Master Thesis Information Sciences

Radboud University

Electronic Identity Management Systems in the European Union

Author:
A.H. Zwilling
Armin.Zwilling@student.ru.nl
s4227646

Supervisor:
dr. J.E.W. Smetsers
s.smetsers@science.ru.nl

Second reader:
prof. dr. M.C.J.D. van Eekelen
M.vanEekelen@cs.ru.nl

July 2, 2017

Abstract

Since the beginning of the 21st century European countries started developing systems for electronic identification. These systems should improve the services towards its citizens. In this research we investigate how systems of member states compare to the Dutch system. In 2017 the Dutch government wants to implement a new platform for electronic identification. In earlier attempts implementing these platforms in other countries mistakes were made and we want to know if the Dutch government learned from the mistakes and opportunities of the other member states. First of all we conducted a small research to select a few systems that we wanted to investigate further. Then we created a methodology to compare these systems.

The legislation of the European Commission is used for comparing the systems, since it forms the basis for all European Member states. In two Regulations the European Commission set out the minimal requirements for electronic identification management systems where the member states need to oblige to. In this paper we created a methodology to gather and structuring the data, making a classification system and classify the structured data. The research concludes that the new Dutch system is not the optimal system at this moment, but has the potential to be.

Acknowledgements

This thesis is the result of months of hard work to complete my Master Information Science. This research was conducted at the Radboud University in Nijmegen.

First of all I want to thank Sjaak Smetsers, my supervisor, for this opportunity and helping me throughout the whole journey. He provided me with a lot feedback to improve this research. Secondly I want to thank Marko van Eekelen for being the second examiner and reading my thesis. Thirdly I want to thank my father for reading my thesis and giving me useful feedback. Finally I want to thank my family and friends for supporting me along the way.

Table of Contents

List of Figures

List of Tables

List of Abbreviations

BSN	Burgerservicenummer
BRP	Basisregistratie Personen
CA	Certificate Authority
CIPEI	Central Infomation Point e-ID Investigations
CMB	Citizenship and Migration Board
CRL	Certificate Revocation List
CSP	Cryptographic Service Provider
EC	European Commission
EIC	the International Electrotechnical Commission
eID	Electronic Identity
eIDAS	EU Regulation No 910/2014 on electronic identification and trust services for electronic transactions in the European internal market.
eID system	Electronic Identity Management System
ENISA	European Network and Information Security Agency
EU	European Union
FEDICT	Federale Overheidsdienst voor Informatie- en Communicatietechnologie
FP	Final Pseudonym
FPO	Federal Printing Office
ICT	Information Communication Technology
ISO	International Organization for Standardization
KvK	Kamer van Koophandel
LoA	Level of Assurance
LoAs	Levels of Assurance
NR	National Register

PKI	Public Key Infrastructure
PP	Polymorphic Pseudonym
QAA	Quality Authentication Assurance
RA	Registration Authority
RRN	Rijksregisternummer
SA	Stelselautoriteit
SSO	Single-Sign-On
STORK	Secure idenTity acrOss boRders linKed

1. Introduction

Since the beginning of the 21st century, when the internet was uprising, different states of the European Union (EU) started developing systems for electronic identification. In 2006 the European Union created a strategy to accelerate the possibilities and usage of eGovernment in Europe [14]. The resulting i2010 eGovernment Action Plan describes all the actions of the European Union to accelerate this process from 2006 till 2010 [12]. Every five years the EU reviews the steps that have been taken and writes a new roadmap for the coming years. The ambition that was formulated in 2006 regarding Electronic Identity Mangement Systems (eID systems) stated as follows: *By 2010 all European citizens, businesses and administrations shall benefit from secure means of electronic identification that maximize user-convenience while respecting data protection regulations. Such means shall be made available under the responsibility of Member States but be recognized across the EU* [28].

Every five years the EU makes a plan to improve the existing developments, raise awareness and implement concrete solutions. The ambition for 2015 stated as follows: *European public administrations will be recognized for being open, flexible and collaborative in their relations with citizens and businesses. They use eGovernment to increase their efficiency and effectiveness and to constantly improve public services in a way that caters for user's different needs and maximizes public value, thus supporting the transition of Europe to a leading knowledge based economy* [13].

The implementation of this eGovernment Action Plan resulted in a number of projects for cross borders eGovernment services like Secure Identity Across Borders Linked (STORK)[1]. STORK is a project to enable European citizens to use their electronic identification in member states with which they can authenticate themselves. All projects have the same goal: to create an interoperable framework. STORK created a Quality Authentication Assurance (QAA) [32]. This framework describes how the individual national authentication can be mapped to the QAA levels to ensure interoperability. The stronger the requirements, the higher the level of assurance will be. The requirements are divided by organizational and technical factors. The organizational factors describe the offline and online registration phase and the technical factors describe the electronic authentication phase. The higher the needed assurance, the higher the corresonding requirements, the higher the Level of Assurance (LoA) realized. The higher the desired LoA, the higher the corresponding requirements, the higher the provided assurance of the user's identity [43].

[1] Secure Identity Across Borders Linked (STORK) `https://www.eid-stork2.eu/`

1.1 International Organization for Standardization

The International Organization for Standardization (ISO) and IEC (the International Electrotechnical Commission) are known for developing the most important international standards for almost all aspects of technology and business. They adopted the STORK-project and standardised it. They started the project in 2011 and finished it in 2014. ISO/IEC focuses on electronic transactions within or between ICT systems that depend on a specified level of confidence, whereas STORK focuses on the interoperability of the different systems of the member states. The ISO/IEC 29115:2013 [33] standard provides a framework for managing entity authentication assurance in a given context.

1.2 eIDAS Regulation

Besides the action plan by the EU (and a whole digital agenda), the EU created regulations on electronic identification and trust services for electronic transactions in the internal market (eIDAS). A regulation is a legal act and is immediately enforced as law in all member states. The goal of eIDAS is *to boost trust and convenience in secure and seamless cross-border electronic transactions by promoting the widespread use and uptake of electronic identification and trust services (eIDAS services).* There is a number of regulations that are crucial in relation to this subject. Regulation 910/2014 [51] was the first step towards creating an online environment that is essential for economical and social developments. This Regulation describes the minimum technical specifications and procedures for assurance levels for electronic identifications on electronic identification and trust services for electronic transactions in the internal market. This Regulation is based on STORK and the ISO/IEC 29115:2013 standard and focus on three main matters:

- Under which conditions electronic identification of natural and legal persons are recognized which are identified at another member state
- The rules for trust services (mainly electronic transactions)
- The legal framework for all electronic identifications and authentications

Implementation Regulation 2015/1502

On 8 September 2015, the European Commission created Implementation Regulation 2015/1502 based on the 910/2014 Regulation [52]. This paper will use the Implementation Regulation to compare the eIDs that are mentioned in chapter 4. This Implementation Regulation is used rather than the STORK and the ISO standard since a regulation is immediately enforceable as law in all member states. Furthermore this regulation is based on both the STORK-project and ISO standard. The specifications and procedures described in this 2015/1502 regulation are divided in four elements: Enrollment, Electronic identification, Authentication and Management and Organization. These elements are all based on Article 8 of Regulation 910/2014. This paper will use the elements enrollment and electronic identification to compare the procedures concerning identity proofing and obtaining, suspension and reactivation of the electronic identification means. In chapter 5 these elements are described and and the chapter will consist of the comparison study.

1.3 Idensys

The Netherlands started developing a system called 'DigiD' that allowed citizens to authenticate themselves with for online services of the government in 2003. This was a result of the plan 'Andere Overheid' in which the government aimed to improve the quality, efficiency and effectiveness of their services. There was an important role for the ICT in this plan, since the government could be modernized. The service towards citizens was also extended to 24 hours, seven days a week. This new system was introduced in January 2005 [53].

After a few years the government started to develop a new system in cooperation with private businesses with which organizations could authenticate themselves for the online services of the government, just like DigiD.

The government saw that citizens and organizations had a lot of authentication tokens to remember/use for different services like user name/password, sms-codes and card-readers. Since this is not very convenient the government aimed to create a platform with which citizens and businesses could choose one way to authenticate and then could use several services without using another authentication method. Furthermore this platform is not limited to the services of the government, private organizations like web shops also can join this initiative. Since 2014 the government has been developing this system called 'Idensys'. Thus, Idensys is a platform to which multiple authentication services and service providers are connected where the user only needs one authentication means. With one authentication means it is possible to use all the services without logging in separately for each one.

This paper will compare the new developed Dutch system Idensys is compared to other systems used in the European Union, based on the regulations of the European Commission on electronic identity management.

1.4 Research Question

The goal of this research is to find out to what extent the Regulations determine the trustworthy of the electronic identity management systems in the European Union. To determine the trustworthiness it is necessary to understand how these systems work and what the differences are between these systems.

Mapping the systems to the LoAs (classification) should clarify whether the regulation gives a good example of trustworthiness of these systems. Does mapping multiple systems to the same LoA mean that they are even secure/trustworthy? Are the criteria of the regulation specific enough or formulated too generally? Thus in this research we want to find out what the usability is of comparing different eID systems using the Regulations provided by the European Union. For this research we formulate the main research question as follows:

Is Idensys the best electronic identity management system in the European Union?

To answer this question, this research will also address the following sub-questions:

- What is an electronic identity management system?
- How are the criteria for the classification determined?
- How are the eID systems being classified?
- How do the eID systems measure with the new Dutch system?

1.5 Outline

Chapter 2 gives an introduction of the basic principles of an eID system. Concepts like Public Key Infrastructure and the use of certificates will be addressed in this chapter and are necessary to understand how electronic identity management systems work. The method used for this research is mentioned in Chapter 3. Chapter 4 contains the description of the eID systems that are a result of the short survey. The classification of the eID systems is provided in Chapter 5. The following chapter contains the conclusion of the research. The full description of the requirements of the Levels of Assurance, the Quickscan and the used coding can be found in the Appendix.

2. Background

This research will look at the eID systems of multiple governments of the EU. The goal of these systems is to distribute electronic identities across multiple digital domains. With this distribution users get authenticated and authorized on multiple domains without the need to log in separately every time. Besides authentication the eID systems suffice in making digital signatures. Through digital signatures, the user confirms the correctness of specific information. The digital signatures offer the possibility to do online tax returns. For this example it is important that the identity of the user is determined with certainty. Furthermore, that specific user needs to confirm the information and not someone else. This chapter will discuss the operation of authentication and creating digital signatures. Firstly, we will describe the basics of encryption that form the basis of these methods.

2.1 Public Key Infrastructure

Public Key Infrastructure (PKI) is a method with which users and computers communicate in a secure manner and with which the identities of both parties are determined with certainty. To encrypt messages in PKI public key cryptography is used. This cryptography is an implementation of the asymmetric-algorithm, meaning the key used for encrypting a message is not able to decrypt that same message. Public key cryptography used two keys; a public key and a secret key. The public key is shared and available to anyone and the secret key only known to the owner. Below are a few examples described to understand the public key encryption-process.

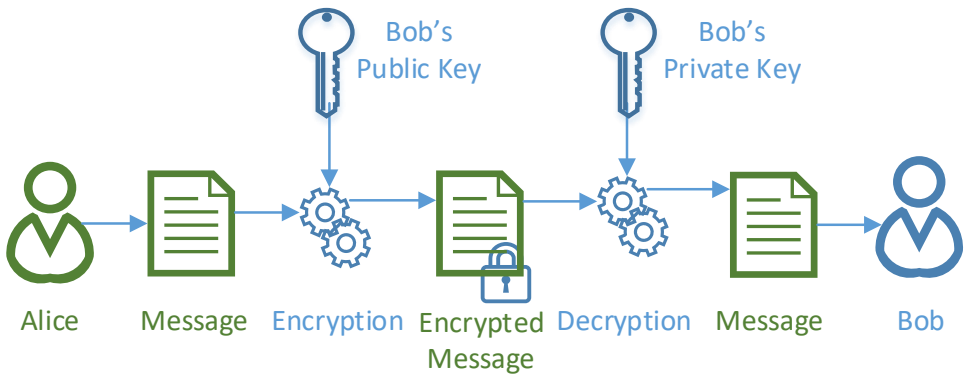

Figure 2.1.1: Example encryption with Public Key and Private Key

The process shown above is of Alice, who wants to send a message to Bob which only he is allowed to read. Alice used the public key of Bob, this key is available to anyone. Alice encrypts the message with this key. At present, no one is able to open the message except Bob, since he has the corresponding private key. Bob decrypts the message using his private key. In this process Bob is not able to determine that the message he got is from Alice.

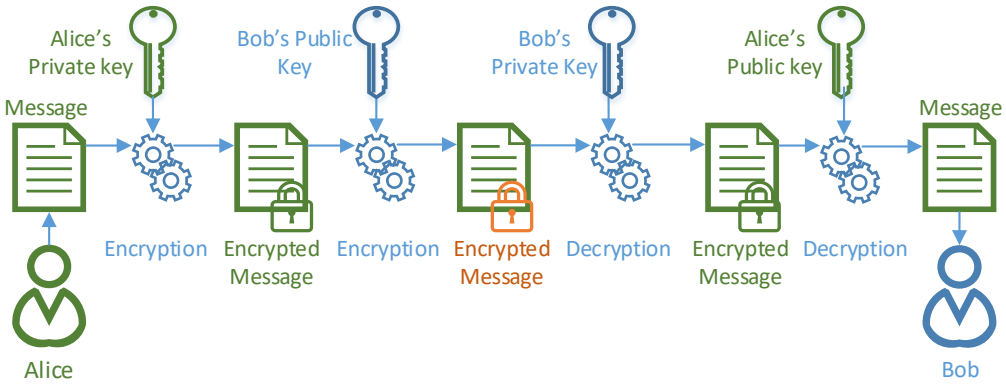

Figure 2.1.2: Basics Public Key Encryption

The process illustrated above is a more complex version of the first example. In this example Alice starts with encrypting the message with her private key. Then she encrypts it with Bob's public key and sends it to Bob. Bob uses his private key to decrypt the message. He uses the public key of Alice to retrieve the original message. In this process Alice shows that the message is sent by her and Bob is the only one who is able to read it. This process seems safe, yet it is still not possible to say with certainty that the public keys used actually belong to the parties who were intended to communicate. An attacker can impersonate Alice allowing Bob to think he is communicating with Alice, while in reality he is communicating with someone else. A PKI also uses certificates, in addition to the public key cryptography. A certificate is an electronic document that testifies that a public key belongs to a specific person, company or computer.

