice of the central multiPKI signature and certificate validation platform.

- **@FIRMA:** “Declaración de prácticas de Validación @firma”; http://www.dnielectronico.es/seccion_aapp/FirmaV5p0_DPV_F20080526_V8_3.pdf.

  It is a national Validation Platform, focused on the creation of interoperability between the existing and future CSPs. It provides freely eSignature and eCertificate validation services to eGovernment applications: It binds the authentication services of the DNIe card and other public and commercial PKI certificates together, allowing application owners to use both identification solutions. Currently there are about 180 available services using the platform.

Although we cannot consider, in a strict sense, LISI, a law affecting directly to this legal framework because it points more directly to private sectors, it will have future effects on it; because it focus on eliminating the breach among Autonomous Communities as well as diminishing digital differences in the Information Society with Europe. So, it is would be expected a high increase on demanding trans-border services by the citizens.

[306] LFE. “Ley 59/2003, de 19 de diciembre, de firma electrónica.”; http://noticias.juridicas.com/base_datos/Admin/l59-2003.html.

- **LISI:“**Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información.”; http://noticias.juridicas.com/base_datos/Admin/l56-2007.html.

  This law strengthens two aspects of the Information Society. On one hand, it establishes the citizen’s right to interact online with companies from different sectors: financial, energy, telecommunications, transport etc.; this right means an obligation for these companies to adapt their ICT systems, so their clients authenticate themselves with qualified certificates and can carry out some procedures with juridical validity using electronic signatures. Thus this project is an opportunity for those companies, to allow not only some certificates, but all EU identifications.

  On the other hand this law foresees a procedure, within the European Community, for collaboration between member states to regulate the adoption of restriction measures regarding services, according to paragraph a) of part 4 of article 3 of the Directive 2000/31/CE, coming from countries of the European Economic Space. This could help on the implementation of a common cross-border procedure for incident and incidences handling as suggested further below.

DNIe

As mentioned in article 1 DNIe-law using DNIe card has ***identification quality effects*** as is also recognised on LFE because it attests physical and electronic identity to anyone (“erga omnes”), not only to public administrations. The DNie allows ***proving signatory's identity***, the holder's ***data*** and the integrity of the documents signed with electronics signature devices, thus, equalling the electronic signature to the hand-written one.

The personal identification number known as DNI number, is composed of nine digits and a checksum. This number is used in other documents granted by the Administration such as the passport or the drivers licence. Many applications use this number as a primary key to identify persons.

The chip of the smartcard contains two types of certificates (X.509v3): the authentication certificate and the signature certificate with legally defined data contained in them. If there is a ***necessity for more data***, they might be collected from ***other attribute sources*** taking into account legal restrictions.

Also, the DNIe regulation indicates the possibility of interchanging data required for the expedition of the DNIe among administrations in charge of this process. For example, this allows taking data from the census of the city councils without requiring the citizen to present a valid document.

If DNIe usage for digital signature requires the public or private authority that issued it (Police VA), to maintain a history of data related to the certificate in its information systems for 15 years after expedition. This implies that digital signatures created with Spanish qualified certificates can be validated during this period. To avoid any misuse of this information, LFE had taken into account the Spanish data protection act LOPD and a public file has been created, of which data may only be gathered directly from people or with their prior consent.[307]

LOPD

This regulation is **applicable to data of natural persons** and is not applicable to the treatments of data referred to legal persons. The data to be treated should be accurate, pertinent and not excessive to the explicit and legitimate purposes for which these data have been obtained or recollected.

This requires ***previous consent by the person to gather their data***, except when collected by some Public Administration process to fulfil other legislation, when there is a contractual relationship be-

[307] La Firma electrónica. Aspectos legales y técnicos Autor(es) Raúl Rubio Velázquez, Carlos Rodríguez Sau y Ramiro Muñoz Muñoz, Ediciones Experiencia, julio 2004,

tween the person and a third party, or when the data are needed to protect a vital interest of the person. Exceptions are highlighted on LOPD article 34 and on further works on Binding Corporate Rules. (article 29 Data Protection Working Group).

Likewise, the data will be ***stored during*** the time in that some type of ***responsibility can be demanded*** deriving from a relationship, a juridical constraint or obligation, the holding of a contract or the application of pre-contractual measures requested by the interested person.

When a person needs to verify or report his/her data and they are already registered by any public administration, the application is allowed to check his name and family name, as well as his current address in order to verify their authenticity.[308]

As Stork is currently being developed in the European Economic Space (EES) it is presumed that ***restrictions to international data transfer are not applicable***. We should consider these restrictions if data are sent out of the European Economic Space by means of a data communication, a cession, or data are to be processing or treated on behalf of the controller.

If data is processed or treated in Spain, the owner of the file will have to designate a representative settled down in Spanish territory.

It seems reasonable that each participating member state should review their respective legislations, because as indicated in the Article 90 of LOPD for any ***incident, notification and administration procedures should exist***, and any incidences, that may affect the personal data, must be registered. Therefore, it is possible that the implementation the STORK project will be affected when data from Spain suffer some incident in say, UK. Thus, cross-countries incidences must raise and the owners of the systems/files from the affected countries need to be aware. This **international incident handling procedure** must be agreed on by all participating MS.

What can also affect the Spanish partners in the pilots is that, as stated on Article 93 and 98, it is necessary to establish the security ***measures for unequivocally Identifying a person*** and his/her authentication (application users profiles). Depending on the security level, several mechanisms and process must be in place, that guarantee confidentiality and integrity for delivering credentials distribution procedure, limiting reiterated unauthorized system attempts. This is of course also applicable to them without Stork

LFE

The LFE signature law affects Certificate Services Providers which reside in Spain or that offer services from abroad, but has a permanent establishment in Spain, which implies being registered at Companies Registries. From a juridical point of view LFE talk about two kinds of certificates: qualified or not qualified and three types of electronic signatures: simple, advanced and qualified.

The LFE, in its section 3 determines the necessity to develop a national framework for digital signatures with additional conditions. These conditions should be "objective, proportional, transparent and not discriminatory and they may not block the benefit of certification services to the citizens when different national or EES public Administrations are involved. *These* ***conditions*** *should be applied with a global view* ***for certificates,*** *as well the ones that exist already as the new ones that may arise*.

[308] "ORDEN PRE/4008/2006, de 27 de diciembre, por la que se establece la configuración, características, requisitos y procedimientos de acceso al Sistema de Verificación de Datos de Residencia"; http://www.csi.map.es/csi/pg2004.htm.

"ORDEN PRE/3949/2006, relativa al Sistema de Verificación de Datos de Identidad"; http://www.csi.map.es/csi/pg2002.htm.

The authentication concept versus signers' identification managed by LFE could embrace both the ***authentication of the person and the authentication of data***; rendering this way a wider amplitude to the definition offered by the EC directive.

The LFE settles down in its article 11 the identity ***information*** that should ***be stored in qualified certificates***: the signatory's identification, for natural persons is made using their name and last names and their ***number of DNI***, or through an alias that can be set unequivocally; for legal persons, their denomination or corporate name and their Tax identification number. However, there is ***no definition for a normalized structure of data to store this information***. Thus, no ***common method of extraction*** of the identity information ***exists,*** neither exact rules that allow decomposing this information in its concrete elements.

The LFE requires physical presence for issuing qualified certificates but it is not required when:

- the signature in the application form has been witnessed by notaries.
- the identity and other circumstances of the applicant are known by CSP due to a pre-existing relationship. E.g. this could be presenting a DNIe.
- When a new certificate requests is made by presenting a valid one issued to the subscriber in accordance to the identification requirements established by law. The CSP has to confirm that the time passed after the identification is not longer than 5 years.

Qualified certificates, also require:

- The indication that has been issued as qualified.
- A unique identifier.
- Name of the CSP's that issues the certificate and its address.
- CSP's advanced electronic signature.
- Check people identity and circumstances (i.e.: people representing a company)
- Verifying that all the information on the certificate is accurate and mandatory
- Making sure that the signer possesses all data for signature creation and that those data correspond to the ones on the certificate
- To indicate the validity period.
- To indicate its limits and the limit on the amount of the transactions that can be made, if these limitations exist.

LFE provides three assurance levels:

- Simple Electronic Signature Assurance Level 2: Normally passwords used by closed groups of users.
- Advanced Electronic Signature Assurance Level 3: Based on qualified Certificates.
- Recognised Electronic Signature Assurance Level 4: Based on qualified Certificate on a Secure Signature Creation Device (SSCD).

Additional Conditions

Both LFE and LAECSP respect the legal authority of Public Administrations. So, this can render technically incompatible certificate services, that can raise problems for free recognition of electronic signature certificates. In order to avoid this, the "additional conditions", mentioned in both laws, develop and implement a general reference Framework as a strategy for identification and authentication among different authorities, which is called "Politica de firma y certificados". This framework is supposed to help in the development of a general consensus about the national schema for security and interoperability "Esquema Nacional de Interoperabilidad y el de Seguridad" among credentials and services implementations.

It is a framework schema for the application of identification systems and authentication foreseen in LAECSP, as well as to the ***additional conditions*** of the application of the electronic signature in the environment of the public Administrations, as it is established in article 4 of LFE.

They establish the basic aspects of interoperability of certificates and of representation using them as means for the identification, although from the law, others methods can be inferred like the secure *codes of verification*.

These additional conditions need to establish the following:

- **Conditions for the Certification Services Providers**: Organisational dispositions related to the services and their security. Basic characteristic and functionalities offered by the services for issuing and state confirmation of the certificates emitted by the CSP.

- **Condition for the Electronic Certificates:** dispositions related to the offered services and the semantics peculiarities of the certificates that establish their necessary characteristics when configuring the emitting certificates profiles.