Certificates

PKI uses a model of trust where the Certificate Authority (CA) is the trusted entity to issue and manage certificates. When the CA issues a certificate, the identity described effectively belongs to the party holding the certificate. Examples of certificates include websites of banks, shops and news pages. When a certificate is used it can be seen when the address bar in the browser turns green or a lock appears. Figure 2.1.3 shows a example of the ING bank. The CA testifies that the identity of the website belongs to the ING. A certificate state what the objectives/identity are of the person(s)/entity, the identity of the CA, date of validity, the corresponding public key and the algorithm is used for encrypting.

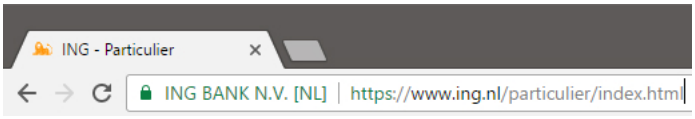

Figure 2.1.3: Example ING Certificate

Certificate Issuance

The CA manages all certificates, but the actual issuance is handled by the Registration Authority (RA). This is an instance that is certified by the CA and uses the services to issue certificates. At every request for a new certificate the issuing party needs to provide information to prove their identity. Depending the objective of the entity more or less information needs to be provided. This can vary from a check of registration in the Companies House of corporate information to a full personal verification by checking identity cards, contracts and positions in companies. When the information is checked by the RA, the information is sent to the CA to create a new certificate. This certificate is signed with the private key of the CA. Anyone is able to check the authenticity of the certificate authenticity using the public key of the CA. After creation, the certificate is sent with the corresponding private key to the applicant.

The CA maintains a database of requested, valid and revoked certificates. When a certificate is revoked, when it has expired for example, it is added to the on the Certification Revocation List (CRL). This means that the certificate is no longer valid and that the identity of the party concerned is not guaranteed.

2.2 Authentication

The first step using an eID system is the determination of the identity of a user. Is the user actually who he says he is? Most eID systems use a phone, tablet or a smart card with which users authenticate themselves. At the authentication request of a user, the certificate of a service provider is used to prove the user is actually communicating with the service he wants to. The user authenticates himself by, for example, a smart card. He logs in by entering the PIN corresponding to the smart card. The eID system checks the authentication message with the public key of the user to determine the identity. Subsequently, the eID system sends a message to the service provider that the identity of the user is known and checked, and that he is logged on. Finally, the user is able to use the service of the service provider.

Figure 2.2.1 schematically shows this authentication process. At step (1) and (2) the user indicates that he wants to make use of a particular service. The certificate of the service provider is displayed in the browser so the user sees he is using the intended service. Then the service provider sends the user to the eID system in step (3) for authentication. The eID system sends an authentication message to the user (4). The users uses the smart card to authenticate locally (5) & (6). After a successful authentication, an authentication message is encrypted with the private key of the user. This, together with the certificate of the user is sent to eID system which checks the identity (7). After this check the eID system sends a message to the service provider that the user is authenticated (8). The user is now able to make use of the service (9).

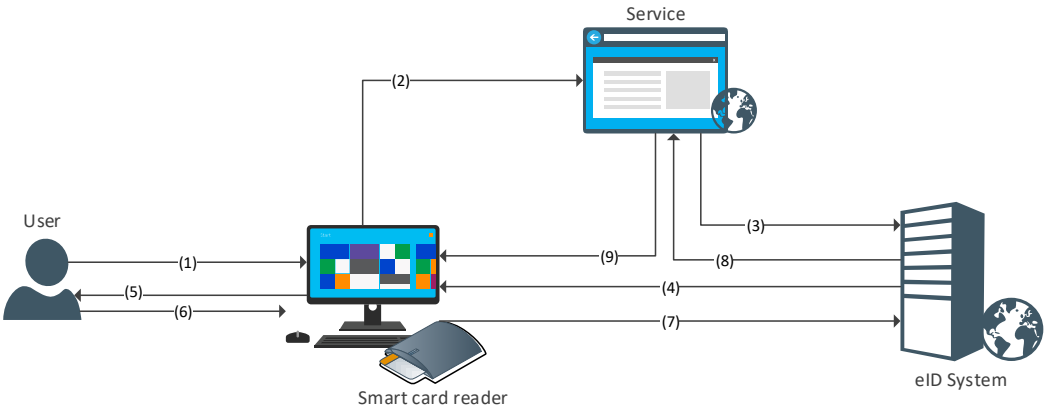

Figure 2.2.1: Authentication process eID system

2.3 Digital Signatures

Digital signatures are intended to sign digital information. With these signatures the correctness of information is confirmed. It is important that it determines with certainty that a particular user has signed the information. The intention of a user needs to be recorded. It is hereby assumed that the user has already been authenticated.

In the late nineties, the European Commission (EC) created European Directive nr.99/93/EG[2] for digital signatures. *'The purpose of this Directive is to facilitate the use of electronic signatures and to contribute to their legal recognition'.* The Netherlands adopted a law for electronic signatures ('Wet Elektronische Handtekeningen') in 2003, which determines when a digital signature is valid. In this law three distinctive forms of electronic signatures were made in this law; simple, advanced and qualified signatures.

Simple signatures are signatures *'with electronic data attached to or logically associated with other electronic data and which serve as a method of authentication'.* These are, for example, scanned signatures. An advanced signature is a signature where algorithms calculate a unique code from the message and the identity of the user. A qualified signature is an advanced signature with a qualified certificate. These certificates are only issued by accredited CA's.

[2] European Directive 1999/93/EG
`http://eur-lex.europa.eu/legal-content/NL/ALL/?uri=CELEX:31999L0093`

3. Method

In order to determine how the new Dutch system Idensys compares to other eID systems in the European we conducted a small research of the existing systems in the EU. Instead of examining all the eID systems we chose a small selection that we wanted to examine more thoroughly. The selection is made based on the unique aspects and features of the various implementations. This reveals the different perspectives that played a part during the development of the systems, making it possible to distinguish the differences. Next we made a method to operationalize the process from determining the criteria to the comparison of the systems.

3.1 Operationalization

The goal of operationalization is to create a method to gather information and classify the systems on a systematic, consistent and replicable manner to avoid subjective discrimination/interpretation. Furthermore this process should be representative and thus should be applicable to multiple situations where other systems are analyzed based on the information from literature. This process is schematically shown in Figure 3.1.1. The steps shown in the Figure and the manner in which they have been applied in this research are discussed below.

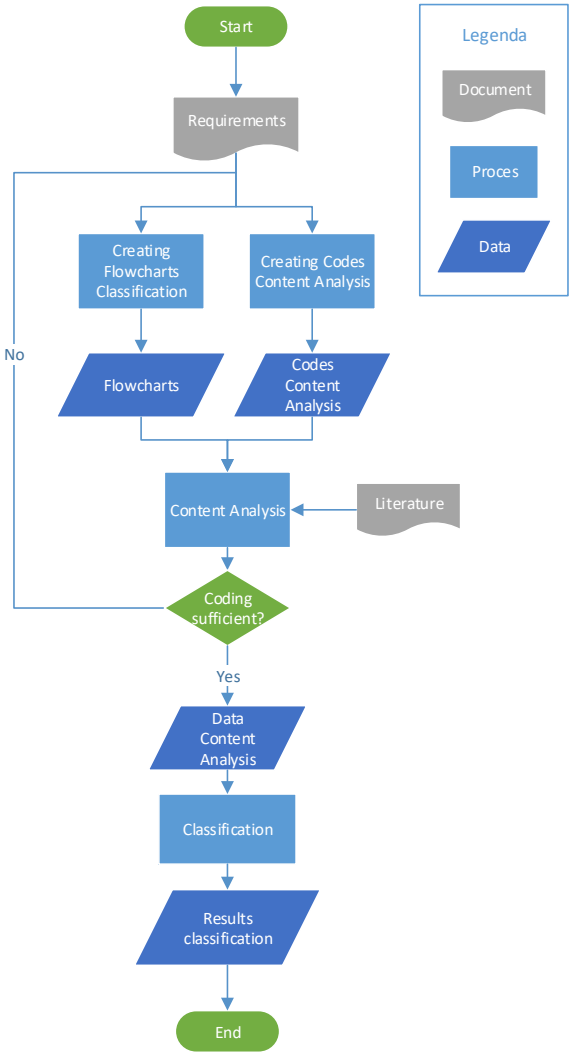

Figure 3.1.1: Flowchart Classification

Requirements

To compare the systems we first need to determine the criteria on which we want to compare the systems. We chose a common basis of the eID systems for the criteria; the EU Regulations. These Regulations are law enforceable and applied in its entirety across the member states of the EU. The LoAs described in the Regulaton 910/2014 [51] and the Implementation Regulation 2015/2012 [52] will be used as criteria which are described in Chapter 1. The aspects of the Regulation that are used in this research are: 'Application and Registration', 'Identity proofing and verification of a natural person', 'Electronic identification means characteristics and design', 'Issuance, delivery and activation', 'Suspension, revocation and reactivation', 'Renewal and replacement'. The other

categories are disregarded, since they are not relevant for this research.

Creating Flowcharts

The flowcharts are a step-by-step visual description of the requirements the level of a LoA will be reached. The requirements are often quite extensive, which is the reason the goal of these charts is to see at a glance to what LoA the systems needs to be classified. The core and the distinctive elements of the requirements are schematically shown in these flowcharts. With these charts the classification is done on a systematic, consistent and replicable manner.

Flowcharts in practice

All core and distinctive components of the requirements of a category are translated into a flowchart. These flowcharts are then used for classification. In the table below the requirements are listed for identity proofing and verification of a natural person.

Table 3.1: Identity proofing and verification (natural person)

Assurance Level	**Elements Needed**
Low	1. The person can be assumed to be in possession of evidence recognized by the Member State in which the application for the electronic identity means is being made and representing the claimed identity. 2. The evidence can be assumed to be genuine. 3. It is known by an authoritative source that the claimed identity exists and it may be assumed that the person claiming the identity is one and the same.
Substantial	Level low, plus one of the alternatives listed in points 1 to 3 has to be met: 1. The person has been verified to be in possession of a genuine and valid evidence that is recognized by the member state and steps have been taken to minimize the risk that the person's identity is not the claimed identity. 2. An identity document is presented during a registration process in the member state where the document was issued and the document appears to relate to the person presenting it and steps have been taken to minimize the risk that the person's identity is not the claimed identity. 3. Where electronic identification means are issued on the basis of a valid notified electronic identification means having the assurance level substantial or high, and taking into account the risks of a change in the person identification data, it is not required to repeat the identity proofing and verification processes.

Table 3.1 – continued from previous page

Assurance Level	**Elements Needed**
High	Requirements of either point 1 or 2 have to be met: 1. Level substantial, plus one of the alternatives listed in points (a) to (c) has to be met: (a) Where the person has been verified to be in possession of photo or biometric identification evidence recognized by the member state, the evidence is valid according to an authoritative source and the applicant is identified as the claimed identity through comparison of one or more physical characteristic. (b) Where electronic identification means are issued on the basis of a valid notified electronic identification means having the assurance level high, and taking into account the risks of a change in the person identification data, it is not required to repeat the identity proofing and verification processes. Where the electronic identification means serving as the basis has not been notified, the assurance level high must be confirmed by a conformity assessment body referred to in Article 2(13) of Regulation (EC) No 765/2008 or by an equivalent body and steps are taken to demonstrate that the results of this previous issuance procedure of a notified electronic identification means remain valid. 2. Where the applicant does not present any recognized photo or biometric identification evidence, the very same procedures used at the national level in the Member State of the entity responsible for registration to obtain such recognized photo or biometric identification evidence are applied.

As seen in the example above the requirements are quite extensive. The requirements of the identity proofing are analyzed and the most important aspects are modeled as shown in Figure 3.1.2. These flowcharts gives a step-by-step visualization when the system comply with a LoA. This should make the classification easier and reducing the subjectivity. All of the others flowcharts and an elaboration of the results of the classification are given in Chapter 5.