- **Admission Schema for Certification Services Providers:**
  - Acting protocol for the admission of certificates: Mutually agreed by the MAP and MITyC according to the mechanisms to settle down in the Schema of Identification and electronic Signature. Inspection and control (Politica de firma y certificados. Inspección y control)
  - General and authorising conditions for requesting admission for new CSPs/certificates
  - Notification of the additional general conditions to the European Commission
  - A model in which an admitted CSP don't have to sign any previous agreement

LAECSP

The LAECSP Law of Electronic Access of the Citizens to the Public Services promotes the use of Information Technologies and Communications in the relationships among Public Administrations and citizens, thus improving the services and reducing the digital gap breach.

The LAECSP references through all its extension that the systems, the data, the communications and services, which are operated by Public Administrations should fulfil the guarantees of security, confidentiality, integrity, etc. Especially, it stresses several direct ***references to the LOPD***.

In their Second Chapter, it regulates the way of identification, authentication and electronic signature, both for citizens and Administrations. It also enables ***DNIe as general means for relationships*** between citizens and Public Administrations; but, also admits the existence of other recognised electronic certificates systems that must be accepted and recognised by any Public Administration in accordance with LFE on articles 15 and 21. Also, these alternative electronic signature systems might use previously registered concerted keys, shared secrets, or other non cryptographic systems, under the terms and conditions that are determined in each case (usually automated administrative processes). This means that there would be coexistence of strong authentication with authentication by knowledge mechanisms like userid / password.
It is evident that this law creates a multilevel legal framework for electronic identity and digital signature in relations among citizens and public administrations, and among several administrations. If advanced signatures are used instead of the recognised one, then the public body need to inform about

the admitted advanced signature systems. That means that a public administration can choose to ask for a simple electronic signature (for example a password) or an advanced electronic signature.
Article 23 enables a person ***acting as a representative*** for a natural or legal person by means of specific conditions.
In addition, Article 15.3 of the LAECSP settles down that the Public Administrations will admit the electronic ***certificates issued to entities without legal personality***, as foreseen in LFE, in the terms that will be determined in future regulations.
At the moment, various types of digital certificates exist (DNIe, Civil servants certificate, public administrations certificate, etc) and there is no definition for a normalised structure of data to store this information. Thus, no common method of extraction of the identity information exists, neither exact rules that allow decomposing this information in its concrete elements. But, as foreseen by Law, these Qualified Certificates can include some additional requirements on their extension while not affecting their interoperability. Thus, this type of certificates, its extensions and how data is stored, is going to be standardised and endorsed with the development of the “Additional Conditions”.

Policy:

There are currently various initiatives and projects to develop a common policy to improve the performance of the eGovernment services .

PLAN AVANZA (Go Ahead Plan)

Plan Avanza, approved on November 2005, is part of the strategic axis for boosting the R+D+I (Research, Development & Innovation) that the Government has put in operation through the Program Genius 2010.

The purpose of the Plan Avanza is to get the appropriate use of the ICT to contribute to the success of a model for economic growth based on raising competitiveness, productivity, and promotion of the social and regional equality and the improvement of the social welfare quality of the citizens' life.

The plan considers four big acting areas:

Digital citizenship whose objectives are:

- To increase the proportion of equipped homes and its daily use of ICT.
- To increase the knowledge of the benefits of ICT among the citizens, as well as the proportion of people that use the ICT in their daily life.

Digital economy that pursues:

- To increase the grade of adoption of the ITC on Small & Medium Enterprises –SME– (PYMES) for example adopting the electronic invoice.
- Raise the percentage of connected companies to the broadband.

Digital Public services whose goals are:

- A totally developed Electronic Administration.
- Guarantee citizens and companies rights for interacting electronically with the Public Administrations.
- To transform education based on traditional models to one founded Information Society.

Digital context that seeks:

- To extend telecommunications infrastructures in demand disregarded areas.
- To extend the use of Broadband connections and mobility.
- To raise public awareness and knowledge in citizens, companies and Public Administrations, regarding ICTs security .

- To boost digital identity.

PLAN CONECTA (Connect Plan)

The “Plan Conecta” aimed at the stimulation of Government technological modernisation, in order to construct the “European Information Society”. It wants to centre the attention putting a special emphasis on growing citizen’s demands towards the administrations services.

It also pretends to connect administrations and persons by means of a modernisation plan with five big metaprojects:

- **Certifica**: Substitution of 80% of the paper certificates required by administration by secure data interchange
- **eDNI**: A new DNI that allows us to authenticate in the Network
- **ciudadano.es:** A Web Portal for direct contact between citizen and administration
- **Simplific**a: Simplification of procedures and times to connect administrations and attend citizen’s demands
- **MAP en red:** Program of Excellence in the Public Administration Ministery to improve the relationship between civil servants and citizens

DNIe Protection Profiles

For DNIe there are four Protection Profiles being elaborated for digital signature creation and verification applications, using the DNIe as sure secure signature creation device for the use in eGovernment applications. These profiles will be recommendations and not of obliged fulfilment

The Protection profiles of the DNIe are based on the Common Criteria standard and their description contains:

- the safety problem in a normalised form
- the objectives for development to solve the security problem, and the relation with this problem
- the specifications that will have to be fulfilled to meet the objectives

The DNIe is, according to these profiles, level EAL4+ compliant.

15.4 eID model

The Spanish law foresees a model of two types of electronic identification:

1. **DNIe** a SSCD cryptographic smartcard for natural persons that have two qualified certificates that need to be used in a segregated manner by the applications. Spanish legislation grants that the use of the DNIe must be recognised by public administrations and, in the case of economical services, companies. It has proposed assurance level 4.
2. **Qualified certificates** issued by authorised CSPs based on PKI. They can be supported on different types of tokens: software, smartcards, crypto-cards. This can be used by anyone: natural persons, legal person o persons without legal entity. The assurance level for these credentials varies between proposed level 3 and 4.

15.5 Analysis

In this chapter we are going to describe only as Spanish eID: the DNIe, though we cannot forget that there are actually 15 CSP that can provide **another valid authentication mechanisms**, some of then ***cannot be done by the DNIe***.

eIDentity: DNIe

As stated before, today in Spain, two types of authentication mechanisms are being used that are usable in international context: the national DNIe card and other electronic certificates, based on a PKI infrastructure. At present, there is no difference between the on-line services offered for both types of authentication systems, although it is true that as an official identity method before authorities, only the DNIe card is valid. This means that the DNIe must be accepted by eGovernment administrations; other certificates may be accepted.

The existing ***DNIe token*** in Spain is the electronic national identity card “DNI electrónico” or “DNIe” that is a ***customised SSCD cryptographic smartcard, common criteria certified EAL4+,*** whose uses and contents are regulated by law [2]. To generate this DNIe card, a person needs to be physically present at an office of the Police General Directorate where the DNIe is issued with a combination of identifiers:

- The card itself contains a general personal identification number known as DNI number (also known as NIF when added a code letter). This number is evidenced in other documents granted by the Administration such as the passport or the drivers licence. It is commonly used . The ***DNIe certificates are obliged to contain this number***
- The chip of the document contains two types of certificates (X.509 v3): the authentication certificate and the signature certificate. These certificates are generated and granted according to legal specifications.[309]

The DNIe card ***distinguishes*** between ***signature and identity functionality*** thus, ***their usage is segregated*** because it serves to electronically and undoubtedly verify the identity of the person, as well as to eSign documents with a legal value equal to the handwritten signature.

Name

Electronic national identity card (Documento Nacional de Identidad electrónico): DNIe

Form

The DNIe card uses contact ICs, with ISO 7816-3 compatible access and with an EEPROM size of 34 Kb for data. The electronic Chip models are st19wl34 y ICC ST19wl34 with a proprietary OS DNIe v1.1.

The cards itself used for the national DNIe use the standard PKCS#15 and follows these other standards: ETSI TS 102 042, ETSI TS 101 456, ETSI TS 101 862, CWA 14167, CWA 14172, CWA 14.890. As a smartcard, follow the standards PKCS#11, CSP and API PC/SC.

The electronic certificate on the card used by the DNIe card and by other smart cards includes cryptographic capacities though ***there is no a certificate for encryption***.

The hierarchy concerning the PKI of the national DNIe card consists of a two-layered model:

- A first level where the Root CA (“AC Raíz”) is located, representing a confidence key point for all the system. This way, all natural, corporate, public or private persons will recognise the effectiveness of the DNIe card for vouching the identity. This AC only issues certificates for itself and its AC Subordinates. It will only be operating during the realisation of operations for which it is established and the dependant Police General Directorate exercises these functions.
- A second level constituted by the CA subordinated to the Root CA (“AC Subordinada”) that will issue the identification and signing certificates included in the DNIe card.

[309] E-SIGN DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 1999 on a Community framework for electronic signatures http://europa.eu.int/information_society/eeurope/i2010/docs/esignatures/esignatures_en.pdf And the (eSignature) Ley 59/2003, de 19 de diciembre, de firma electrónica. http://www.mityc.es/NR/rdonlyres/62297ED5-20DF-426B-B2DD-9A76996527A0/0/15LEY59_2003.pdf

The description of the fields of the signature certificate is contained in the table below. Please not that in the Spanish case there is a difference between the ***Citizen Signature Certificate (CSC)*** and the ***Citizen Authentication Certificate (CAC).*** As their technical description is almost the same, differences are directly highlighted along the table. Also, note that this table refers only to DNIe though in Spain others types of certificates exist.

e-ID Citizen Signature Certificate / Citizen Authentication Certificate					
Base Certificate	**OID**	**Include**	**Critical**	**Value**	
Certificate					
SignatureAlgorithm					
Algorithm		X		SHA256 with RSA Encryption SHA1 with RSA Encryption	Fixed
SignatureValue		X		Issuing CA Signature	
TBSCertificate					
Version		X		Standard X.509 v3	
SerialNumber		X		Not sequential	dynamic
Signature		X		SHA1 with RSA Encryption *(note: SHA256 with RSA Encryption is foreseen for citizen certificates by 2009.)*	
Validity					
NotBefore		X		Key Generation Process Date/Time	
NotAfter		X		Key Generation Process Date/Time + 30 months	
SubjectPublicKeyInfo		X		RSA Encryption – Key length: 2048 bits	
Issuer					
CountryName	{id-at-6 }	X		ES	Fixed
CommonName	{id-at-3 }	X		CA DNIE XXX *(note: XXX= number that identifies the issuer CA)*	Fixed
Organization		X		Dirección General de la Policía	Fixed
Organizational Unit		X		DNIE	Fixed
Subject			**Required**		
CountryName	{id-at-6 }	X	YES	ES	Fixed
CommonName	{id-at-3 }	YES		**CSC:** 1st Surname 2nd Surname, GivenName (signature) **CAC:** 1st Surname 2nd Surname, GivenName (authentication)	Dynamic
Surname	{id-at-4 }	X	YES	provided by RRN	Dynamic
GivenName	{ id-at-42 }	X	YES	provided by RRN	Dynamic
SerialNumber	{ id-at-5 }	X	YES	Citizen ID number, including letter *(Note: The letter is a control digit used in Spain to avoid transcription errors.)*	Dynamic
Standard Extension	**OID**	**Include**	**Critical**	**Value**	
Certificate Policies	**{id-ce 32}**	**X**	**FALSE**	**N/a**	
PolicyIdentifier		X		CSC: 2.16.724.1.2.2.2.3 CAC: 2.16.724.1.2.2.2.4.	Fixed

PolicyQualifierrs					
PolicyQualifierId	{ id-qt-1 }				
Qualifier		X		http://www.dnielectronico.es/dpc	Fixed
Qualified Certificate Statement					
qcStatement	{id-etsi-qcs 1 }	X		id-etsi-qcs-QcCompliance id-etsi-qcs-QcSSCD	
Key Usage	**{id-e 15}**	**X**	**TRUE**	**N/A**	
Digital Signature		X	TRUE	**CSC** : 0 **CAC** : 1	
NonRepudiation (Content Commitment)		X	TRUE	**CSC** : 1 **CAC**: 0	
Key Encipherment		X	TRUE	0	
Data Encipherment		X	TRUE	0	
Key Agreement		X	TRUE	0	
Key Certificate Signature		X	TRUE	0	
CRL Signature		X	TRUE	0	
Key Identifiers	**{id-ce 35}**	**X**	**FALSE**		
AuthorityKeyIdentifier		X	FALSE	Application of SHA-1 Hash on CA PKI	
Subject Key Identifier		X	FALSE	Application of SHA-1 Hash on Subject PKI	
CRLDistributionsPoints	**{id-ce 31}**	**X**	**FALSE**		
DistributionPoint			FALSE	It will not be used	
FullName					
Netscape CertType					
Subject Info		**X**			
Biometric info		X	FALSE	Hash of biometric data SHA256/SHA1	
Personal data info	2.16.724.1.2.2.3.1 .	X		Hash of biographic data (printed data on eID card) SHA256/SHA1	
Subject Directory attributes		X		Date of Birth	
Private Extension	**OID**	**Include**	**Critical**	**Value**	
AuthorityInfoAccess	**{id-pe 1}**	**X**	**FALSE**		
accessMethod	{id-ad-2 }				
accessLocation		X		OCSP http://ocsp.dnie.es Root CA http://www.dnie.es/certs/Acraiz.crt	
accessMethod	{ id-ad-1 }				
accessLocation					

Table 7: Description fields for (CSC) and (CAC).

Eligibility

DNIe is granted to all nationals and is compulsory for all Spaniards above 14 years old.

In Spain, the procedure for citizens to obtain their national DNIe card is summarised in two steps:

Physical Phase: physical personalisation of the card and documentary presentation

1. The citizen who requests his DNIe card for the first time and thereby, the associated electronic certificates, must be present into a Police Office to obtain DNIe card an will be indispensable to present the required documents: birth certificate, photo, census certificate
2. The delivery of the ID card and of the associated certificates will be done personally to its bearer on the very moment he requests its issuance.

Logical Phase: logical personalisation of the chip

1. In the presence of the bearer, the officer charge data on the chip of the support card: codes generation on the card and after, the qualification of a random PIN delivered in a closed envelope.
2. Afterwards, the citizen may change his PIN number for added security. After having obtained the DNIe card, the citizen may use the Administration bodies' online services. Services.

The DNIe card will allow others CSP to issue certificates without requiring the physical presence of the petitioner, which will sensibly reduce their needs for infrastructures, as well as facilitating the procedures for citizens.

Issuer

General Directorate of the Police, at Police Stations.

Ministry of Public Administrations (MAP) helps in co-operation with others public administrations to the Police.

Responsible authority

Ministry of Interior (Ministry of Internal Affairs)

Attributes

The data attributes printed on card and stored in the chip is regulated by the DNIe Decree[310] and Citizen Security Protection Law[311]. The data organizes as follows:

On the front side:

- photograph and signature of the bearer,
- name(s), and surnames (the father's first surname followed by the mother's first surname),
- date of birth,
- gender,
- nationality,
- personal number (national register number or personal numerical identifier.) and verification character corresponding to the Identification Tax Number. The Tax Administration assigns a letter to each contributor that added to the personal number conforms the Tax Identity Number, a

[310] **DNIe** Royal Decree 1553/2005, of December 23, ruling the national identity card and its eSignature certificates. http://www.dnielectronico.es/marco_legal/RD_1553_2005.html

[311] Citizens Security Protection Law "Ley Orgánica 1/1992, de 21 de febrero, sobre Protección de la Seguridad Ciudadana."; http://noticias.juridicas.com/base_datos/Admin/lo1-1992.html.

number that must be consigned in all returns and communications that are presented or maintained to the Tax Administration.

On the back side,

- place of birth,
- province-region,
- parent’s name,
- residence,
- place of residence,
- region
- OCR-B letters for mechanical reading (OACI travelling document)

Also on the card, there is the expiration date of the document and the support card number. Language is Spanish and any other national language of the autonomous community where it is issued.

on the chip of the support card,

- Personal Details.
- Digitalized Photo Image.
- Digitalized Handwritten Image.
- Fingerprint template
- Qualified Certificates for authentication and signature
- Private and public key pair for both certificates..
- Issuing authority certificates.

On DNIe certificates, there are no extended data for exchanging additional information like occupation, studies degree etc. If an application or process, need to obtain them they might be requested from another service.

This is the case of the Identity and Residence Verification Systems (Sistemas de Verificación de Datos de Identidad y Datos de Residencia). These systems avoid the citizen to hand over photocopies of the DNI card[312] (Royal Decree 522/2006) and census certificate in a public procedure[313] (Royal Decree 523/2006) for data that the administration already have. These systems are regulated through specific Ministry Orders “ORDEN PRE/4008/2006”[314] and “ORDEN PRE/3949/2006”[315]. They are working online since 1 January 2007. In addition, LAESCP in its article 6.b stress on ***citizens’ rights not presenting previously given data***.

[312] “Supresión de la aportación de fotocopias de documentos de identidad RD_522_2006.pdf http://www.csi.map.es/csi/pdf/RD_522_2006.pdf.

[313] “Supresión de la aportación del padrón municipal RD_523_2006.pdf”; http://www.csi.map.es/csi/pdf/RD_523_2006.pdf.

[314] “ORDEN PRE/4008/2006, de 27 de diciembre, por la que se establece la configuración, características, requisitos y procedimientos de acceso al Sistema de Verificación de Datos de Residencia”; http://www.csi.map.es/csi/pg2004.htm.

[315] “ORDEN PRE/3949/2006, relativa al Sistema de Verificación de Datos de Identidad”; http://www.csi.map.es/csi/pg2002.htm.

Conditions for use

The National Document of Identity DNIe is a personal and non-transferable document emitted by the Ministry of the Interior. Therefore, from in its physical point of view it is an official public document and can be used whenever required according to law. Attending to their electronic capabilities, it is going to be commonly used among citizens and public bodies' online services.

The DNIe holder has to keep and preserve it and to exhibit it when asked to do so by the Authority or their Agents.

Creation and termination

DNIe has two validity aspects to consider:

Time validity for the DNI is as stated in RD 1553/2005[316]

a) Five years for people under thirty years.

b) Ten years between thirty and sixty.

c) Permanent over sixty.

The DNIe, or the Stored Certificates in the chip have an expiration date of thirty months after issuing or start of validity, but limited to the expiration of the card.

15.6 Authentication Authority

One of the other important phases of the Authentication process, is the moment where the claimant (citizen), uses the DNIe that he/she has obtained. This electronic authentication phase can be governed by regulation and contracts. For example, it can be legally confined who may authenticate himself in front of an AA, or which organisations may connect to the AA. Such requirements can be a ***barrier for cross-border authentication***.

As mentioned previously, for this purpose the MAP has established a validation authority called @firma, which is operational for all certificates to be included in the STORK project. It is a ***national Validation Platform***, focused on the creation of interoperability between the existing and future CSPs. It provides freely eSignature and eCertificate validation services to eGovernment application. Currently there are about 180 available services using the platform. It also binds the authentication services of Validation Authorities for the DNIe card and commercial PKI certificates together, allowing application owners to use both identification solutions.