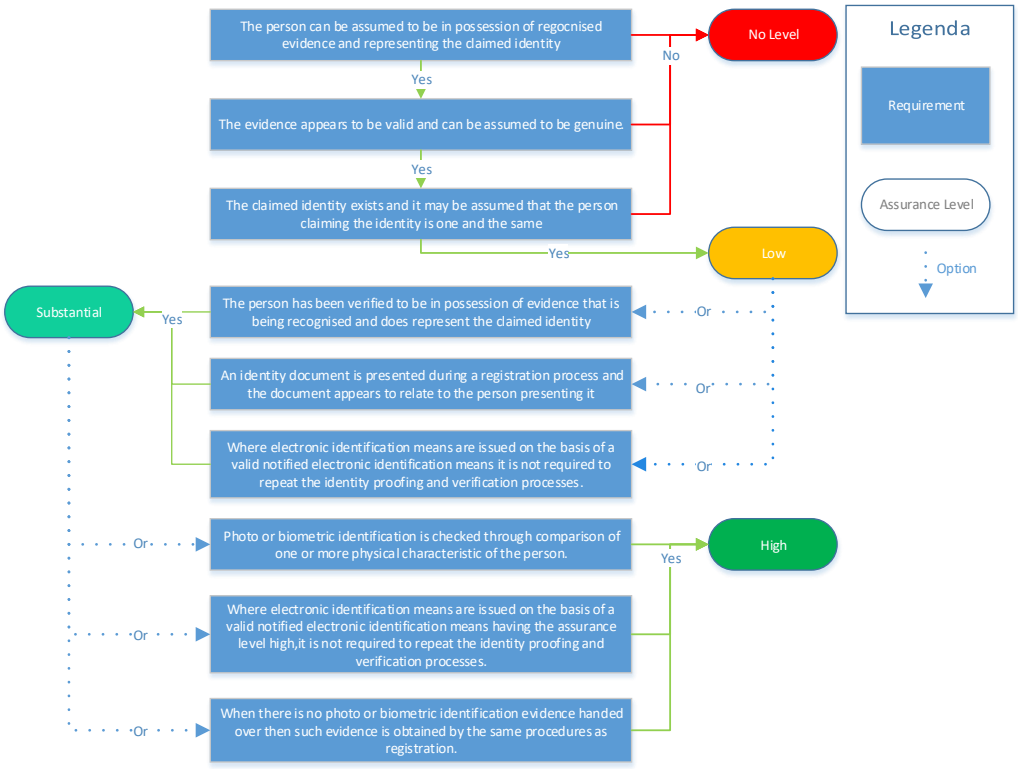

Figure 3.1.2: Flowchart Identity proofing and verification

Creating Codes & Content Analysis

Analyzing these systems will be done using the flowcharts and qualitative content analysis [6, 40]. *"Content analysis is a reasearch technique for the objective, systematic and quantitative description of the manifest content of communication"* [4]. Using content analysis we will reduce all available data to manageable data to identify patterns and gain insight. This research will use inductive coding (coding not based on previous research or theoretical framework), since there is no theoretical framework for this kind of research. The LoAs will be the basis for determine the coding. By coding, the data will be grouped and used to extract information. Using this method we want remove all subjectivity when the systems are classified.

When the resulting data from the encoding do not adhere to indicate whether systems meet certain requirements, the encoding is adjusted. This adjustment should ensure that more or more specific data could be grouped, which gives an answer to the question whether the system meets a requirement or not. This process repeats itself until the encoding is sufficient to gather all necessary data for every country as shown in Figure 3.1.1.

Content Analysis in practice

In the figure below an example from practice is shown where information of a paragraph from [11] is grouped for multiple codes.

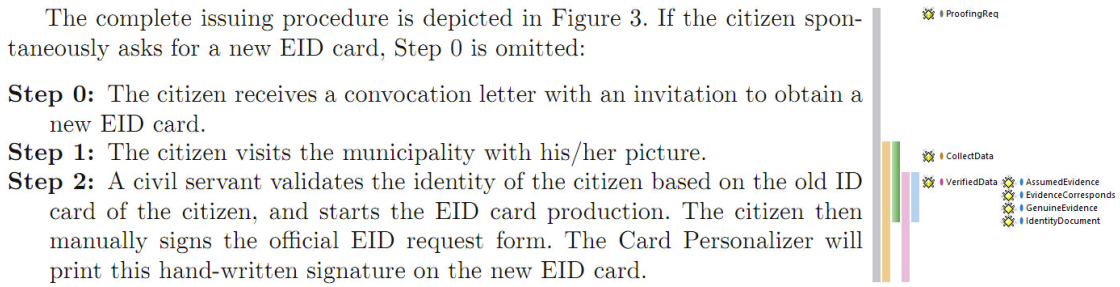

Figure 3.1.3: Coding Example

The figure shows that information from the paragraph is grouped for seven different codes. The length of the bar shows to which line of a paragraph the group goes. When groups overlap, each subsequent grouping gets a different color. As shown in the example, groupings may contain information for various codes. The coding for each country is then combined to use for the classification. Each paragraph of each paper has been carefully examined so that all possible information is grouped and encoded.

In Appendix C the codes are listed which are used in this research. The elaboration of the content analysis for Belgium are specified in Appendix C.1

Classification

The data from the content analysis is used for the classification to evaluate the systems and to see whether the new Dutch system is the new ideal system. The grouped data from the content analysis is used with the step-by-step representation of the flowcharts. The data shows whether a system met the requirement and thus should be classified to a LoA. With the results of the classification we can evaluate the systems. The results of the classification are described in Chapter 5.

4. Electronic Identity Management Systems

For this research we conducted a short survey to investigate which countries in the EU have an eID system implemented. The purpose of this survey is to arrive at list of countries that have different implementations of eID systems and select a few systems that will be investigated further. As described in chapter 3, we made a selection based on the unique aspects/features of the systems. The selected countries that will be discussed in this chapter are Belgium, Estonia, Germany, The Netherlands and Spain. The short survey is described in Appendix B.

4.1 Belgium

History

In 2000 Belgium launched a study to develop an electronic identity card (eID card) [17]. The aim is to create a system where (non) commercial parties improve their services using the eID card without the need to develop their own identity management system. With this system users are able to authenticate and sign documents digitally without (non) commercial parties need to invest heavily to set up a system for this. This card is the successor of the earlier existing identity card, but with the online features. After four years of development Belgium began with the deployment of the eID card in 2004. Since 2009 every resident of Belgium has the new eID card [70].

Children over twelve years can obtain this card, but it is not mandatory for them to use it. At the age of fifteen it is mandatory for all residents to carry the card with them at all times. Both EU and non-EU foreigners living in Belgium can apply for an eID card as well. This card contains, besides the national emblem of the Member State and type of residence, the same information and features as a normal eID card.

eID card

The Belgium law states that all personal data on the card should be visible in any case so people are identifiable. Besides the visible information, the card contains a chip that contains all visible information. The chip is also required to use the electronic services. All the data on the card do come from the National Register of Belgium. Data such as surname, first name, date of birth, place of birth and national identification number (RRN) are listed on this card[3].

The RRN is unique to each resident and is composed of eleven digits. The first six digits are the date of birth (yy-mm-dd). The next three digits make up the daily count of the date of birth.

[3] De elektronische identiteitsdocumenten
`http://eid.belgium.be/nl/meer_weten_over_de_eid/de_elektronische_identiteitsdocumenten`

Odd digits are assigned to men and even to women. The last two digits are for verifying. This number is calculated by the first nine digits modules 97 and then subtracting the result from 97. For persons born in 2000 and later, a two is added to the nine-digit number for calculating the verifying digits[4].

Figure 4.1.1: eID card Belgium

The chip contains all visible data of the card and also the current address of the resident. Furthermore, the chip contains a few certificates and keys used for online services. The following certificates are stored on the card: Citizen's CA Certificate, Authentication Certificate, Non-Repudiation Certificate and the RRN Certificate [7].

This card uses PKI, as described in Section 2.1. The Citizen's CA Certificate is used with the Basic Key to show whether the card is authentic and is still valid. The Authentication Certificate and corresponding key are used to authenticate the user. During log in, the user must enter the PIN number which he proves that he indeed possesses the card specified identity. The Non-Repudiation Certificate and key are used to create digital signatures. For creating digital signatures the user also needs to enter a PIN number, but this one differs from the authentication PIN. For each digital signature the user needs to enter the PIN, where the authentication PIN only need to be entered once. The final certificate, the RRN Certificate, is used to verify the data of the card with that registered in the National Register (NR). This certificate is also used to change the current address.

When the user wants to use multiple services it is not necessary to authenticate separately for each service, since the eID system uses Single-Sign-On (SSO). At the first authentication a session is started. If the user switches of service the session is shared by exchanging credentials and the user is authenticated at the other service. It is not clear what data is exchanged when changing service. This could vary from only the necessary data to all data. Thus, the user does know immediately what happens to his data [18].

During a session, the data used by the services is invisible for the user, but users could see that afterwards. A user could request the data used by the services at the Federale Overheidsdienst foor Informatie- en Communicatietechnologie (FEDICT). FEDICT is responsible for the infrastructure of the online public services. With the request for information at FEDICT users could see what information is used by the services.

[4] Hoe zit de structuur van een rijksregisternummer in elkaar? `https://www.ksz-bcss.fgov.be/nl/bcss/page/content/websites/belgium/services/docutheque/technical_faq/faq_5.html`

Issuance Procedure

Every citizen of Belgium receives a request to renew the ID card when the end of the validity is almost reached. The resident must go to the town hall with this request, a new resembling photo and the current identity. When the identity card is lost, stolen or broken the resident should report it at the police station and a replacement document will be issued. This replacement document is then mandatory for issuing a new eID card. The civil servant at the town hall will verify the identity of the applicant by checking the documents and photo with the information known by the NR. When the identity corresponds a request for a new eID card is sent to the NR.

The NR receives and send the request to the party that makes and manages all cards. This party will print the eID card and generates the keys. The NR receives a part of the activation code for the card from that party. At the same time the CA, responsible for issuing and managing all certificates, receives a request for creating new certificates for the eID card. Not only the certificates themselves are made, the CRL is updated as well. All certificates that are no longer or not yet valid are listed on this list. The party responsible for making the eID cards will store these certificates on the chip of the card. Next, the personal data is stored on the card and the card will be deactivated. The party sends two letters holding the PIN numbers, part of the activation code and the message to retrieve the eID card at the town hall to the resident. These letters are sealed. When the seal is broken during transport, the resident must contact the town hall to request a new code.

At the town hall the civil servant begins the activation process when the identity of the resident is verified. The two parts of the activation code are used to activate the card and the certificates will be removed from the CRL. Next, the old identity card is handed in and destroyed[5]. The new card is ready to use [16, 17].

Authentication and Digital Signatures

To use the online services the user needs, besides the eID card, a card reader. This reader is connected to the computer. There are a variety of card readers are supported by this system. The first is a simple reader without a screen, where the PIN needs to be entered with the keyboard of the computer. The second and more advanced reader has a screen and keyboard on which the PIN has to be entered on the card reader itself. Some computers have built-in card readers where the PIN also needs to be entered on the computer itself.

Special software needs to be installed on the computer for the authentication and making digital signatures. This software is provided by the government. The user chooses a service they wish to use, the service asks the user to authenticate using the eID card [23]. The user must connect the card reader and enter the corresponding PIN. At a match, the user will be authenticated and may use the service, for example, online tax returns[6].

[5] Belgian eID Card Technicalities
`http://www.danishbiometrics.org/admin/files/belgian.eid.card.technical.overview.pdf`

[6] Uw online overheidsdienst `http://my.belgium.be/`

4.2 Estonia

History

Estonia became fully independent in 1991. During the period before tthat hey were still a apart of the soviet regime. This meant that Estonia used the identity system of the USSR until 1991. After gaining independence, they started to develop their own identity system. In 1992, the structure for this system was set [46]. Since that moment, Estonia has produced and distributed their own passports. In this system the Citizenship and Migration Board (CMB), a part of the Ministry of Interior, is responsible for managing the population register and the identity documents.

The passports issued in 1992 were valid until 2002. Estonia saw this as a good opportunity to introduce eID cards. This new identity card became the primary document for identification. This card was introduced in January 2002 [46]. Estonia is therefore one of the first European countries to introduce an eID card with an eID system.

In 2007, the government introduced Mobile ID. Mobile ID uses the same system, but a mobile phone is used as an authentication means in stead of the eID card. Mobile ID does not replace the eID card, since it may not be used as an offline identification means like the eID card. Only the online services may be used with Mobile ID. Furthermore, an eID card is required to activate Mobile ID.

Estonia is, after the early introduction of the eID card and Mobile ID, the first country to implement internet voting on a large scale [37, 59]. The eID card is used to authenticate and authorize users during the voting process. Since 2005, residents are able to vote via the internet. In the parliamentary elections in 2015 30.5% of all votes were done via internet[7].

eID card

The eID card has two functions: it serves as a physical identifier and as an authentication means to gain access to electronic services. The card is the primary identification document for people from the age of fifteen. Although compulsory, no penalties follow when someone does not have one [58].

The visible information on the card include name, photo, date of birth, gender, national identification number and the validity dates. This allows the owner of the card to identify themselves with. Example of the eID card is illustrated in Figure 4.2.1.

Figure 4.2.1: eID-card Estonia[8]

[7] Estonia Voting Statistics `http://www.vvk.ee/voting-methods-in-estonia/engindex/statistics`

[8] Estonia eID-card `https://www.politsei.ee/en/nouanded/dokumentide-naidised/identity-card/identity-cards-issued-since-01012011.dot`

In addition to the visible information, the card also includes a chip. The chip contains all visible information (except the photo and signature) of the card as two certificates with associated private keys and PINs used for online services. The first certificate is used for authentication and the other for digital signatures. A PUK code is also stored on the card, so that the PINs can be changed when the cardholder lost these codes.

Issuance Procedure

The CMB is responsible for the registration and management of the eID cards in Estonia. Producing the cards is done by the private party TRÜB Baltic AS. The third party in the production process is AS Sertifitseerimiskeskus. This is also a private party and is the CA that produces and manages all certificates [7].

IF a resident needs a new eID card, he needs to apply for a new one at one of the service centers of the CMB. The service center checks the provided information with the population register. If the data match, a request for a new card will be sent to the TRÜB Baltic AS. The TRÜB Baltic AS produces the card and personalize it with the applicant's personal data. Next, the TRÜB Baltic AS gives the command to generate the keys. This is done by the card itself, so the keys never leave the card. TRÜB Baltic AS will then create the PINs associated with the keys and a letter for the applicant is written with these codes.

After the production of the card and storing the keys and PINs on the card, the TRÜB Baltic AS sends a request for two certificates to Sertifitseerimiskeskus. One certificate is for authentication and the other for digital signing. The Sertifitseerimiskeskus creates these certificates, stores them in the database and sends them back to the TRÜB Baltic AS. These certificates are stored on the card and this finalizes the card production. The TRÜB Baltic AS sends the card and the letter to the service center of the CMB. At issuance, the identity of the applicant is checked once more and the card is given to him [58].