Name

There are several Authorities that will ***validate*** the different certificates' current status by ***using OCSP or CRLs*** *mechanisms*:

For DNIe validation exist three, authorised by law[317], VA with defined roles

- **MAP** (Minstry of Public Administration). It Provides @firma Platform v.5.0 for validation services for overall Public Administration sectors.
- **MITYC** (Tourism and Industry Ministry) will provide services to small and medium enterprises (SME).

[316] **DNIe** Royal Decree 1553/2005, of December 23, ruling the national identity card and its eSignature certificates. http://www.dnielectronico.es/marco_legal/RD_1553_2005.html

[317] **DNIe** Royal Decree 1553/2005, of December 23, ruling the national identity card and its eSignature certificates. http://www.dnielectronico.es/marco_legal/RD_1553_2005.html

- **FNMT** (the Mint) It will be a universal VA for whole public and private sector: citizens, companies, public bodies etc.

For the validation of other certificates issued by authorised[318] CAs, there are other VAs

- **MAP @FIRMA:** In addition to DNIe validation for public Administrations mentioned before, it also validates public and commercial certificates issued by, both public and private, commercial CSPs which can be used in a large number of eGovernment (state, regional and local) applications for authentication services. In this way it guarantees the interoperability between these different kinds of certificates
- **CATCert** and other public and privates authorities have their own validation mechanisms.

It is worth noting that @firma also binds the authentication for all certificates to be included in the Stork project.

What

Here we briefly describe the @firma functioning. Full information is contained in the document[319] "Declaración de certificados de @firma" (Declaration on @firma certificates), issued on July 2008.

Certificates than can be used are determined by LFE and LAESCP and there is current work on developing technical additional conditions envisaged through them. According to LFE all CSPs will have a Certification Practice Statement to establish all procedures related to the life cycle of the certification activity (issuance, revocation, validation, etc). It cannot be considered as a law but it is an obligatory document that binds the CSP activity.

There are three groups of certificates, widely used by citizens/enterprises within their relation with public Administrations. They classify according to their nature: certificates related to natural persons, corporate persons or components.

- **Natural Persons (NP) Certificates**, directed to citizens or individuals as a way of eIdentification on the Internet, which allow the creation of recognised eSignatures.
- **Corporate Persons or entities (CP) certificates**, usually issued to the company's legal representative (or person empowered to Law on behalf of the company), recognised in many eGovernment applications for the signature of administrative procedures.
- **SW Certificates or components for coded SSL**, for machines or automated processes where online petitions or answers have to be eSigned; for the creation of safe channels for the data exchanging between the server and citizen (e.g. applications of online Registry). This type of certificate is not recognised yet (SW based certificates are free for citizens in most cases).

The currently working services that can be requested from @firma are:

Validation Service

- X.509v3 certificates validation through http, ftp, ldap, OCSP
- Obtaining certificate information
- Electronic signature with multiple formats: XMLDsig, XAdES, CMS, CADES, PDF, ODF
- Complete Block signature validation

[318] **LFE**. "Ley 59/2003, de 19 de diciembre, de firma electrónica."; http://noticias.juridicas.com/base_datos/Admin/l59-2003.html.

[319] **@firma:** "Declaración de practicas de Validación @firma"; http://www.dnielectronico.es/seccion_aapp/FirmaV5p0_DPV_F20080526_V8_3.pdf.

- Document Block signature validation
- Multi level certificates validation recognised for @firma
- OCSP responder
- Cache validation service
- Server Signature service
- Server Signature CoSign
- Server Signature CounterSign
- Signature and multi-signature on client files
- Non repudation elements custody

Responsible authority

The following entities take part in the management of the DNIe card:

- The Police General Directorate, as competent organ to issue and manage the DNIe card;
- The Authority approving the policies, as a PKI Executive Committee responsible for the elaboration and updating of the Declaration Draft about Certification and Practice Policies, as above mentioned; and the organ that will study the possibility of an external CA inter-acting with the PKI of the DNIe card or the provision of validation services by third parties.
- Certification Authorities (CA), as outlined below:
    - A Root CA that only issues certificates for itself and its subordinated CAs. Certifications of Root CA.
    - Three subordinated CAs that issue certificates for DNIe card holders. Certifications of subordinated CAs.
    - Registry Authorities: constituted by all offices that issue the national ID card, that will assist the CA in all proceedings related to citizens concerning their identification, registry or authentication, guaranteeing the correct assignment of keys to the applicant.
- Validation Authorities (VA): that will check the certificates' current status by using the Online Certificate Status Protocol (OCSP) or Certificate Revocation List (CRL) as mentioned above.
- Relying Party: any person or entity, different to the holder, which accepts and trust on the certificates contained in the DNIe card.

Input (looking for better term)

DNIe holder can change its identification key number at police stations or via Web.

When an applicant needs to be authenticated for an eGovernment service, the eGovernment service (relying party) will check @firma platform for validity

Output

Validity or Invalidity of the certificate.

For whom is the authentication Authority

As outlined above, in the Infrastructure of Public Key adopted for the electronic DNI, it has been segregated the functions of Validation Authority and Certification Authority, in order to ***isolate the validation of an electronic certificate versus the identity and data of the holder***.

These validation services are carried out based on Online Certificate Status Protocol (OCSP) and WEB services an client/server model where client sends a petition on the state of the certificate to the Authority of Validation, that after consulting its database it offers an answer.

Process

Presently in Spain, all Public Administrations offer eGovernment services that rely on users' certificates. The connection between a citizen and an entity (public or private) is established as follows:

1. The citizen makes a request for an authenticated security connection.
2. The Public Organism (or Private Entity) creates an authenticated message and sends it to the citizen.
3. The citizen verifies the validity of the service certificate offered.
4. The code for the session and its cipher is generated with the public key of the Public Organism (or Private Entity).
5. The message for the exchange of codes is constructed.
6. The citizen introduces the DNIe card in the reader and, with the electronic authentication certificate, validates the codes exchange message.
7. The private channel is established.
8. The Public Organism (or Private Entity) verifies the message to open the session.
9. The Public Organism (or Private Entity) verifies in the Validation Authority the validation status of the Citizen's Authentication Certificate.
10. A secure channel is established and the SSL tunnel is closed.

AS can be seen this outlined process of authentication between both parts requires the use of two certificates. On one hand, a Certificate from the Public Body (or Private Entity) that guarantees that the citizen is connecting with the proper body mentioned and not to another. A Certification Authority under the LFE framework must guarantee the veracity of this certificate. On the other hand, the citizen uses his own authentication certificate, in order to be identified before the organism (or Private Entity). In this manner, the Organism (or Private Entity) may determine the identity of the citizen to offer a personalised service. The Police General Directorate in the case of the DNIe card shall determine the veracity of this certificate.

Assurance level

The assurance level is provided by the broad spectrum of certificates that can be derived from LFE and LAECSP and, of course, by the segregation of use of the certificates and their keys.

- **DNIe**: It have a proposed assurance level 4.
- **Qualified** or **not qualified certificates** issued by authorized CSPs based on PKI. The assurance level for these credentials varies between proposed level 3 (qualified certificates) and 4 (qualified certificates on SSCD with segregated key usage) depending on their underlying support and the authorization process. A priori, not qualified certificates are not to be considered; but if so, they would range between levels 1 and 2.

Other

The DNIe card system is not based on Liberty alliance, WS Star, or SAML

The national DNIe card allows the biometric verification of the identity of its bearer although this function will only be available at controlled points of access. The system uses the fingerprint of the user for his identity, and to do so, it uses the Match on Card algorithm.

15.7 Conclusions

The Spanish law foresees mainly a model of two types of electronic identification ***DNIe*** and public and private *CSP Qualified Certificates*. Though, it there could be some others particular cases restricted to specific and limited conditions that are not going to be taken into account.

The ***DNIe***, a customized SSCD cryptographic smartcard, common criteria certified EAL4+**,** whose *usage is segregated* by means of two types of certificates (X.509 v3): authentication and signature ones. So, it *distinguishes* between *identity and signature functionality*

The first one has ***identification quality effects*** (authentication of the person) thus serving to electronically and undoubtedly verify the identity, ONLY, of the ***natural person***. The second one allows *proving signatory's identity*, the holder's *data* and the integrity of the documents signed (and the authentication of data); equalling the electronic signature to the hand-written one. Both are ***general means for relationships*** between citizens and Public Administrations and everyone else.

The ***DNIe*** card is unlocked by a ***personal identification number*** that is commonly used as authentication by knowledge mechanism in real and electronic world. The certificates contain specifically regulated data. In case it would be necessary to obtain additional data, they might be collected from the user himself or ***attribute providers;*** of course, taking into account legal restrictions.

Reflecting the segregated usage of the certificates, the underlying Public Key Infrastructure architecture adopted for the electronic DNI has separated the functions of Validation Authority and Certification Authority, in order to *isolate the validation of an electronic certificate versus the identity and data of the holder*.

The Stored Certificates in the ***DNIe*** chip have an expiration date of thirty months after issuing or start of validity, but limited to the expiration of the card.

The ***Qualified Certificates*** issued by public and private *CSPs have to* be accepted and recognised in identification procedures by any Public Administration according to the Law. They can be emitted to anyone: ***natural persons, legal person or persons without legal entity***, and for any other of the endorsed usage. It is worth mentioning that for ***legal persons*** and their ***general powers granted*** exist a necessity to verify this status accurately.

At the moment, various types of digital certificates exist and there is *no definition for a normalised structure of data to store this information*. Thus, no ***common method of extraction*** of the identity information ***exists,*** neither exact rules that allow decomposing this information in its concrete elements. But, as foreseen by Law, these *Qualified Certificates* can include some additional requirements on their extension while not affecting their interoperability. Thus, this type of certificates, its extensions and how data is stored, is going to be standardised and endorsed with the development of the "***Additional Conditions***".

In general there are several Authorities that will ***validate*** the different certificates' current status by ***using OCSP or CRLs***:

One of the other important phases of the Authentication process, is the moment where the claimant (citizen), uses the DNIe that he/she has obtained. This electronic authentication phase can be governed by regulation and contracts. For example, it can be legally confined who may authenticate himself in front of an AA, or which organizations may connect to the AA. Such requirements could be a ***barrier for cross-border authentication***.

Current DNI Law foresees *citizens' rights not presenting previously given data; thus raising the possibility of data interchange between administrations****.*** Because this regulation is **applicable natural person's data included in the DNI, it** requires ***previous person consent to gather them.*** These data will be *stored during* the time in that some type of *responsibility can be demanded****.***

In the STORK project scope ***no restrictions to international data transfer*** are expected, though a prior concern is that each participating member state should review their respective legislations, in order to articulate a **procedure** for ***incident and incidences notification handling*** that may affect the personal data. Therefore, it is possible that the implementation the STORK project will be affected when data from Spain suffer some incident in say, UK. Thus, cross-countries incidences must raise and the owners of the systems/files from the affected countries need to be aware.

Pilots, demonstrators or proof of concepts would have to take into account the application security *measures for unequivocally identifying a person (user)*

16 Country report: Sweden[320]

16.1 Structure of the Administration

Sweden is a constitutional monarchy, but the King has no political power. The political system is that of a parliamentary democracy. Legislative power is held by a unicameral parliament (Riksdagen). Executive power is held by the Government, headed by the Prime Minister and responsible to the Riksdag.[321]

The structure of the Swedish administrative system has three main entities: central ("Statliga myndigheter", 250), regional (County council "Landsting", 21) and local (Municipality "Kommun" 283) level. Apart from these entities, the Swedish public sector also comprises functional organs and institutions responsible for administering governmental tasks.

The bulk of public administration is at local level. The work of a municipality's county administrative board ("Kommunfullmäktig") is based on its role as central government representative in the region and coordinator for issues passed on to it by central government. Municipalities are the primary providers of government services; they are responsible for hundreds of services. Other main (e)government services are provided by the Swedish Tax Agency (Skatteverket), the National Board of Student Aid (Centrala studiestödsnämnden), Swedish Social Insurance Agency (Försäkringskassan), and Swedish Public Employment Service (Arbetsförmedlingen).

Formal identities are provided by the state and ID-cards are issued by the Swedish Police Service, employers and from next year also the Swedish Tax Agency. Official ID documents are: identity card, passport and National ID-card (Nationellt ID-kort). These documents are based on the information present in the National Population Registry. The information that may be registered in the population register includes, name, personal identity number and co-ordination number, place of birth, in Sweden or abroad, citizenship, civil status, spouse, children, parents, guardian(s) and adoption, address, property, parish and municipality in which you are registered, immigration to and emigration from Sweden, address abroad, death and place of burial. Dates of the information in the register, such as date of marriage, are also registered.

The method of defining and constructing an infrastructure of eIDs is based on procurements and has been successful during an initial phase; however Verva's judgement is that this will not be acceptable for future developments. Verva is the 'Administrative Development Agency' and is responsible for coordinating the development of Central Government in Sweden and is one of the Government's central advisory agencies. As the expert in the field of Public Administration development, the Agency intervenes in several key areas. In addition, the Swedish Government has given Verva the assignment to stimulate the use of new eServices and the use of the Swedish eID (*e-legitimation*).[322]

16.2 Debate (and history)

The eGovernment vision for Sweden is that of having "the world's simplest and most efficient e-Government and e-Governance that respect the citizens' right to good administration, encourage enterprising and attract competent civil servants". It makes the former vision of an 'Information Society for All' even more concrete.

A citizen-focused Public Administration must build on a close co-operation between the different Government authorities and levels of Government. In line with the 24/7 Agency concept, the provision

[320] Based on analysis by the TILT team complemented by a country report written by Arvid Welin.

[321] Factsheet - Sweden - Country Profile; epractice.eu, July 2008.

[322] Factsheet - Sweden - Actors; epractice.eu, July 2008.

of 24/7 services shall take place regardless of the division of responsibilities between Government Agencies or other public organisations.[323]

In Sweden, eGovernment has been on the policy agenda since the mid 90s.

The measures proposed for the Government to take during 2008 regarding eIDs include:

- authorise a more detailed investigation into the forms for statutory regulation of Swedish eID etc.
- authorise the setting up of a co-ordination function and commission it to commence the task of developing functions and services for public administration, including the transition from the current situation to the proposed solution, and
- establish that it will be possible to download the Swedish eID onto the chip in the national ID-card.

Regarding electronic identification by relying on Qualified Certificates, a common personal eID should be restricted to include basic identity information that is normally consistent over time. Information regarding different "roles" that users/citizens may have should instead be collected from attribute providers momentarily when the eID is verified (this is also related to the line of action of the STORK pilot). In our view324 the Qualified Certificate should include a minimum of information for cross-border purposes that would make it possible for each Member State to include information for national use.

Regarding authentic e-documents, it is not common practice in Sweden to base IT-solutions on documents, but on information. We acknowledge that there will probably be a need for e-documents for special purposes. It is still important that common and long term strategies for eGovernment development should focus on content (information) rather than format (documents).

Sweden is working on a strategy for different types of official eIDs.[325]

16.3 eID model

Sweden has been successful introducing eServices and eIDs based on public and market needs.

As of today the usage is 50/50 between the two sectors. The eIDs in production today support both PKI-based identification and signature and include support for revocation control.

The eID certificates can be either software based or smartcard based. There are three major IDP:s of eID for official certificates.

Sweden has approx. 1,5 million software based certificates and about 2 million card based certificates. All with the official certificate. One major IDPs provides the certificate on every credit card issued. This means that all 2 million card based certificates are not yet "actively used".

In 2007 there were no less than forty or fifty million eID-transactions registered for public, banking and private sectors eServices.

Approx. 25% of the transactions for public eServices concern eSignature. There are no such figures available for the banking and private sectors eServices.

[323] Factsheet - Sweden - Strategy; epractice.eu, July 2008.

[324] Country report Sweden by Arvid Welin, Sweden.

[325] Country report Sweden by Arvid Welin, Sweden.

16.4 Principal legislation and policy documents

Legislation:

The eIDs that are currently offered to individuals have been specified in connection with public procurements and there is consequently no statutorily regulated definition of them. There is therefore a need to introduce a system that is uniform, open and sustainable in the long-term for the eIDs that are to provide access to the administration's e-services. Verva therefore proposes that the terms *Swedish eID* and *Swedish corporate eID* are introduced and defined in the statute. A statutory regulation provides the necessary legitimacy and means that a Swedish eID can be protected and respected within Sweden and in relation with other countries. A Swedish eID must be available for all individuals that are entitled to a Swedish ID-document and who have a need to use public e-services in Sweden.

Fundamental requirements placed on the Swedish eID are that it must:

- be based on a regulation that defines current and future functional requirements,
- comprises functions for both electronic identification and electronic signature,
- be based on applicable European security standards, and
- be possible to use for e-services within the public sector as a whole and be open for application within the private sector. [326]

Swedish legislation does not stipulate any basic requirements for eIDs. The Act on Qualified Electronic Signatures (*Lag (2000:832) om kvalificerade elektroniska signaturer*) deals with electronic signatures in general and does not refer to eIDs specifically. The different regulations by authorities concerning the provided e-services refer in many cases to the use of an eID, but without defining the eID requirements.[327]

The reason for the lack of definition of the eID in Swedish laws and regulations is that the Swedish eIDs are commercial products that have been selected in a public procurement process. The requirements presented in this public procurement process represent the policy essence of the services and certificates used. The requirements were derived from, in principle, the CA-policy presented in ETSI TS 101 456.34.[328]

Swedish legislation does not make a literal translation of the e-signature definition in the European Directive. Rather, a Swedish electronic signature includes both authentication and integrity requirements. *Electronic signature* is defined as "data in electronic form attached to or logically associated with other electronic data, and used to verify that the content originates from the alleged issuer, and has not been altered." The definition thus includes not only the authentication aspect, but also an integrity requirement.[329]

EG-directives implemented in Sweden[330]

- Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free move-

[326] Country report Sweden by Arvid Welin, Sweden.

[327] IDABC interoperability for PEGS country report Sweden, November 2007, p. 16 and 17.

[328] IDABC interoperability for PEGS country report Sweden, November 2007, p. 16 and 17.

[329] IDABC preliminary Study on Mutual Recognition of Signatures for eGovernment applications, national profile Sweden, April 2007, p. 13.