The card itself is valid for ten years, the certificates on the card three years. Sertifitseerimiskeskus made an application allowing users to renew their certificates from home. The card must therefore be connected to the computer using a card reader.

Authentication and Digital Signatures

The user must be in possession of an eID card, a card reader and a computer with the software given by Sertifitseerimiskeskus to use the online services. When installing the software, three programs are installed: ID-card utility, DigiDoc3, DigiDoc3 Crypto. The ID-card utility is used for authentication, updating certificates and changing the PINs of the card. For signing documents the other two programs are used. DigiDoc3 Crypto is used for encrypting the document and DigiDoc3 is used for securely sending the documents.

When the user wants to use an online service he goes to that website. The service will ask to log in using the eID card. The user needs to connect the card reader with the card reader and the ID-card utility will ask to enter the PIN for authentication. When the certificates are valid and the PIN match, the user will be authenticated and is able to use the service.

For digitally signing of documents DigiDoc3 is required. The user opens the client and selects the document that he wants to sign. The user will be asked to enter the PIN. When matched DigiDoc3 Crypto will encrypt the document using the private key of the card. After this the file is signed and can be sent securely using DigiDoc3. With DigiDoc3 digital signatures of others also could be verified.

Mobile-ID

In addition to the eID card residents have the possibility to use Mobile ID. Mobile ID utilizes a mobile phone for authentication and digital signing instead of the eID card, card reader and computer. All applicants must hold a valid eID card to apply for a Mobile ID, since it used during application and activation. The registration process of the mobile service providers is not found to be reliable and therefore the eID card is used for application and activation [46].

An applicant needs to submit an application at one of mobile service providers that support Mobile ID. There are three mobile providers that support Mobile ID in Estonia: Telia, Tele2 and Elisa[9]. Applicants will first have to sign a contract with the mobile service provider and identify themselves with the eID card. When the identity is verified, the card is valid and the contract is signed the mobile service provider will send a request for a new SIM card that is suitable for PKI. The Sertifitseerimiskeskus produces as with the eID card, two certificates for authentication and digital signatures. The PINs on the SIM card differ from those on the eID card. When the SIM card is sent to the mobile service provider when it is produced. At issuance, the identity of the applicant is verified with the contract and eID card. The SIM card is not activated when issued. This is done by logging in online at the site of the police and customs. The user logs in using the eID card and then follows the steps for activating the Mobile ID. After this procedure the user could use both the eID card as Mobile ID for authentication and creating digital signatures [58].

Authentication and Digital Signatures

To use the online services, the user goes, as with the use of the eID card, to the website of the service he wants to use. This could be done on a mobile phone or on a computer. Instead of choosing authenticating using the eID card, the users chooses Mobile ID. The user is asked for his personal identification code and his mobile number. A authentication message will be sent to the mobile phone. On the website a verification code will be shown. This will be shown together with the name of the service on the phone. This forms an extra check, since the user is able to verify that he is communicating with the correct service. The user enters the PIN for authentication and the phone will send a message to the service. By this the user is authenticated at the service.

Signing documents with Mobile ID does not differ much from signing these documents with the eID card. The user authenticates himself first. Second, he selects the document he wants to sign. Next, the application on the phone for signing will ask for the PIN of the user. When the PIN matches, the document is signed and will be sent to the service.

[9] Estonia Applying for a Mobiil-id `http://id.ee/index.php?id=36915`

4.3 Germany

History

It did take long before the eID card was introduced in Germany. This has to do with the historical background of the country. In 1876 the government took over the administration of citizens from the churches. Just before the Second World War, in 1939, the identity card with fingerprints was mandatory for all residents of Germany (and also for occupied territories). For Jews, there was an additional identifier that was used for deportation. After the war, there was much ado about the use of these identifiers and in 1981 the parliament and the constitutional court decided that an unique identifier may not refer to a specific person[10]. The serial number of the identity card/document, which uniquely refers to a person, may only be used by law enforcers [50].

A long time nothing happened regarding the development of the identity card. This changed with the rise of the internet for the general public. Official government documents were available publicly. However, these documents needed to be printed, signed and sent by letter, otherwise they were not legally binding. Germany then introduced a low in 1997 regarding digital signatures. By this law it is possible to send online documents that are legally binding.

After the introduction of this law, Germany launched the eGovernment program in 2000. This would ensure that all public services would be available online in 2005. This was not successful and therefore a second program was created in 2006. This program includes the introduction of the eID card in 2009. This ultimately lasted longer, since new laws needed to be formulated before the roll-out of the eID card.

In 2009, Germany accepted a law for the development of an eID card and eID system. In late 2009 they began with the first pilot. After eighteen months they introduced the eID card on November 1st, 2010 as replacement of the old identity card [45]. Since that date, the eID card is compulsory. Old identity cards which had not reached the expiry date remained valid. The entire process of the development of the eID system of Germany is shown in Figure 4.3.1.

[10] Act on Identity Cards and Electronic Identifiction
`http://www.gesetze-im-internet.de/englisch_pauswg/englisch_pauswg.html`

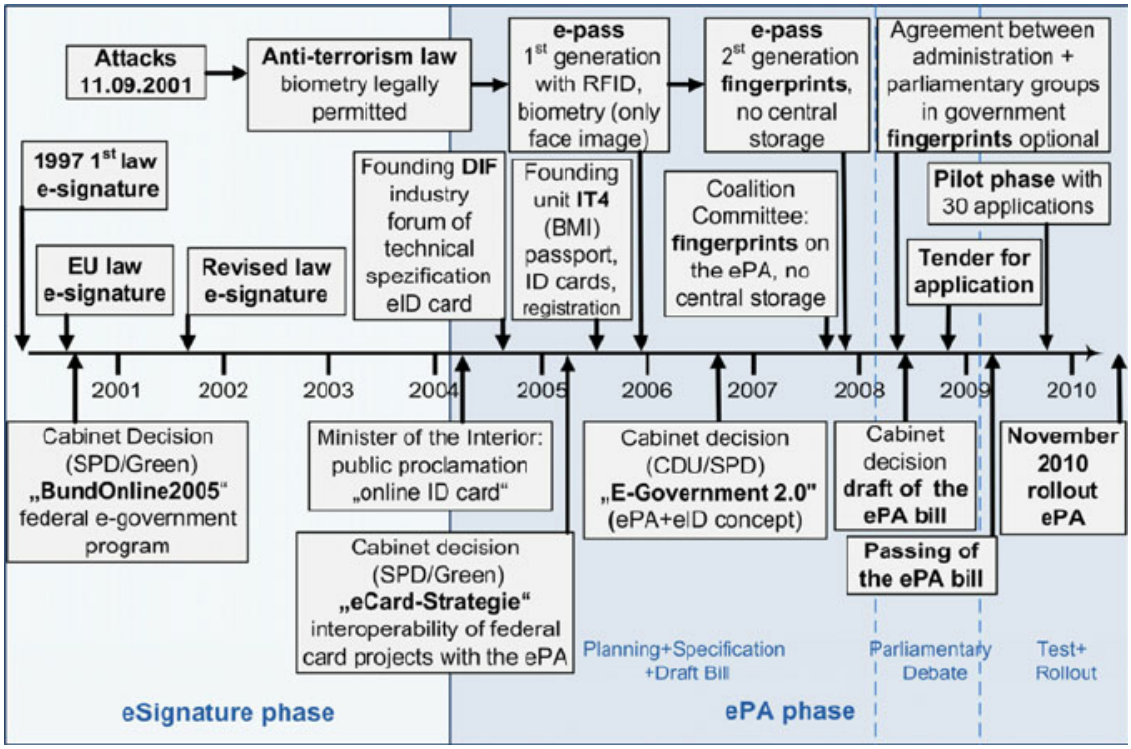

Figure 4.3.1: Development of the Online Authentication in Germany [50]

eID card

The eID card is the physical document used to identity residents. The card contains visible personal information, such as first name, last name, height, gender and the validity dates, just like the other Member States[11]. The German eID card aslo contains additional information such as eye color and doctorate [7, 20]. As previously indicated, identity cards do not hold unique identifiers, except for the serial number of the document. This number changes when a new card is issued.

The visible data of the card is also stored on the chip. Additional information such as current address and community ID are also stored on the chip. Furthermore, the certificate for authentication with the associated PIN is stored on the chip. The certificate for creating digital signatures is not stored by default and is sold separately [3].

Germany has a different version of the identity card. For children under sixteen it is possible to apply for an identity card without electronic capabilities. Children older than sixteen and adults always get an eID card. The validity of an identity card or eID card for people younger than 24 is six years. For residents older than 24 the card is valid for ten years[12]. In Figure 4.3.2 the German eID card is illustrated.

[11] BSI - The electronic ID card
`https://www.bsi.bund.de/EN/Topics/ElectrIDDocuments/eIDcard/eIDcard_node.html`

[12] Application `http://www.personalausweisportal.de/EN/Citizens/The-New-Identity-Card/Application/Application_node.html;jsessionid=2A61A0ADDFCD88F5B93282AB5F0D33F0.2_cid297`

Figure 4.3.2: eID card Germany

When applying for the eID card residents may store fingerprints on the card. This is on voluntary basis. These fingerprints are used for identifying and reduce the risk of identity fraud [8]. The fingerprints are stored at the office until the card is issued. Then they will be deleted, since the German law prohibits to store data of the identity cards.

Issuance Procedure

To renew the identity card, the resident needs to go the town hall. He needs to bring his current identity card and also a similar looking photo[13]. For children under the age of sixteen the application must be submitted by a parent or guardian. In the case of a first application, when the card is lost or when the information provided does not match the information in the population register, the applicant must prove his identity with his birth certificate.

When the payment for the new card is made, the identity of the applicant is verified and the application is signed, the civil servant sends a request for a new eID card to the Federal Printing Office (FPO). The FPO is responsible for producing the card. The FPO prints all data on the card and stores the data on the chip. The chip contains all visible information, bio-metric data, card serial number, key pairs, certificates, PIN and PUK codes and a code word to block the eID card. The code word is used when the card is lost or stolen. The PIN/PUK codes and the code word are sent via a stamped letter to the address of the applicant with the message that the eID card is ready for retrieval.

The new eID card is sent to the town hall where the application took place. At issuance the identity of the application is verified once more. When verified, the new card is handed over and the old identity card must be returned, this will be destroyed.

Digital Signatures Certificate

There is an additional requirement for creating digital signatures. By default the certificate required for these signatures is not stored on the chip. This certificate is only issued by one of the CAs that is under additional supervision of the government. The cardholder must purchase a certificate from one of these CAs before he may create digital signatures[14].

[13] Foto-Mustertafel `http://www.personalausweisportal.de/SharedDocs/Downloads/DE/Weitere-Informationen/Fotomustertafel.pdf?__blob=publicationFile`

[14] Accredited Certification Service Providers `https://www.nrca-ds.de/en/index_e.html`

Authentication

A cardholder chooses whether he wants to use the electronic capabilities of the eID card, since they are not mandatory. To use a electronic service, the user goes to the website of the service he wants to use. During the log in phase, a secure connection is set up when the appropriate software (AusweisApp) is installed. This software checks the card connection to the reader and whether the service provider and the eID card are authenticated. The user receives the certificate of the service provider, which the card verifies it is the right service provider. Additionally, the data of the service provider will be displayed when the user checks whether he is communicating with the right provider. During this step the user verifies which data is sent to the service provider. The user user enters the corresponding PIN to transmit the data. The data first goes to the eID server for verification and an authentication response. The service provider checks the information and complete the authentication [31].

Digital Signatures

As mentioned before, the user must be in possession of a certificate issued by an accredited CA. Moreover, a card reader which has its own keyboard and display must be purchased.

When someone has purchased a certificate from a CA, he will be sent a link which he can register himself with Sign-me. Sign-me is the web application that is required for creating digital signatures. The user logs in with the eID card and an authorization will be sent to the users home. When the authorization code is entered the user is able to create digital signatures.

To create digital signatures the user needs to authenticate himself through the AusweisApp at one of the service providers. After authentication, he signs documents using the Sing-me web application. As with the authentication, the user must enter a PIN to sign the document [24].

4.4 The Netherlands

DigiD[15] is the main authentication service for using online government services by citizens in the Netherlands. In the online service of the government it is essential to verify the identities of users. Through this service citizens enter, for example, their online tax returns. For organizations there is eHerkenning to do their business with the government online.

DigiD

The development of DigiD began as a result of the Action Plan 'Andere Overheid' [53] in 2003. This action plan is designed to improve the services for citizens with the government. The government saw that ICT could play a very important role and therefore the development of a system such as DigiD is required. Moreover, the service will be extended through the use of ICT to 24 hours a day, seven days a week, which makes for greater ease of use.

To apply for DigiD the applicant must go to the DigiD website. Upon registration, the applicant is asked for his social security number (BSN), date of birth, postal code and house number (and addition). This data is checked with the data in the population register. Additionally, a user name and password must be chosen. Users may specify a mobile number to which a transaction code is sent during the log in process. As a result, an additional authentication factor is added to the log in process. Using multiple authentication factors reduces malicious use of your identity. Explanation on the use of one or more authentication factors is described in Section 5.3. For some government services it is obliged to make use of this additional authentication factor, for example, Dienst Uitvoerend Onderwijs (DUO). For others, for example, Mijnoverheid.nl user name and password suffice.

After the application the applicant will receive an activation code within five working days at his address. At the first log in attempt (with user name and password) the applicant will be asked for his activation code. When correctly entered, the account will be activated and the user may use various services of the government. If the user has selected for the SMS-verifier he needs to log in with his user name/password and the authorization code sent by SMS.

In 2018, the Dutch government wants to allow citizens to authenticate through their driver's license or ID card [39]. This should eventually replace the use of user name and password. The advantage of using a driver's license or identity card is that always two authentication factors are used. Furthermore, the identity of a person is more often verified, since its verified during application/registration, issuance and renewing. This ensures that the card is used by whoever it belongs.

eHerkenning

The Dutch government started with developing eHerkenning with a number of private organizations[16] in 2009. This system ensures that organization can easily use various services of the government easily and/or organizations affiliated to eHerkenning. Users no longer need to log in at each service separately. Moreover, this ensures that multiple services can be used without requiring separate authentication means.