[330] Country report Sweden by Arvid Welin, Sweden.

ment of such data (Dataskyddsdirektivet) – *Implemented in Sweden as Personuppgiftslagen (PuL), SFS 1998:204*

- Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures. The law applies to certificate providers established in Sweden and who issue qualified certificates to the public - *Implemented in Sweden as* Lag om kvalificerade elektroniska signaturer*, SFS 2000:832*
- Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market - *Implemented in Sweden as* Lag om elektronisk handel och andra informationssamhällets tjänster*, SFS 2002:562*
- Directive 2002/19/EC of the European Parliament and of the Council of 7 March 2002 on access to, and interconnection of, electronic communications networks and associated facilities - *Implemented in Sweden as* Lag om elektronisk kommunikation*, SFS 2003:389*
- Directive 2002/20/EC of the European Parliament and of the Council of 7 March 2002 on the authorisation of electronic communications networks and services - *Implemented in Sweden as* Lag om elektronisk kommunikation*, SFS 2003:389*
- Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services - *Implemented in Sweden as* Lag om elektronisk kommunikation*, SFS 2003:389*
- Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services - *Implemented in Sweden as* Lag om elektronisk kommunikation*, SFS 2003:389*
- Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector - *Implemented in Sweden as* Lag om elektronisk kommunikation*, SFS 2003:389*
- Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information (PSI) - *Implemented in Sweden as* Förordning om villkor vid vidareutnyttjande av information från statliga myndigheter*, SFS 2008:31*
- Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks
- Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on Services in the Internal Market (Tjänstedirektivet) – *Not implemented in Sweden, work in progress.*
- Directive 2007/2/EC of the European Parliament and of the Council of 14 March 2007 establishing an Infrastructure for Spatial Information in the European Community (INSPIRE) *– Not implemented in Sweden, work in progress.*

16.4.1 National legislation[331]

- SFS 1949:105 (Omtryck: SFS 2002:908), Tryckfrihetsförordningen (2 kap. om handlingsoffentlighet)
- SFS 1980:100, Sekretesslagen
- SFS 1990:782, Arkivlagen
- SFS 2003:770, Förordning om statliga myndigheters elektroniska informationsutbyte
- SFS 2005:661, Förordning om nationellt identitetskort
- SFS 1998:527, Lag om det statliga personadressregistret (SPAR)
- SFS 1998:1234, Förordning om det statliga personadressregistret

Other legislation

[331] Country report Sweden by Arvid Welin, Sweden.

- Government Ordinance on Qualified Electronic Signatures (*Sw:Förordning (2000:833) om kvalificerade electroniska signaturer*).
- Government Ordinance on the financing of the National Post and Telecom's operations (*Sw:Förordning (1999:836) om finansiering av Post- och telestyrelsens verksamhet).*
- Post and Telecom Agency's regulations on fees according to the Act on Qualified Electronic Signatures (*Sw: Post- och telestyrelsens föreskrifter om avgifter enligt lagen (000:832) om kvalificerade elektroniska signaturer; PTSFS 2002:1).*
- The Technical Conformity Assessment Act (*Sw: Lag (1992:1119) om teknisk kontroll*).
- The new Swedish Companies Act (SFS 2005:551) (*Aktiebolagslag (2005:551)*) that entered into force on 1 January 2006 explicitly mentions in Section 13 the signing of documents using an electronic signature. According to this Section any document that has to be signed may, if not otherwise stipulated, be signed with an advanced electronic signature as defined in the Swedish Act on Qualified Electronic Signatures.[332]
- The personal identity number is a unique identification number for Swedish citizens, appearing on the eID and its microchip. The legal framework for the issuing of the personal identity number is laid down in the Population Registration Act (SFS 1991:481) (Sw: Folkbokföringslag (1991:481)). Section 18 of the Population Registration Act stipulates that each person registered in the Swedish population registration system receives a personal identity number. [333]

16.4.2 Sectorial regulations:

In areas like human care, taxes, social services etc. there are specific regulations concerning IT-services and data storage.

Policy:

Verva considers that it is essential that the Swedish eID is given a stable basis and legitimacy with the aim of rapidly establishing it in society. This is best achieved by regulating the forms of Swedish eID in law. The necessary regulation should partly comprise an administrative system for issuing Swedish eID, partly an obligation on the part of the authorities to accept this ID for identification when their e-services are used.

Verva proposes that a co-ordination function is established in the form of an authority. The co-ordination function's task will be laid down in law and it will have its own regulatory powers within the area. The co-ordination function will supply technical services to affiliated authorities and manage relations with issuers in a way that is coherent for both the administration and the users.

The goal of a co-ordination function is that it will:

- link up with and further develop the currently established solutions,
- provide a uniform user interface in connection with e-authentication both for those who construct e-services and those who use them,
- be sufficiently versatile to meet new requirements in terms of issues concerning application and new technologies,
- be able to handle the two forms of eID and the two forms of certificate that are described above,
- be able to handle three classes (1-3) of security, and also

[332] IDABC interoperability for PEGS country report Sweden, November 2007, p. 16 and 17.

[333] IDABC interoperability for PEGS country report Sweden, November 2007, p. 16 and 17.

- be able to handle the different forms of attributes, roles and rights in conjunction with eIDs and certificates that will be required for new e-services within new areas.[334]

16.5 Analysis

The current PKI-based eIDs (‘e-legitimation’) are provided by private entities like banks and a telephone company. They support identification as well as signature using different key-pairs. Claimants that want an ‘e-legitimation’ apply for it or, more commonly, use their internet bank electronic security system to obtain it. A soft ‘e-legitimation’ (software certificate) can then be downloaded to the PC. Some of the eID-providers also distribute ‘e-legitimation’ with every issued Mastercard or Visa-card. Banks even provide their customers with a pinpad cardreader. For most electronic services these assurance levels are regarded sufficient. Qualified certificates are now being introduced in Sweden, but the usage has not yet been seen. However, ‘e-legitimation’ can be regarded to be an electronic Signature according to the 2004 Electronic Signature Act.[335]

On 1 October 2005, the Swedish Government introduced the ‘official’ electronic ID card containing biometric data. The new ‘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, and it is issued by the passport offices and manufactured by the same supplier as the biometric passport. In addition to the contact-less chip containing a digital picture of the holder, it also has a traditional chip which may be used to securely access eGovernment services in the future.[336]

Verva proposes eIDs to be issued in three classes:

Class 1 – soft eID

Advanced electronic signatures with encryption keys protected in encrypted software (data file). The security requirements should correspond to the European standard ETSI TS 102 042 NCP.[337]

Class 2 – hard eID

Advanced electronic signatures with encryption keys protected in hardware (microchip or equivalent). The security requirements should correspond to the European standard ETSI TS 102 042 NCP+.

Class 3 – qualified eID

Advanced electronic signatures are included as a requirement together with qualified certificates and secure arrangements for production of signatures in accordance with the Qualified Electronic Signatures Act in order to produce qualified electronic signatures in accordance with the Act’s definition. The security requirements should correspond to the European standard ETSI TS 101 456.

eIDentity: Soft eID's

e-legitimation = “eID” or “official eID” - represents the infrastructure used today, basic information of the person

The current PKI-based eIDs (‘e-legitimation’) are provided by private entities like banks and a telephone company. They support identification as well as signature using different key-pairs.

[334] Country report Sweden by Arvid Welin, Sweden.

[335] Country report Sweden by Arvid Welin, Sweden.

[336] Factsheet - Sweden - National Infrastructure; epractice.eu, July 2008.

[337] The European Telecommunications Standards Institute (ETSI).

BankID is an IT-infrastructure for electronic identification purposes that can be used by any bank fulfilling one of the following requirements: it must have a customer-identification process that guarantees the customer's identity, and it must provide some BankID-approved Internet security solution. At the moment 8 banks make use of this infrastructure. It has been used in the public sector by the National Tax Board and the National Social Insurance Board.

Steria has introduced the organisational certificates for personal use. This type of certificate contains the organisational number, the name of the organisation, as well as the name and the role of the person. It is worth noting that none of the organisational eIDs contain the personal identity number which is considered to be sensitive information.[338]

A remarkable initiative was the introduction of an open standard in June 2006 for the secure electronic identification by means of mobile devices. These systems will use the SIM card of a mobile phone and the mobile eID are mostly issued by Swedish banks. To further develop and maintain the mobile eID standard a non-profit association called WPKI was set up[339]

Form

Advanced electronic signatures with encryption keys protected in encrypted software (data file). The security requirements correspond to the European standard ETSI TS 102 042 NCP.

Issuer

The e-legitimation is issued by procured banks (one major bank as well as a co-operation of 9 other major banks) and the telephone company Telia in accordance with a policy in the procurement contract.

When public or private entities obtain the right to issue physical personal ID-cards, the e-legitimation can be down-loaded to and stored on the Company ID-card. It can then be used for identification and signature of the holder, not the company.

Nb. Qualified certificates are about to be introduced in Sweden by SignGuard Europe AB, having not yet come into use in the public eServices.[340]

eIDs are issued in two ways; by ordering and downloading it from the user’s Internet bank while being logged on (and thus identified by the bank), or by ordering the eID on the Internet. In the latter case the user will receive an activation code by registered mail which has to be collected in person, providing a due physical ID (passport etc). If the eID is issued on a smart card, the user, after having ordered it via the Internet bank, will need to collect the eID at a bank or post office, showing a physical ID.[341]

Attributes

BankID

BankID eIDs can be issued either on smart cards or as files to be stored on the hard disk.

For key, certificate and cryptographic access BankID provides both CSP and PKCS#11 drivers. As to middleware, on the client side BankID provides an authentication and signing plug-in that all users must use.

The BankID organizational structure does not depend on or include any Certificate Policy and Certification Practice Statement. Instead, BankID signs contracts with all parties. These contracts are not public.

As to the CA hierarchy it starts with the BankID Root CA. Below there are intermediary CAs for the different banks that are part of the BankID consortium. Each bank then has between two and five different CAs, (some of) which issue certificates to the users (bank customers).

[338] Modinis IDM Country report Sweden, June 2006.

[339] Modinis IDM Country report Sweden, June 2006.

[340] Country report Sweden by Arvid Welin, Sweden.

[341] IDABC interoperability for PEGS country report Sweden, November 2007, p. 22.

The user receives two certificates: one authentication and one for signing. These certificates are very similar; they have the same name (subject DN) and are issued and revoked together (and constitute from a user perspective “one eID”). The personal identity number is used as the subject serial number.[342]

Steria

Steria’s eIDs can be issued either on smart cards or as files to be stored on the hard disk.