To provide a level of assurance regarding privacy, security and reliability eHerkenning uses level of assurances that are similar to that used in this research. The level of assurances is based on the STORK project and the ISO27001 standard[17]. The ISO27001 standard is a standard in the

[15] **Digitale Identiteit (DigiD)** www.digid.nl
[16] eHerkenning `https://www.eherkenning.nl/nl/over-eherkenning/ontwikkelingen/`
[17] ISO/IEC 27001 - Information security management `http://www.iso.org/iso/iso27001`

field of information security. All organizations that participate in eHerkenning must be ISO27001 certified.

Application eHerkenning Authentication Means

To apply for an authentication means at eHerkenning an organizations must first make an inventory of all employees who need eHerkenning and what the risks are. Then they have to see what services they want to use and what the desired level of assurance is.

At the lowest level of assurance less sensitive information is exchanged and the use of a user name and password will suffice. At a high level of assurance, the potential damage from abuse is much higher and a user name and password is not sufficient. The service that will be used will determine which information is exchanged and whether it is important to use a high level of assurance. Furthermore, the registration and authentication process for each service and level of assurance varies. At a low level of assurance, a copy of a passport will suffice during the registration process, while at a high level of assurance a verification by physical characteristics is mandatory. After the personal verification the authentication means will be issued. For the lowest levels a confirmation email will suffice, while at a high level, the means is sent by a registered letter or need to be retrieved at the authentication provider.

Idensys

The Dutch government began drafting a plan in 2013 to create a standardized platform for authentication and authorization [65]. The aim is to combine multiple authentication services, so users may use multiple services without the need to remember multiple user names and passwords or authentication means. The government wants to create a *'future-proof and reliable electronic identity infrastructure that can be used by both public and private service providers and is public-private developed and managed'* [47].

The government wants to merge private services (web shops etc.) with public and public-private services. DigiD is an example of a public service and eHerkenning of a public-private one. These two services will be the first two big authentication services.

The solution of the Dutch government differs from other Member States. Whereas other countries often choose for one authentication method, the Netherlands chooses for multiple ones. This provides for greater convenience; the user chooses with which method he authenticates himself with. At each log in users have the option to use the service as a private person, a professional or as a organization.

The government has also examined whether it was possible to introduce a separate eID card, but this was not feasible. The costs were too high and it would take too long to develop this card and implement it. The Minister of Interior therefore did stop with the eID card in 2014[18]. In 2015 the government introduced Idensys and then began with several pilots. These pilots would have run until the end of 2016, but at the moment of writing they are not finished. The ambition of the Dutch government is that citizens and organizations in 2017 do all their business with the government online. Idensys is the point of focus in this goal. The government wants to create a reliable platform where identity fraud is prevented. Before we discuss how Idensys works, we will give a brief explanation of some key terms used in this system.

[18] Kamerbrief over eID Stelsel en DigiD-kaart
`https://www.rijksoverheid.nl/documenten/kamerstukken/2013/12/19/kamerbrief-over-eid-stelsel-en-digid-kaart`

Pseudonym A name/alias someone uses instead of their real name.

Master Data A set of personal information that is unique to a user consisting of, inter alia, first name, surname and place of birth. These personal data are found on the identity document. This data is used to create a Polymorphic Pseudonym.

System Authority (SA) The trusted third party in the system that makes the PP and keys with which EPs and FPs can be created. In Idensys the government fulfills this role.

Polymorphic Pseudonym (PP) A pseudonym that is made by the system authority, and which is issued to the authentication services. The properties of a PP are that it is specific for a user and an authentication service, and can be randomized without having an effect on the Final Pseudonym. A PP is derived by making use of the Master Data and the public key of the authentication service.

Encrypted Pseudonym (EP) An authentication service encrypts the PP using the identity and public key of the service provider. This results in an EP. An EP has the properties that it can be randomized and that it only can be decrypted by the service provider.

Final Pseudonym (FP) The EP is sent to the service provider, which it decrypts it with its private key. The results in the FP. It does not matter which authentication service is used; the FP will always be the same for a user for a particular service.

In Idensys there are four parties that play an (active) role; the user, the service providers, the authentication providers and the government (System Authority). In addition there is the Central Information Point eID Investigations (CIPEI) that initially plays a less active role. The department may seek abuse of the system, but is not relevant in the context of this research.

Authentication

When one wants to use a service within Idensys, the user is redirected to the authentication service. If the user tries to log in for the first time, then the authentication service will request a new PP from the SA. The authentication service will provide a set of personal information of the user to the SA, such as family name, first name, other initials, date and place of birth. These data are checked by the SA with the aid of the personal data stored in the Basisregistratie Personen (BRP), which is the population register. If these data are unique, then one BSN will be found. It may occur that there emerges a plurality of BSNs. In that case, the user must supply more data to achieve a unique hit, such as the card number of an identity card. The unique data form the Master Data.

The BSN is not used to create a unique PP, but only to show that the data refer to a unique BSN, which means it also refers to a unique person. The Dutch Law imposes strict requirements on the use of a BSN. An organization that uses the BSN, must always demonstrate the legal basis for the use of it. Not all organizations involved with Idensys can prove this, therefore, the BSN is not used for creating the key for the PP.

The Master data are used to derive a PP. For this, a hash value is calculated from the Master Data and the public key of the authentication service. Together this data is encrypted with a random exponent and the private key of the SA forms the PP. For each authentication service a separate PP is generated. The PP is then stored by the authentication service, so at the next log in attempts the user will not have to reapply for a PP.

The PP has the quality that it can be randomized, without having any effect on the FP. For example, additional data can be added, so that another PP is emitted, but the resulting FP

remains the same. This means that it does not matter which authentsication service/-means is used, the FP will be the same for the user and service provider [66, 72].

When the authentication service has received the PP for the respective user, the service will use different private keys to encrypt the PP to an EP. The first key is used to transform the PP into the domain of the service provider. The other key is used to encrypt the PP to an EP. The last step included the identity and the public key of the service provider are used.

The service provider then receives the EP of the authentication service and decrypts it with two keys; one key to decrypt the EP and one to transform the EP to the FP. After this last step, the user is successfully logged in at the relevant service provider. To summarise, the following specifications apply on Idensys [29, 66, 72]:

- It is not possible to retrieve personal information from a pseudonym.
- An FP at a service provider is always the same for a user.
- Only a service provider can create a FP.
- An authentication service can not decrypt EP's.
- FP's of the same user at different service providers can not be linked.
- EP's of the same user at different authentication services can not be linked.

The full description of the used cryptography in Idensys is written in [66].

Criticism

Recently, Hoepman (associate professor Radboud University) wrote a column about Idensys[19]. In this column he questioned the security of Idensys. Idensys is a so-called federated identity management system. The user has an account at an authentication service and the service provider refers to the authentication service, rather than that the user has an account at a service provider. The user logs into the authentication service, and if this successful, authentication data is sent to the relevant service provider and the user is authenticated at that service. In Idensys uses DigiD and eHerkenning (and possible others on a later moment) as their authentication service.

Hoepman states in this column that the user of these systems, especially Idensys, ensures that the third party knows too much about the users. For example, it is possible to sign in to Spotify using a Facebook account. This ensures that the user only needs one account for multiple services, but the authentication service (Facebook in this example) sees which services the user uses.

Verheul (Radboud University professor) wrote a response to this column[20]. He states in this response that authentication services in both non- and federated systems essentially do not differ much from each other. Both use a trusted third party. Hoepman responded that it is safer to use tokens, smart cards, smart phones or a laptop[21]. These examples still use a third party, but only as creator of the authentication means. The authentication service does not play a role in the system after issuance.

In Idensys users are authenticated by an authentication services with their associated authentication means. When the authentication is succesful, the user is sent back to the service he wants

[19] Wilt u af van de authenticatie-pooier?
`http://blog.xot.nl/2016/02/10/de-authenticatie-pooier-onder-de-loep/`

[20] Reactie column "Wilt u af van de authenticatiepooier?"
`https://www.cs.ru.nl/E.Verheul/presentations/Reactie_column_FD.pdf`

[21] De authenticatiepooier onder de loep
`http://blog.xot.nl/2016/02/10/de-authenticatie-pooier-onder-de-loep/`

to use. The role of the authentication service is much greater than in the case when the third part only issues the authentication means. The third party now knows which services a user logs into. Verheul therefore indicates that in the situation in Idensys this 'problem' can be solved by using PP. These PP's are then stored on, for example, a smart card. *The authentication service would be able to operate between the user and service provider without being able to determine the identity of the user.* Matto, J.H. et al. [47] indicates that this solution would add to a level of privacy protection based on the principle of data minimization. They also state that it is not possible in this example to see what use is made of the authentication means. This increases the risk of the reversal of the burden of the person concerned in the event of misuse of the authentication means, if an audit trail is not maintained. Moreover, in Idensys only a PP is used when the user chooses for the highest two level of assurances [67]. This means that at the lower levels the authentication services will find more about the use of services by the user.

4.5 Spain

History

Spain presented the plan 'Info XXI Initiative'[22] in 2000. This plan focuses, among other things, on the development of eGovernment. The key was that residents would do their business with the government over the internet. This plan mentioned the eID card for the first time. The set-up of the technical framework had already finished in 2002, only a few years later the eID card was introduced [30]. This was because there was no funding for further development and production, which changed when in 2004 a new vice president was appointed and provided a boost for the introduction of the eID card [2]. She approved the new plan for the financial and technical resources. This resulted in the deployment of the eID card in 2006. After a year, 1.5 million residents possessed the new eID card. In 2010, all public services were made available online.

eID card

The eID card is mandatory for all Spaniards from the age of fourteen and is valid for a period of ten years. This card shows all personal data such as name, date of birth, height, gender and personal identification number. This number consists of eight digits and a character verification. This character is calculated using modular arithmetic. In Spain the digit 23 is used; this is the amount of characters in the Spanish alphabet without the i, o, u and ñ. The digit after the modular arithmetic is between 0 and 22. The character associated to one of these 22 characters are listed in Table 4.1.

There are 100 million possible combinations for this identification number. This would be no problem on a population of 47 million, only these combinations are not used anymore if the resident in question has passed away. Spain currently issued 56 million unique combinations, but will have to come with an alternative to term. In the current situation, each municipality receives a series of combinations which they may issue. If this series runs out, they receive another random sequence.

Table 4.1: Verification Identifier

0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**
T	R	W	A	G	M	Y	F	P	D	X	B
12	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**	**21**	**22**	
N	J	Z	S	Q	V	H	L	C	K	E	

[22] El Plan de Acción INFO XXI `http://www.acta.es/medios/articulos/cultura_y_sociedad/027059.pdf`

Besides the visible information the eID card also has a chip. The chip contains all the personal data of the resident with photo, the handwritten signature and fingerprints. Furthermore, the chip has three certificates with associated private keys. One certificate is used for authentication, the second for creating digital signatures and the final certificate is of the CA [7]. The data on the chip is stored in three different 'Areas'. On the 'Public Area' the certificate of the CA is stored and this area is accessible to anyone. On the 'Private Area' the certificates for authentication and digital signing are stored. These are protected by a PIN. The last area, the 'Security Area', contains all personals data. Access to this data is only possible at a police station. This information is not used for online services. There is a dedicated eID reader at a police station with which some personal data can be changed and where the certificates can be updated. Only the rightful cardholder is able to change his data or update the certificates, since the data is only accessible using the fingerprint scanner on the card reader. Information as address could be changed on the card. The certificates on the card expire after 30 months and must be renewed in this manner and must be done a few times, since the card is valid for ten years.

Figure 4.5.1: eID card Spain[23]

Issuance Procedure

Whereas in many countries residents go to town hall if they need a (new) eID card, in Spain they must go to the police station. At the first application, residents must bring a copy of their birth certificate, two similar looking photos and a certificate of registration with the municipality. When renewing only the photos are required, unless the person has moved. At the police station the identity of the resident will be verified with the provided information and the data known in the population register.

When personal information (name, surname, gender) is changed, a new birth certificate must be submitted to prove the changes. If everything is correct, the card will be produced. This is done at the police station itself. The application and issuance of an eID card therefore takes about half an hour [25, 30].

[23] eID card Spain source:
`https://www.dnielectronico.es/PortalDNIe/PRF1_Cons02.action?pag=REF_100&id_menu=[1]`

Authentication and Digital Signatures

To use the online services, the user must be in possession of the eID card, a certified ISO7816 card reader[24] and a computer with the drivers provided by the Cryptographic Service Provider (CSP). The user then goes to the service in question and tries to log in. The services sends an authentication message and the users checks the message and whether the certificate of the service is valid. After a positive result, the public key of the service is used to encrypt the session. The user then uses the card with the card reader to authenticate himself. He does this by entering the PIN code of the card for authentication. The service checks whether the user's authentication certificate is valid. When this is the case, a secure connection is established and the user may use the service [7].

For creating digital signatures, the user must be authenticated. Then he selects the document he wants to sign. The installed software asks for the PIN code to sign the document. When the PIN code does correspond, the document is signed and is send to the service.

Cl@ve

It is not necessary to use the eID card for online services of the government in Spain. Spain developed an platform called 'Cl@ve' which enables to use the services with other authentication services. This platform provides identification, authentication and digital signing[25].

Spain developed this system, since there were many different systems for the services of the government. The eID card could, for example, be used for tax returns, but not for other services. The users needed to install several applications and remember various codes. Cl@ve connects different systems, including private systems, where the user chooses at which authentication service he wants to sign in. Cl@ve claims that is is prepared for STORK, allowing authentication systems of Member States to connect easily and use the services offered by Spain.