Steria provides different PKI client middleware based on customer needs.

The user receives two certificates: one for authentication and one for signing. These certificates constitute a pair; they have the same name (subject DN) and are issued and revoked together (and are from a user perspective “one eID”). The personal identity number is used as the subject serial number.[343]

Nordea

Nordea eIDs can be issued either on smart cards or as files to be stored on the hard disk.

For key and certificate access Nordea provides the middleware Nexus Personal to Nordea customer.

Nordea does not have a CA hierarchy but works with a flat solution with self-signed CAs, which includes separate CAs for eIDs issued on cards and on files.

The user receives two certificates: one certificate for authentication and one for signing. These certificates constitute a pair; they have the same name (subject DN) and are issued and revoked together (and are from a user perspective “one eID”). The personal identity number is used as the subject serial number.[344]

TeliaSonera

TeliaSonera’s eIDs can be issued either on smart cards or as files to be stored on the hard disk.

CAs used for issuing TeliaSonera’s eIDs are currently not part of a common CA hierarchy. A Root CA has, however, been created, under which TeliaSonera potentially will gather these CAs. Today only the CA that is used for issuing eIDs on files to be stored on the hard disk is signed by the Root CA.[345]

Commercial CA certificates

There are no accreditations, registrations, certifications or other requirements for CAs that want to issue non-qualified certificates to the Swedish public. Furthermore, there is nothing that prevents an individual public authority or municipality to accept other certificates than the eIDs (that have been subject to a public procurement process).[346]

WIPK

Over time WAP had gone forward and resulted in a specification of how a PKI-based security solution should be designed (WAP PKI or WPKI). Since the Internet bank Handelsbanken had established already used PKI as method of security, WPKI-based mobile services could be possible to integrate without further extensive amount of work.[347] To further develop and maintain the mobile eID standard a non-profit association called WPKI was set up. The secure electronic identification by means of mobile devices use the SIM card of a mobile phone and the mobile eID are mostly issued by Swedish

[342] IDABC preliminary Study on Mutual Recognition of Signatures for eGovernment applications, national profile Sweden, April 2007, p. 18.

[343] IDABC preliminary Study on Mutual Recognition of Signatures for eGovernment applications, national profile Sweden, April 2007, p. 17.

[344] IDABC preliminary Study on Mutual Recognition of Signatures for eGovernment applications, national profile Sweden, April 2007, p. 17.

[345] IDABC preliminary Study on Mutual Recognition of Signatures for eGovernment applications, national profile Sweden, April 2007, p. 19.

[346] IDABC preliminary Study on Mutual Recognition of Signatures for eGovernment applications, national profile Sweden, April 2007, p. 19.

[347] Sverker Arvidson, Use the mobile phone as a secure channel with Wireless PKI, http://www.wpki.net/files/WPKI_History.pdf.

banks.[348] It has a standardised infrastructure with well-defined roles and agreed interfaces for RA/CAs (certificate issuer), Mobile Operators, Relying Parties and End Users. It is a hard key PKI-solution based on existing infrastructure (mobile phones, SIM-cards, mobile Internet access). It is making the mobile telephone a personal trusted device in a variety of contexts and for a multitude of services.[349]

Authentication Authority

Steria

For the validation of electronic signatures created with Steria eIDs Certificate Revocation Lists (CRLs) are used. The Online Certificate Status Protocol (OCSP) is planned to be supported in the future.

Nordea

For the validation of electronic signatures created by means of the eID the Online Certificate Status Protocol (OCSP) is used. However, there is also a possibility to use the Certificate Revocation Lists (CRLs).

TeliaSonera

For the validation of electronic signatures the Online Certificate Status Protocol (OCSP) is used for all TeliaSonera eIDs, except for electronic signatures created with certificates issued by one older CA, where Certificate Revocation Lists (CRLs) are still used.

eIDentity: Svensk e-legitimation (Swedish eID)

Svensk e-legitimation = "Swedish eID" - proposed to the Government, issued for natural persons, basic information of the person

Svensk e-tjänstelegitimation = "Swedish corporate eID" - proposed to the Government, issued for natural persons in their capacity as employee or contractor, which contains details of organisational affiliation. Basic information of the person as well as information of the corporation and attributes of the person/employee are included.[350]

Form

Advanced electronic signatures with encryption keys protected in hardware (microchip or equivalent). The security requirements correspond to the European standard ETSI TS 102 042 NCP+.

NB. Qualified certificates are about to be introduced in Sweden, having not yet come into use in the public eServices.[351]

Eligibility

An e-legitimation can only be obtained by individuals that are registered in the National Registry. One of the reasons for this limitation is that the information in the National Registry is used to verify the individual's claims and to obtain the physical address to which the activation code will be sent (by ordinary mail). Another limitation is that the individual must be over 16 or 18 years old.[352]

Legal persons can also use an eID, though it must be linked to a user with a Swedish personal identity number. In this case, two types of certificates come in question, namely the server and stamping cer-

[348] Modinis IDM Country report Sweden, June 2006.

[349] WPKI Project and Infrastructure, Presentation, 2005; http://www.wpki.net/files/WPKI_general_presentation_1.pdf.

[350] Country report Sweden by Arvid Welin, Sweden.

[351] Country report Sweden by Arvid Welin, Sweden.

[352] Country report Sweden by Arvid Welin, Sweden.

tificates, for authentication and signing respectively. The certificates contain the name of the organisation and the organisational number, and may also contain an URL. The contact person ordering organisational certificates must have an authorisation for this purpose from a person authorised to sign on behalf of his/her organisation. So the legal person as such cannot have an eID. [353]

Responsible authority

The Administrative Development Agency VERVA is responsible for the procurement process stating that the contractor (CA) is responsible for issued eIDs, – procured banks and Telia. [354]

Attributes

The e-legitimation and the QEC each hold:

CN(commonname)=efternamn & förnamn (familyname & first name)

SerialNumber=personnummer (unique personal number, incl date of birth and sex)

C=SE nationalitet (nationality). [355]

Since the personnummer includes date of birth and sex this information can be obtained.

(yymmdd-nnNc) nn = serial number, N shows sex – even figure = female, uneven figure = male, c is a quality control figure.

There is no other attribute than name and nationality concerning role or status obtainable from the e-legitimation. [356]

Conditions for use

Data stored on the RFID chip is not encrypted and can be read out by anyone, which is a huge privacy issue. It is also not clear what will be the implications of storing biometric information in a central database. [357]

Creation and termination

The e-legitimation is issued after a personal eye to eye meeting with a representative of the issuer. The identity attributes are downloaded from the SPAR catalogue which consists of information from the National Population Registry.

The e-legitimation shall be terminated by the holder if the e-legitimation or the personal keys have been lost or may have been copied.

The validity is restrained to 3 – 5 years. [358]

16.6 Authentication Authority

For verifying identities and electronic signatures specified software is used at the Relying Party. Using this software each end-user transaction with the e-legitimation used for identification or signature a control (OCSP) will be performed by the issuer for the certificates relevance including contact with the issuer's revocation service.

[353] Factsheet - Sweden - National Infrastructure; epractice.eu, July 2008.

[354] Country report Sweden by Arvid Welin, Sweden.

[355] Country report Sweden by Arvid Welin, Sweden.

[356] Country report Sweden by Arvid Welin, Sweden.

[357] Modinis IDM Country report Sweden, June 2006.

[358] Country report Sweden by Arvid Welin, Sweden.

The SPAR catalogue holding basic identity information of Swedish citizens, originating from the National Population Registry, is open for all parties through a contract with SPAR. Before the contract can be signed the need of relevant information is decided. [359]

16.7 Conclusions

Sweden has been successful introducing eServices using eIDs and eSignatures using a pragmatic approach. Still it is time to take a second step evolving the infrastructure from one based on procurement and contracts into one of a legislative nature. The new infrastructure has been proposed to the Government and will be decided upon by the spring of 2009. It will introduce a single point of contact for the public sector and parallel points of contact for industry using the same eID. Attribute services will be introduced as well as the SAML technique in order to meet the needs of information for relying parties' e-services. In order to meet the needs of employees to be identified in their work procedures a Swedish corporate eID will be introduced including information of the person as well as the corporation in parallel with the Swedish eID including basic information of the person.

Sweden uses a system of soft certificates issued by a large number of CA's.

The SPAR catalogue holding basic identity information of Swedish citizens, originating from the National Population Registry, is open for all parties through a contract with SPAR. Before the contract can be signed the need of relevant information is decided. [360]

[359] Country report Sweden by Arvid Welin, Sweden.

[360] Country report Sweden by Arvid Welin, Sweden.

17 Country report: United Kingdom

17.1 Structure of the Administration

It is for each Government Department and Local Authority to consider whether it has the power to deliver their own eID services. In the UK it is not possible to mandate the use of centrally provided infrastructure or eID.

The Identity and Passport service has the Identity Management Policy lead for the UK Government and together with UKBA the responsibility for delivering the National Identity Scheme (NIS).

The NIS is currently defining its strategy and therefore Government Departments and Local Authorities currently take their policy guidance for registration and authentication from the Central Sponsor for Information.

Currently, none of the centrally issued citizen documents enable eID for the citizen. Passports and Driving licenses do not currently have means of being read electronically over the internet. It is currently unclear whether the proposed ID card will be applicable for eServices for the citizen.

In the absence of a national eID scheme, and given financial constraints of the project do not permit data obtained for passports to be used as a basis for an eID, this response instead focuses on the user ID and password citizens may obtain if they wish to access certain central or local government services through the UK Government Gateway.