[24] Cuerpo Nacional de Policía `http://www.dnielectronico.es`

[25] STORK2.0: Cl@ve `https://www.eid-stork2.eu/index.php?option=com_k2&view=item&id=2078:clave_spanish_public_services&Itemid=130`

5. Classification

This chapter offers a classification of the systems based on the LoAs of various categories. A LoA indicates the degree of certainty or reliability of an eID means. There have been several projects to classify eID systems whose STORK [32] is probably the best known example. The ISO/IEC organization made an international standard [33] classifying such systems. This standard is among other things based on the data of the European Network and Information Security Agency (enisa), which is in his turn based on the data from, inter alia, the STORK-project. Subsequently the EC created a Regulation based on the STORK-project and ISO-standard. A Regulation is a legal act and is immediately enforceable in the EU Member States. The 910/2014 Regulation seeks *'to enhance trust in electronic transactions in the internal market by providing a common foundation for secure electronic interaction between citizens, businesses and public authorities, thereby increasing the effectiveness of public and private online services, electronic business and electronic commerce in the Union'.*

The Implementation Regulation 2015/1502 contains the minimum technical specifications, standards and procedures to enhance that trust. The LoAs formulated in the Regulation are used to classify the eID systems. With this, the EC wants to create the right conditions for mutual recognition of systems, which allows the use of critical facilities. A more detailed description of the Regulations is described in Chapter 1.

Chapter 3 describes the method used for the classification that is done in this chapter. Per chosen category the step-by-step plan will be given for the determination of a LoA. Furthermore, a summary will be given per Member State followed by an overview of the results of the classification. The chosen categories are 'Application and Registration', 'Identity Proofing and verification (natural person)', 'Electronic Identification mean characteristics and design', 'Issuance, delivery and activation', 'Suspension, revocation and reactivation', 'Renewal and replacement'.

5.1 Application and Registration

The category Application and Registration concerns the applications of the electronic means of authentication. It is important that the user is informed of the recommended safety precautions and general conditions. Moreover, the correct personal information should be collected for authentication. Figure 5.1.1 describes the requirements associated with the LoAs.

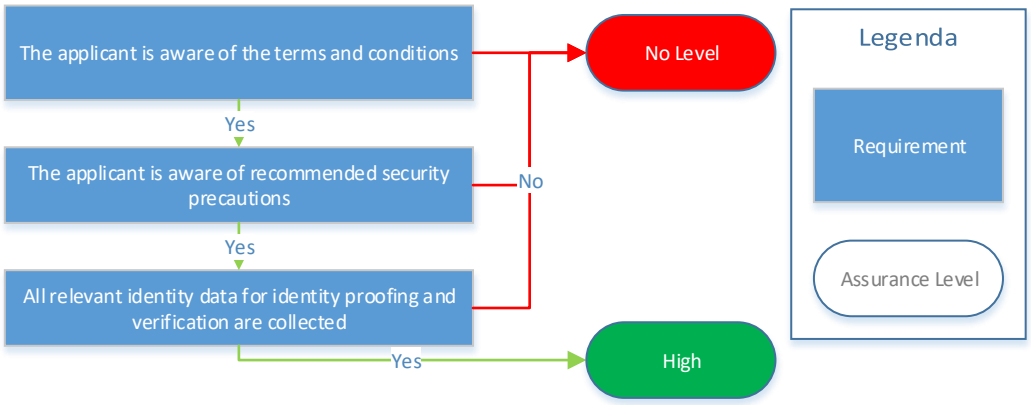

Figure 5.1.1: Flowchart Application and Registration

Belgium

In Belgium, a eID card is used that also functions as an identity card. The card is therefore obligatory for every occupant. The general conditions around the offline use, for example, identifying at the request of the police, are well known. In order to use the online functions of the card the applicant must sign a form during the registration process. Furthermore, the application should go to the Belgian eID website[26] to activate the card before the online capabilities may be used. This website identifies the specific hardware and software the user needs to use for the online features.

To possess a eID card (or renew one) the resident must bring a resembling picture and possibly the old identity card. The submitted information is then checked with the data in the population register. When a match is found a request to produce a new eID card with the new information is sent. The cards for children also have the option to save phone numbers so that parents can be called in case of emergency. We conclude that Belgium meets all requirements and therefore is classified as High. The data and the used coding are specified in Appendix C.2.

[26] Belgische eID-website `http://eid.belgium.be/nl`

Estonia

The eID card in this country is mandatory for each resident and also serves for offline identification. When registering, data such as name, gender, date of birth, place of birth, address, marital status and personal identification are verified with the population register. At the first application, renewal or replacement, the applicant must provide this information.

At the launch, Estonia paid a lot attention to the promotion, support and acceptance of the eID card. Three sites have been set up for users to look up additional information. General information on the eID card and the services that are accessible using the card are available at `http://www.id.ee`. Information regarding the application is listed on `http://www.pass.ee`. On `http://www.sk.ee` information concerning the technical infrastructure is found. Estonia also launched programs to promote the use of the card, for example, a mobile eID bus, eID stands in shopping centers, courses for beginners and experts to ensure that people (especially the elderly) will make more use of the internet and e-ID card. In addition, a 24/7 help desk is accessible. This resulted more than 50% of the population of Estonia had the new eID card in 2005. In 2016 it was almost 100%.

Residents also have the possibility to use Mobile ID in addition to the eID card. Using the phone should increase the ease of use, as it is possible to use various services without required to use a computer and card reader. For this, applicants must sign a separate contract with a cellular provider.

Based on the measures taken by Estonia, every user is aware of the general conditions and the recommended safety precautions. These also are available online where users also must obtain the necessary software to use the electronic capabilities of the eID card. Estonia fulfills the requirements for level Low, and thus also for Substantial and High.

Germany

At first registration or at renewal when the data do not match those in the population register the resident must prove his identity through his birth certificate. Next, the personal details of the birth certificate will be registered in the population register. When renewing, the data of the existing eID card and the person's identity are verified with the population register. Furthermore, an applicant should bring a resembling picture that will be stored on the card. Residents can choose to put their fingerprints on the card. This is on voluntarily basis.

When registering the applicant receives a information note about the new features and the possibilities of the eID card. Upon issuance of the eID card, the cardholder chooses whether he wants to use the electronic capabilities, this is not mandatory. At any later time, it is also possible to have these capabilities activated or deactivated. This needs to be done a the town hall. If the resident chooses to activate the electronic capabilities on a later moment, a fee must be paid.

In order to make use of the electronic capabilities of the card, the cardholder must purchase a card reader and install special software. The necessary software is obtainable from `http://www.personalausweisportal.de/`. In addition, this web site contains all information about usage, applications and safety precautions. To create digital signatures the card holder must complete several additional steps, as a separate certificate should be put on the card. These certificates can be purchased from one of the certified CAs. In addition, they need to be purchase a "deluxe reader" which is capable for making digital signatures.

Based on the above it is assumed that the user is aware of the general conditions and safety precautions for the use of the eID card. Germany is classified as at level High as LoA.

The Netherlands

The application at Idensys depends on the authentication service and means selected. We will make the distinction between the application of DigiD and eHerkenning.

The application of DigiD is done online. At the first registration the applicant is asked for his BSN, date of birth, postal code and house number. This combination is checked with the population register. Next, the applicant must choose a user name and password. A number of security requirements appear when applying, for example, a password needs to contain a small and capital letter, a number, a special character and needs to be atleast eight characters long. If the data have been verified, an envelope will be sent to the home of the applicant. The combination address and BSN must correspond with the one known in the population register. This envelope holds the activation code for the account and a supporting envelope with information on how to use the account. Furthermore, the general conditions and safety precautions are available at `www.digid.nl`. It is assumed that users are informed of the general conditions and safety precautions.

The application process at eHerkenning depends on the chosen LoA. Applicants must identify beforehand which services they want to use, what LoA satisfies them and what the associated risks and potential damage could be. When the lowest LoA is chosen, only the identity of the applicant and the relationship between the applicant and his organization is checked with the register of the Kamer van Koophandel (KvK). The potential damage is lowest at this level. When choosing the highest LoA the applicant's personal data are checked with his identity card and a verification of biometrics takes place at the authentication service. In addition, the means of authentication varies per level. The potential damage is small at the lowest level; a user name and password would suffice. At the highest level multiple authentication factors are used, such as using one-time password token or via SMS.

The users are always informed of the general conditions and the recommended safety precautions at eHerkenning, since a conscious choice must be made. They should undertake a risk assessment in advance to determine what services are needed and what the risks and potential damage could be.

We conclude that the Netherlands meets all requirements and therefore is classified as at level High as LoA.

Spain

Spanish residents must report to one of the police stations for all applications on eID cards. Both the first application as a renewal the applicant should bring a valid birth certificate, which can be requested at the town hall. This certificate is valid for three months. Within that time, the applicant must request an eID card. The applicant must also be submit two resembling photos. Then all data will be checked with the population register.

For online authentication, the resident must purchase a card reader and install its software. This software is not included as standard, but can be found on `http://www.dnielectronico.es/` together with further explanations. The website provides all information on application, installation, safety regulations and general conditions. Therefore we assume that residents are aware of the general conditions and the recommended safety precautions.

Spain complies with the requirements of levels Low, Substantial and High and will therefore be classified at High as LoA.

Results Application and Registration

What stands out in all the examples discussed is that users have to perform deliberate actions before they can use the electronic capabilities. This happens, for example, when they are asked to install special software. Most Member States make use of the eID card, which ensures that the identity of the applicant is always verified with the population register. As a result, all the relevant data is collected. In the case of the Netherlands, The DigiD information is also compared with that in the population register, but there is no verification of bio metrics like other Member States also offer. The information of the population register is then used to send an envelope to the address of the applicant in order to activate the account. eHerkenning differs at the gathering of data per LoA. The higher the loA is, the more is asked for personal information. Moreover, one must identify himself to the authentication service with their identity card.

In the table below the results are displayed for the category application and registration of the electronic means.

Table 5.1: Results Application and Registration

Country	**Low**	**Substantial**	**High**
Belgium			x
Estonia			x
Germany			x
The Netherlands			x
Spain			x

5.2 Identity proofing and verification (natural person)

The category Identity proofing and verification (natural person) concerns the requirements for determining and verifying a person's identity when applying for the authentication means. For verifying the identity of an individual, it is important what evidence is provided and how these are checked. Figure 5.2.1 describes the requirements associated with the LoAs.

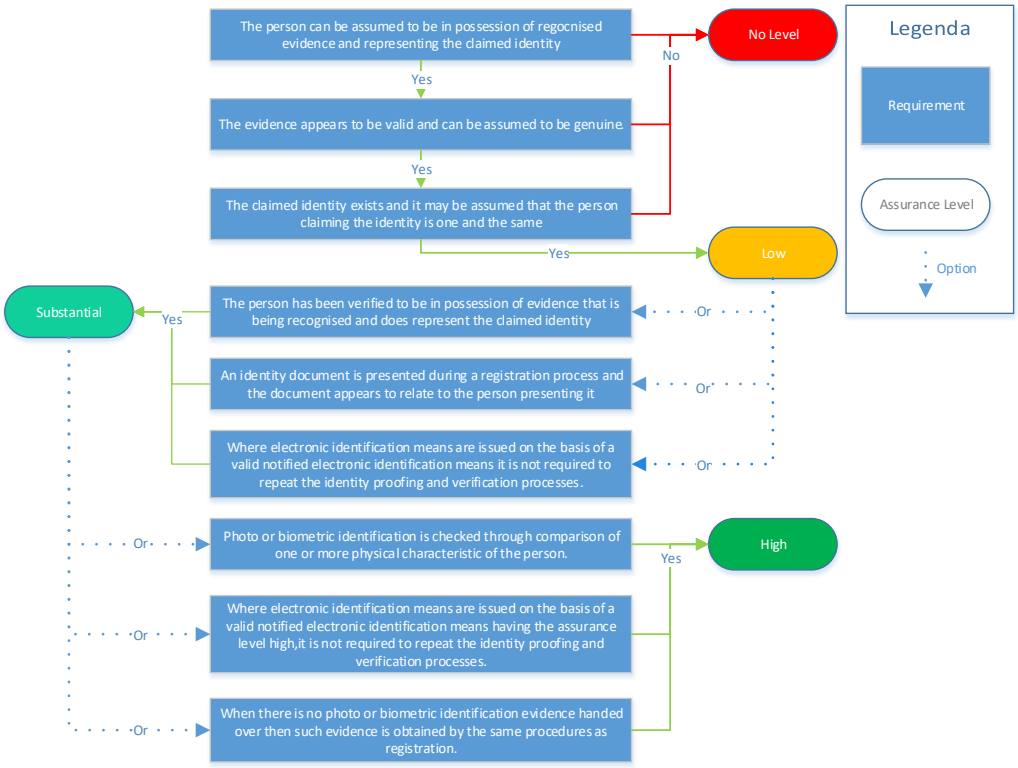

Figure 5.2.1: Flowchart Identity proofing and verification

Belgium

When applying for a new eID card the applicant must prove his identity. Each citizen receives a request to renew the identity card when the end of the expiration date approaches. This citizen must go to the town hall with the request, a new resembling picture and the current identity card. The civil servant then checks the person's identity by comparing the physical characteristics with that stated on the old identity card and the information in the population register. If the identity card is lost, stolen or broken the applicant should request for a replacement document at the police station. This document should then be taken with them to obtain a new identity card.

There are two options when requesting a new eID card: an old (valid) (electronic) identity card or a replacement document issued by the police is handed over. Next, the identity of the applicant is verified by comparing the physical characteristics to the document handed over and

the data in the population register. Through these audits, Belgium fulfills the requirements of Low, Substantial and High, since the identity is checked with the population register and the authenticity/validity of the identity card handed over is checked. The data and coding used for the classification, are listed in Appendix C.3.