The Government Gateway is the current centrally provided infrastructure for accessing government services electronically..Government services providers can chose to use this. . The service is provided by the Department of Work and Pensions. Its target audience is citizens, business and government employees. The predominant token is a user ID and password

17.2 Debate (and history)

There has been considerable debate over a number of years - too much to identify and itemize for this document. Much of the debate has been around the use to which the information would be put and the extent to which this will assist in preventing identity fraud.

17.3 eID model

No national eID scheme exists in the UK. In addition it is not financially possible to link with passport records for the purposes of project STORK. As discussed above, instead this response will focus on the UK Government Gateway

The UK Government Gateway provides the current national infrastructure for integration with central and local government . Government service providers can chose to leverage its functionality of a strategic shared service. The government Gateway acts as data processor for the participating services The users can be citizens, businesses or Government employees. The fundamental principle of the Gateway is that it allows a customer to have a single set of credentials (although they can choose to have different IDs and passwords for each service provider) to be able to interact online with multiple Government Services. As the UK Government does not have central registers, the Government Gateway allows the customer to enroll in online services and verify their identity to each service. The statistics are as follows:

- 97 Identity based services
- 55 Government organisations
- more than 14 Million enrolments into services

The Government Gateway is not a biographical data store. The process of enrolling into services uses biographical data provided by the user which is checked with the service provider. Once the user has proved ownership of that data (via use of an activation pin), the Government Gateway stores the service identifier against the users account and deletes the biographical data.

The Government Gateway supports the Cabinet Office policy for levels of assurance which are 0,1,2,3. The enrolment process can either be a level 1 or a level 2 and this is dictated by the strength of the data questions asked of the user. A one-time activation PIN is also sent in the post to the service registered address. The credentials used are as follows:

- User Id and password – Level 1
- Soft certificates provided by trusted 3rd parties – Level 2 (very low usage due to the business model of user pays)
- Chip and PIN (Using EMV Challenge and Response, PIN Protected) – Level 2 – currently only for Government Employees.
- OATH based one time password tokens (PIN Protected) – Level 2

Planned

- Shared secrets – level 2

the biographical data provided by the user is checked by the service provider against data they already hold. The checks to verify the information already held by a service provider will vary from service to service, therefore the information provided by the user to obtain an enrolment into a service will be checked against information of variable quality.

17.4 Principal legislation and policy documents

Legislation:

The main provisions that regulate our sharing of data internationally are:

- the Data Protection Act 1998 (DPA) which implements the Data protection Directive;
- the Human Rights Act 1998 (HRA) which implements the European Convention on the Human Rights,
- the duty of confidence and the tort of misuse of private information under common law.
- The requirement in domestic public law for a public authority to have a legal power to share information
- domestic legislation which provides for the disclosure of certain types of information to be a criminal offence in some circumstances e.g. Section 123 Social Security Administration Act 1992 which makes it a criminal offence to share social security information without lawful authority
- Art 5 of Directive 97/66 was implemented by Part I of RIPA
- Directive 2002/58 was implemented by the Privacy and Electronic Communications (EC Directive) Regulations 2003
- The fixed line and mobile telephony aspects of Directive 2006/24 were implemented by the Data Retention (EC Directive) Regulations 2007 – we are currently consulting on the Regs which will complete the implementation.
- under domestic law public authorities need to have a legal power to share data

Policy:

The primary legislation for the National Identity Card Scheme is the Identity Cards Act 2006. The

Strategic Action Plan for the National identity Scheme – safeguarding your identity (Home Office December 20060 sets out the policy in relation to the proposed national identity scheme which is not yet in place.

There is a strong policy that we do not want anything that could be interpreted as an EU-social security number/card. This has implications for any form of e-ID which would effectively create such a number

The Government Gateway does not have policy or legislation that supports its use. It is a strategic shared service provided by the Department for Work and Pensions for central and local government services that has always had to prove value to its Government Customers. Use of the Government Gateway user id and password and information from a participating service in default of a national eidentity scheme would represent a novel use of the government Gateway and service information and require the resolution of a number of legal issues

17.5 Analysis

eIdentity: UK Government Gateway User ID and Password

Name

UK Government Gateway User ID and Password (Level 1). This is the predominant form of credentials used by Citizens and Businesses when accessing the government gateway.

Form

User ID and Password linking through to the service identifier. The user can enroll in several services to link their service identifier to their Government Gateway account.(A citizen can have multiple Government Gateway user IDs and passwords as the user can choose to have a different one for each service)

Eligibility

A user ID and Password can be obtained by anyone. (There is no citizenship restriction) Typically, a user can only enroll into Government Services if they already have registered with the service owner through another channel. The Government Gateway allows them to interact with the service provider through the online channel.

Issuer

The Government Gateway issues the credentials however the verification of identity is a service by service activity. Once the user has enrolled into a service and they use their credentials for authentication then the Government Gateway is the Identity Provider and will return the service identifier to the service.

Responsible authority

The Department of Work and Pensions is responsible for the Government Gateway and is responsible for issuing the User ID and Password for use for the Government Gateway. We also trust soft certificates that are issued by 3rd party certificate authorities that are scheme accredited.

Attributes

The User ID is a randomly generated 12 digit number. It is only ever linked to service identifiers which take the format that is defined by the service owner. There is a linking identifier called the credential identifier which allows the user to have multiple credentials that link to their service identifiers.

It is currently not technically possible to obtain reliable information about attributes such as address, age, university enrolment etc from authentic sources.

Conditions for use

The user ID and Password can only be used for public sector services. It can be used for any such service that chooses to leverage the infrastructure, although the user may choose to have different user ID and password for different services.

Creation and termination

The password is created by the user and entered online. The user ID is generated automatically and is returned to the user online. The user ID is also sent in the post to the address for the service that they are enrolling into.

17.6 Authentication Authority (AA)

The Government Gateway is the AA. When a Government Organization requests to use the Government Gateway they need to sign a memorandum of understanding with the department of Work and Pensions.

Name

Government Gateway.

What

The Government Gateway can authenticate its own issued eID as well as those of third parties. The current examples are:

User ID and Password (issued by the Government Gateway for citizens and business)

Soft Certificates (Issued by trusted Third Parties)

Chip and PIN cards (Issued by the Ministry of Defense for their employees)

Responsible authority

Department of Work and Pensions is responsible for the AA.

Input

The Input to the Authentication Authority for citizens and businesses are predominately user ID and password. There are no legal constraints on the user ID and password as the user has been in control of obtaining their credentials in an online environment. The user ID and password are used to access services that the user has chosen to enroll into and can de enroll if they choose to. The sharing of data is based on consent

Output

The Authentication Authority provides the unique service number back to the service. Specifically it can only return the appropriate service number back to the appropriate service. The authentication authority is a data processor and not a data controller and hence it cannot share service identifiers between Government Organizations. The authentication authority complies with the Data Protection Act 1998 as it only processes the data for the purpose that it was intended, which is to enable the citizen to enroll in online services.

For whom

Any Government Organization Service Provider can connect to the Authentication Authority. There is an engagement process with each service provider that connects them to the AA.

They can also decide to deliver their own eID solution.

Process

The user, either a citizen or a business, will chose to enroll in online services. Each service will need to go through an identity verification process to prove that the user owns the service identifier for the service. When the user first does this they will obtain their credentials.

The current authentication process is only online. The credentials are authenticated electronically and the output is a technically signed SAML token which the service provider needs to process. Legally the authentication authority complies with the data protection act as the user is choosing their services to enroll into and it only returns the service identifier back to the service that it was intended.

17.7 Conclusions

Key issues include:

Whether the relevant public authority has the legal power to provide an eID scheme for the purposes of project STORK in the light of legislation relation to the National Identity Scheme and identity cards

Whether the public authority considers it is appropriate to provide an eID scheme in the light of the level of identity assurance STORK participants will require, as measured against the level of assurance that can be supplied in the absence of the National Identity Scheme

Domestic legislation and policy issues affecting the use of social security information, in particular NINOs, as a means of providing an eID and policy views on the undesireability of an EU wide social security card/number.

Identification of a solution that provides sufficient security whilst also being consent based and user drive.

Bibliography

EU (2006). "Consolidated Versions of the Treaty on European Union and of the Treaty Establishing the European Community." Official Journal of the European Union C 321(E/1).

Graux, H. and J. Majava (2007). Analysis and Assessment of similarities and differences - Impact on eID interoperability. eID Interoperability for PEGS, IDABC.

Graux, H. and J. Majava (2007). Proposal for a multi-level authentication mechanism and a mapping of existing authentication mechanisms. eID Interoperability for PEGS, IDABC.

Myhr, T. (2005). Regulating a European eID: A preliminary study on a regulatory framework for entity authentication and a pan European Electronic ID, The Porvoo e-ID Group.

Modinis IDM Study, National IDM Profiles, National Profiles
https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/bin/view.cgi/Main/NationalProfiles

Factsheet – e-practice.eu, April 2008.
http://www.epractice.eu/factsheets

IDABC eID Interoperability for PEGS country, November 2007
http://ec.europa.eu/idabc/en/document/6484/5644

IDABC, Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications
http://ec.europa.eu/idabc/en/document/6485

Country Report 2008 Sweden for International Council for information Technology in Government Administration, Verva, 2008.
http://www.verva.se/upload/english/ICA-Country-Report-Sweden-2008.pdf

Electronic identification and signature in Sweden, Summary from 2008:12, Verva, 2008.
http://www.verva.se/upload/publikationer/2008/Electronic-identification-and-signature-in-Sweden.pdf

Certification Authority, Ministry of Public Administration
http://www.ca.gov.si/eng/eng-tehnicne_osnove.php