Estonia

The eID card is the primary identification document of residents and foreigners living in Estonia. To come in possession of an eID card, the applicant must fill out a form at the service center of the CMB. If the applicant is in possession of a valid identity card and the identity of the applicant will be verified with the card and the information in the population register by comparing physical characteristics. This clarifies that the supplied documentation is valid and that the person is indeed who he says he is. Only an identified and verified person can complete the registration for an eID. After identification, the card is getting produced. The applicant gets an envelope sent home with the announcement that the card can be retrieved. When picking up the eID card the person's identity is again verified through a comparison of physical characteristics.

Residents also have the opportunity to apply for Mobile ID when they are in possession of a valid eID card. Applying for Mobile ID is done at one of the mobile service providers. The identity of the applicant is compared with that on the eID card shown in the application by comparing physical characteristics. When matched, the mobile service provider submits an application for Mobile ID based on the data of the eID card. The new SIM card is produced and the applicant will get an envelope sent home to retrieve the SIM card. Upon issuance, the identity is verified by the data on the SIM card and the eID card. Through these audits, Estonia fulfills the requirements of Low, Substantial and High.

Germany

When renewing the eID card, the applicant must be in possession of a valid eID card. At the town hall, the civil servant will verify the applicant's identity using the eID card and information in the population register by comparing physical characteristics.

At first registration or if the information does not match with the population register, the applicant must prove his identity by his birth certificate. This data is then stored in the registry. Through these audits, Germany fulfills the requirements of Low, Substantial and High, since the identity is checked by comparing physical characteristics when applying for a identity card and a valid identity must be handed over.

The Netherlands

The basis of Idensys lays in DigiD and eHerkenning. DigiD is exclusive to residents of the Netherlands. The DigiD application takes place entirely online. Applicants must enter BSN, date of birth, postal code and house number. The combination of this data is verified using the data known in the population register. The applicant is then prompted to enter a user name, password, email address and optionally a phone number. When this process is completed, an activation envelope will be sent to the address provided. This process verifies that the identity specified exists in the population register and the postal code and house number matches, and no account exists for this identity. There is no verification to compare the identity of the applicant with the information submitted in the application. Thus, DigiD only meets the requirements of the level Low.

In the application process of eHerkenning identity proofing varies for every provider, LoA and the chosen authentication means. The identity of the applicant is checked by the relationship between the applicant and his organization with the information in the KvK-register at the lowest LoA. At the two highest levels a identity document must be submitted. At the location of the authentication service the identity of the applicant is verified by comparing physical characteristics of the person with that displayed on the identity card. Moreover, the relationship of the applicant and his organization is checked according to the KvK-registration.

There are major differences in the verification of one's identity in the Netherlands. At DigiD only the specified data is checked with the population register, but there is no verification of the applicants identity, so the data provided and the identity of the applicant are the same. At the lowest LoA of eHerkenning, there is also no verification of the applicants identity to see whether the provided corresponds. When one of the lowest LoAs are chosen, there will be a more thorough identification. The identity of the applicant is verified with the information on the identity card provided in the application process by comparing physical characteristics. At the lowest eHerkenning will be classified at Low, since it does not meet the requirements of Substantial and High. The highest LoAs of eHerkenning Netherlands is classified to High.

Idensys uses both eHerkenning and DigiD as authentication services and will therefore be classified at the lowest LoA of the two services. In this case, that is DigiD and thus Idensys are classified at Low as LoA.

Spain

Obtaining an eID card in Spain is only possible if the applicant holds a valid birth certificate. At renewal the old (valid) eID card should be handed over. At the police station, the submitted documents (eID card, photos and birth certificate) are checked whether they correspond to the identity of the applicant and the population register by comparing physical characteristics. When this is the case, the card can be produced. The card is produced right away and given to the applicant. Spain fulfills the requirements of Low, Substantial and High, since the identity of the applicant and the validity of the eID card are checked with the population register.

Results Identity proofing and verification (natural person)

All countries except the Netherlands fulfill the requirements of Low, Substantial and High, because that is due to the fact that they all use an eID card with which the identity of the applicant is always verified by comparing physical characteristics with the identity card provided and the population register. In the Netherlands, the requirements of High are met when at eHerkenning is chosen when one of the highers LoAs is chosen at eHerkenning. Netherlands will now be still classified to Low, since DigiD does not meet the requirements of Substantial or High. In the table below the results are displayed for determining and verifying a person's identity.

Table 5.2: Results Identity proofing verification (natural person)

Country	**Low**	**Substantial**	**High**
Belgium			x
Estonia			x
Germany			x
The Netherlands	x		
Spain			x

5.3 Electronic identification means characteristics and design

Category Electronic identification means characteristics and design concerns the protection of the eID means against abuse by others. An important part of that protection is determined whether one or more authentication factors are used. By using several factors during the log in process reduces the chance that an attacker takes over your identity. Using multiple authentication factors means that one's identity is verified by means of a combination of factors: something you know, such as a password or PIN; by something you own, such as a smart card; by physical characteristics, such as finger prints.

The Figure describes the requirements associated with the LoAs.

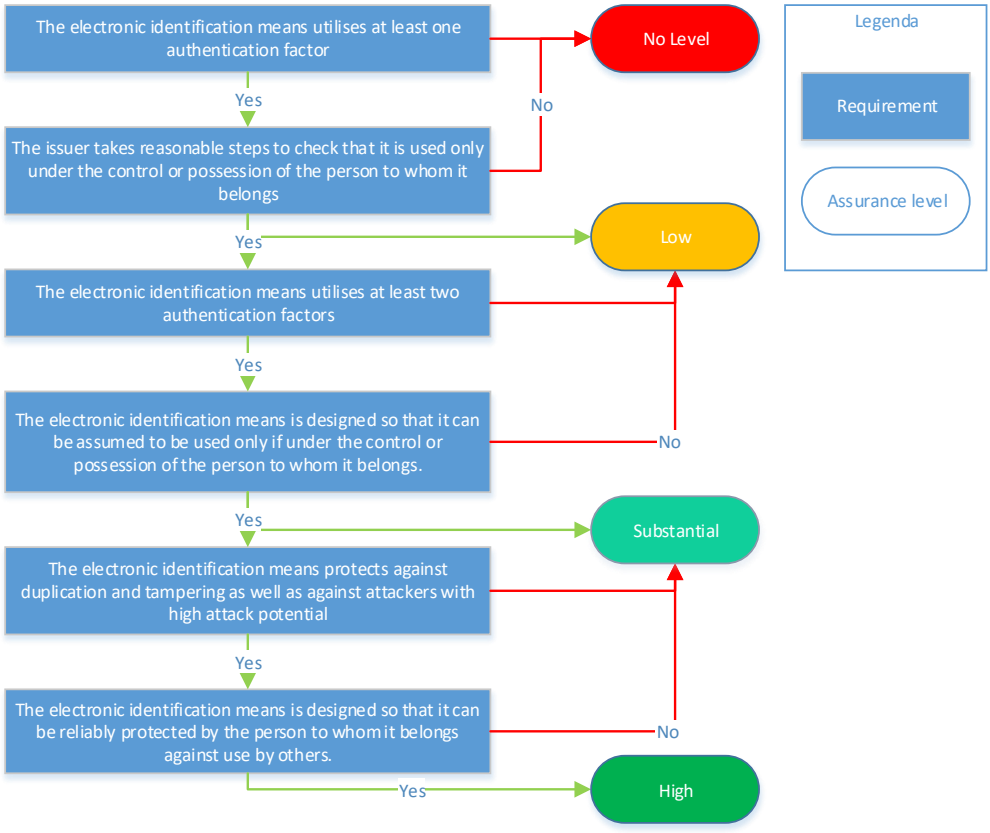

Figure 5.3.1: Flowchart Electronic identification means characteristics and design

Belgium

Belgium uses an eID card. This authentication method uses two authentication factors. The card (something you own) must be used in combination with a PIN (something you know) to log in. This means the card will only be used by the person to whom it belongs, since the card is only issued to that person. This is done by comparing physical characteristics described in Section 5.2.1. The PIN codes are sent in a sealed envelope to the address entered in the population register. Furthermore, the private keys used for authentication are stored on a secure part of the chip. The keys can only be used by entering the corresponding PIN codes, which should counteract abuse of the card.

By using certificates and setting up a secure connection between the card, computer and service ensures that appropriate entities communicate with each other. By making use of card readers with its own screen and keyboard, the PIN codes are entered on the card reader, without the need of the computer. This provides additional security. Using multiple authentication factors, issuing the card and PIN codes only to the person to whom it belongs and protecting against tampering and the use of others this system fulfills the requirements of Low, Substantial and High. Thus, this system will be classified as High. The data and coding used are described in Appendix C.4.

Estonia

Estonia uses an eID card as a means of authentication. The card utilizes two authentication factors; the card (something you own) and the corresponding PIN (something you know). For authentication and digital signatures the card used two different PINs.

The eID card is issued to the rightful owner after comparison of physical characteristics. At the actual issuance of the card the associated PINs are given in a sealed envelope. Therefore, the card and the PINs are only in the possession of the rightful owner or under his supervision. Moreover, the eID card is the primary (offline) identifier therefore people should always have it with them.

All electronic communication in this eID system use secure connections. To use the system the users need to log in using their eID card. This is only possible when the user is in possession of a valid eID card with associated PINs. At authentication the validity of the card is determined by checking the validity of the certificates. When certificates have been withdrawn or are no longer valid, it is not possible to log in. Not all services in Estonia require the use of the eID card, but when services require strong(er) authentication, such as Internet voting and Health Information System, using the eID card is the only option.

When a person wants to use Mobile ID he must sign a contract with a mobile operator. This is only possible when the person is already in possession of an eID card. Upon issuance of the SIM identity is checked again, then the SIM card needs to be activated by logging in using the eID card. After activation the eID card is no longer required to log in. We conclude that Mobile ID is used only by the person to whom it belongs.

By using multiple authentication factors, issuing the card, Mobile ID and the PINs to the person to whom it belongs to and protecting it against tampering and the use of others by using secure connections Estonia fulfills the the requirements of Low, Substantial and High.

Germany

The eID card of Germany uses two authentication factors: the card itself (something you own) and PINs for authentication and digital signatures (something you know). The PIN will be sent to the address the applicant provided during registration. The card itself must be retrieved from the town hall, where the identity of the person is verified again just like at registration. Therefore

the eID card is only given to and used by or under the supervision of the person to whom it belongs.

Germany established requirements that must ensure that the card is used only by the person to whom he belongs, and that this also takes place in a safe manner. Where in other systems, the user authenticates himself only with respect to the service provider, in Germany the service provider also authenticates itself with respect to the user. The service provider uses certificates that are verifiable by the eID card. The certificates determine whether the service provider may be authenticated. Moreover, they indicate which data the service provider is allowed to see. The service provider will have access to a selection of the data instead of all the data. Germany applies the principle of data minimization. Data minimization is the principle where only the minimal necessary data is exchanged.

When a user wants to use a service, he must log in by using the card, card reader, and the associated PINs. A secure connection is established between the card and the card reader. Then the certificates of the service provider are checked and the service provider verifies the card certificates. If the certificates are verified, a secure connection is established between the service provider and the card. All data communication with personal information must be approved by the user. This counteracts unwanted access to the card. With using multiple authentication factors, issuing the card and the PIN codes only to the person to whom it belongs and protect against tampering and unwanted access, Germany fulfills the requirements of Low, Substantial and High, thus will be classified to High as LoA.

The Netherlands

The Netherlands is the only country in this study that does not use an eID card. Instead, it uses various authentication options. DigiD uses the both one and two authentication factors. When choosing only one authentication factor only a user name and password (something you know) is used. A number of services require two factor authentication. In these cases also a SMS-check (something you own) is used. This is not as strong as the two factor authentication at other countries, since the phone number is not checked to see if it belongs to information provided at the registration or that in the population register. DigiD took a number of measures to protect from eavesdropping, for example, encrypting all communication. In addition, all passwords are stored encrypted. Since not all services use two factor authentication DigiD does not fulfill the requirements of Substantial and is therefore classified to Low.

At eHerkenning the number of authentication factors being used differs at the LoAs and authentication services. At the lowest two levels (Level 1 and Level 2) only one authentication factor is being used (user name and password). At levels 2+ and 3, user name and password as a SMS-check or a one-time password (something you own) is used. The highest levels also use SMS-check or a PKI certificate. The certificate works in conjunction with a PIN/password.

When one of the two highest levels is chosen at eHerkenning, the electronic identification means is used only by the person to whom it belongs, since the identity of the applicant is verified at registration and issuance. The corresponding passwords/PINs are also issued only to rightful applicant. The lowest two levels of reliability only meet the requirements of Low. The highest levels of eHerkenning fulfill the requirements of Low, Substantial and High.

Idensys uses both DigiD as eHerkenning as authentication service and is thus classified in the lowest LoA of these two authentication services. In this case, they are both classified to Low.

Spain

In Spain, the eID card uses two authentication factors of two different categories. The first authentication factor is the card itself (something you own) and the second is the PIN (something you know) used for authentication and digital signatures. The card and the PIN codes are issued only to the person to whom it belongs after registration, since the identity of the person is checked by comparing physical characteristics with the information on the eID card.

After authentication, a secure connection is set up between the card, the card reader and the computer. When completed a secure connection is set up between the user and the service provider. The data on the chip is stored into three different areas with different security levels; one section is read-only and contains the certificate of the card, a second area houses the certificates for authentication and digital signatures. This area is only accessible by entering corresponding PINs. The last part with the highest level of security includes all personal data. This section can only be accessed using special card readers that are only available at police stations. These readers verify the fingerprints (something you are/physical characteristic) with the card. This card is designed so that it cannot be used by other people, but only by or under the supervision of the rightful owner. With this measure and protecting the card against tampering by securing communication Spain fulfills the requirements of Low, Substantial and High.

Results Electronic identification means characteristics and design

All countries with an eID card always use at least two authentication factors. Furthermore, the Member States' systems are very similar to each other. The German system is the most focused on security and privacy, but in each system, there are various measures taken to ensure that third parties are unable to eavesdrop or to use it. In all cases all connections/communication is secured.

The Netherlands differs from the other Member States. Two factor authentication is not used in cases. With both Digid and eHerkenning it is possible to use only factor by log in using only a user name and password. Furthermore, the two factor authentication at DigiD is not as strong as a eID card, since the phone number is not to see whether it really belongs to the user. This is also the case for eHerkenning. This occurs when one of the lowest levels is chosen. Therefore, both DigiD and eHerkenning do not fulfill the requirements of Substantial and will be classified to Low.

The table below shows the results of the classification of the category Electronic Identification Means characteristics and design.

Table 5.3: Results Electronic identification means characteristics and design

Country	**Low**	**Substantial**	**High**
Belgium			x
Estonia			x
Germany			x
The Netherlands	x		
Spain			x

5.4 Issuance, delivery and activation

The category Issuance, delivery and activation concerns the requirements at issuance, delivery and activation of the electronic means for authentication. It is important that the device is issued with certainty to the person to whom it belongs. The requirements of this category are also mentioned in the previous categories. The figure describes the requirements associated with the LoAs.

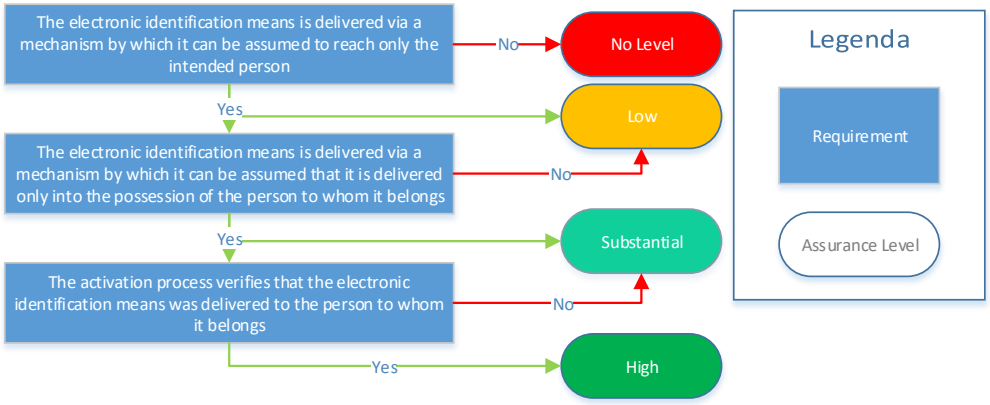

Figure 5.4.1: Flowchart Issuance, delivery and activation

Belgium

When the card is made, the applicant receives an envelope containing the PIN and a part of the activation code. This envelope is sent to the address that was already known in the population or that the person provided during the application. The PIN and activation code will be sent in a sealed envelope. If the seal is broken when received, the resident must contact the town hall to request new codes. It is assumed that the codes will arrive at the right person. Then, when issuing the card the identity of the person is checked by comparing physical characteristics with the information mentioned on the card and in the population register. We conclude that the card only comes into the possession of the person to whom it belongs[27].

To activate the card the applicant should bring the activation code to the town hall. The civil servant will use that part of the code and the code sent to the town hall to activate the card. As the card and codes are only delivered to the person to whom it belongs by checking the identity by comparing physical characteristics, Belgium fulfills the requirements of Low, Substantial and High. The data and the coding used for this category are The data and the coding that is used for this purpose, are listed in Appendix C.5.

[27] Belgian eID Card Technicalities
`http://www.danishbiometrics.org/admin/files/belgian.eid.card.technical.overview.pdf`

Estonia

When applying for the eID card, the person's identity is compared to the person's physical characteristics with that mentioned on the eID card and in the population register. If the check yields a positive result, the new card will be produced. The address in the population register will be used to sent an envelope to the applicant. The envelope indicated that the card is produced and can be retrieved. At issuance, the identity of the applicant is checked again just like at the application to avoid that the card will fall into the wrong hands. When matched, the eID card with a sealed envelope containing the PIN are handed over. The card has been activated by the CMB at issuance. The biggest problem related to the application is that the process to produce the card is very complex, as there are several public and private parties involved. Therefore it may take up to 30 days before the card is produced.

To apply for Mobile ID applicants must be in possession of a valid eID card. At this application the identity is checked at the mobile operator, just like an application for an eID card. Moreover, applicants must sign a contract with the mobile operator. When issuing the SIM card, the physical characteristics of the person and that mentioned on the eID card are compared with the information of the application. The SIM card and PINs for authentication and digital signatures are only given to the person to whom it belongs. The SIM card has yet to be activated before the electronic capabilities of the eID system can be used. This is done by logging in using the eID card and activating the associated SIM card.

Estonia delivers the eID card, the PIN codes as the SIM card by a mechanism that ensures it will only reach the person to whom it belongs. Furthermore, the activation process checks the identity of the user. Estonia fulfills the requirements for Low, Substantial and High.

Germany

After application, the resident will receive a message that the new eID card can be picked up at the town hall. At issuance the identity of the applicant will be compared to the information listed on the card and that in the population register. Next, he has the choice whether he wants to use the authentication capabilities. If he does not want to make use of it, this option is blocked. The option could be activated on a later moment at the town hall. The same verification will then take place.

To make use of the digital signatures option, the cardholder must obtain a certificate that makes this possible. A fee must be paid for this certificate. The cardholder needs to get this certificate from one of the certified CAs and put it on the card.

These procedures ensure that the card is only issued to the rightful owner. Moreover, we conclude that the card is used only by or under the supervision of the cardholder, since only the cardholder has the right information for using it. For this, Germany fulfills the requirements of Low, Substantial and High.

The Netherlands

Upon approval of the application DigiD sends an envelope within five working days with the activation code to address what is known in the population register. For this procedure it is assumed that the envelope will arrive at the address of the applicant, since the applicant has to know the combination of date of birth, postal code and BSN. During the application and issuance there is no verification of the identity of the applicant. The data in the population registration is used for sending the activation envelope. This will confirm that DigiD meet the requirements of Low and Substantial. The requirement of High is not met, since the activation process does not verify the authentication means is delivered to the person to whom it belongs. The activation

process verifies that the activation code is corresponds to the account, not that the intended person activates it.

The delivery process in eHerkenning varies per authentication service and LoA. At the lowest LoA there is no verification to check whether it actually reaches the person to whom it belongs. At the two highest levels of reliability, the authentication means is delivered personally or by registered envelope. This verifies that only the person who owns the authentication means is in possession of it. At the two highest levels, the authentication means is activated at delivery. The lowest two levels only fulfill the requirements of Low and Substantial. At the two highest the requirements of Low, Substantial and High are met. Idensys is classified as Substantial, since DigiD does not fulfill the requirements of High.

Spain

In most countries there is some time between the application and issuing the e-ID card. In Spain, the card is produced and issued immediately upon application. If the application's identity is verified, the card can be personalized on the police station. This process takes about fifteen minutes. The card with the corresponding PIN is given directly to the applicant. The new card is immediately activated and the old eID card is taken. The card always comes into the possession of the person to whom it belongs. Spain fulfills the requirements of Low, Substantial and High.

Results Issuance, delivery and activation

Member States with an eID card have similar procedures concerning issuing, delivery and activation of the eID card. The identity of the applicant is checked several times and the authentication means is only issued to the person to whom it belongs. In Spain, the card is directly personalized, produced and issued after application within fifteen minutes. In countries such as Belgium and Germany applicants could choose whether they want to use the electronic capabilities. At the town hall they could activate the card. The issuance process for DigiD use the address specified at the application for sending the activation code. The combination of BSN, postal code and date of birth must match that in the population register. It is assumed that it reaches the person to whom it belongs. The activation process does not verify that the means of authentication (account) has been delivered to the person to whom it belongs, it only verifies that the code matches the account. This is the reason why DigiD and thus Idensys performs worse than the rest.

In the table below the results of the classification are displayed for the category issuance, delivery and activation of the authentication means.

Table 5.4: Results Issuance, delivery and activation

Country	**Low**	**Substantial**	**High**
Belgium			x
Estonia			x
Germany			x
The Netherlands		x	
Spain			x

5.5 Suspension, revocation and reactivation

The category Suspension, revocation and reactivation concerns the requirements for blocking, levying and reactivating of the authentication means. This situation occurs in case of theft, loss or unauthorized use. Figure 5.5.1 describes the requirements associated with the LoAs.

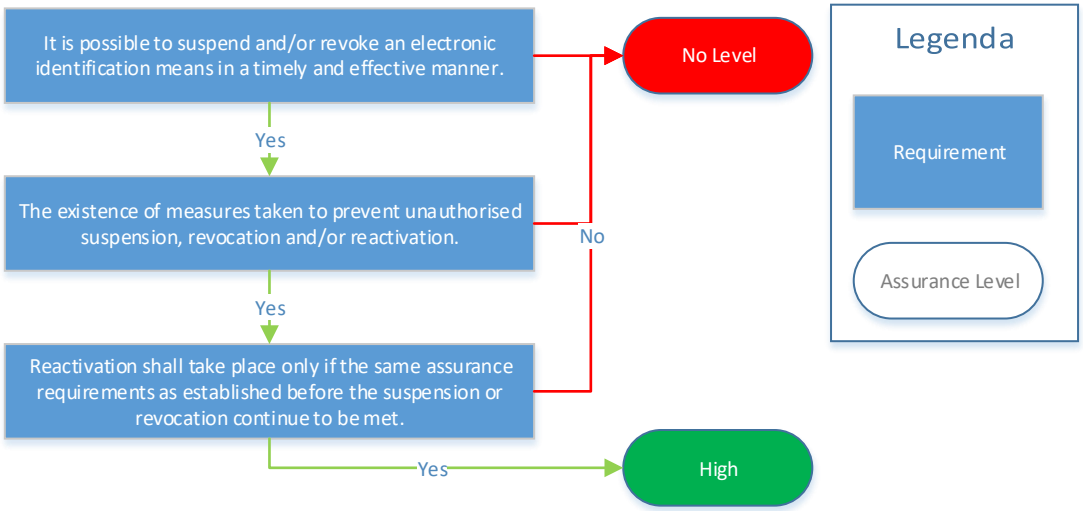

Figure 5.5.1: Flowchart Suspension, revocation and reactivation

Belgium

The certificates are blocked by default before the cards are issued until the card is activated. Furthermore, people have the ability to block the eID card. The card is automatically blocked when the certificates are expired. In case of theft, loss, or damage, the card could be blocked at the police station or at the town hall. When the card is found the cardholder must go to the town hall to reactivate it. The person's identity is verified by comparing the physical characteristics with that on mentioned on the card. If the card is not reactivated within seven days, the card will be permanently blocked.

The certificates are immediately suspended when there is notice of one or more certificates being lost, stolen or are unauthorized modified. The cardholder has the option to reactivate the certificates within seven days if he is certain that the information for blocking the certificates is incorrect. Since it possible to revoke the certificates in a timely manner, only the cardholder is able to suspend/revoke the certificates and reactivation only takes place when the card is back to his rightful owner, the identity is verified and there was no notice of unauthorized modification. By these measures taken Belgium fulfills the requirements of Low, Substantial and High. The data and the used coding for this classification are listed in Appendix C.6.

Estonia

When the card is stolen or lost residents are able to block the card. The first option they have is to go to the police station or service desk and make a report of a lost or stolen card. The other option is to call the helpline. This helpline is available 24/7 and thus allows blocking the certificates immediately. In order to prevent unauthorized suspending the card the helpline will ask for personal information, such as: full name, date of birth and personal identification number.

When the card is found the cardholder needs to reactivate it at the service desk. The person's identity will be verified by comparing his physical characteristics with that listed on the card. Since it is possible to revoke the certificates in a timely manner, only the cardholder is able to suspend/revoke the certificates and reactivation only takes place when the card is back to his rightful owner and his identity is verified. With these measures Estonia complies with the requirements of Low, Substantial and High.

Germany

In case of theft or loss, the card must be blocked. The rightful owner has a few options to block the card. First, the card has a revocation password which he is able to revoke the card at the town hall or police station. This password is used to generate a revocation code; concatenation of date of birth, surname, first name and revocation password. This will be sent to the revocation service that verifies the generated code. The revocation service will send a request to the CA for a new entry for the CRL. The CA will create service-specific CRLs for the certificates. These lists are then sent to all service providers and the card is thus blocked. It may happen that the rightful owner forgets the revocation password. It does not necessarily matter if the owner forgot the password, since all information is available at the town hall and the identity of the person is verified by physical characteristics. This prevents unauthorized suspension.

The other option is to call the hotline. Through this hotline, the cardholder must provide all necessary personal information. Here, the revocation password is necessary. Thus unauthorized blocking of the card is prevented. The hotline is open 24 hours, 7 days a week, thus revocation is possible at any moment. Reactivation is not possible, a new card must be issued. Since it is possible to revoke the card at any moment, unauthorized revocation is prevented. Germany fulfills the requirements of Low and Substantial. It is also not possible to reactivate a card. The requirements of High are met, since the requirements of Low are met. Germany is thus classified as High.

The Netherlands

An account at DigiD does not expire unless it is not used for year and a half. In other circumstances, such as identity theft, the account may be blocked. With identity theft, the user must contact the service desk of DigiD. In reporting this crime the user must provide the correct details of the account. The service desk will decide whether the current account needs to be deactivated immediately and the user needs to apply for a new account. This depends on the severity of the situation. They could decide to reactivate the account and send a new activation code to the address. With these measures taken DigiD does comply with the requirements of Low, Substantial and High.

When a user of eHerkenning suspects that there has been unauthorized use of his account, he is expected to report this to the authentication service. The service could withdraw or suspend the account. With the right information given, the user may reactivate his account. At a number of authentication services a administrator or the organization have to possibility to withdraw or suspend these accounts and reactivate it at a later moment. With these measures taken,

eHerkenning fulfills the requirements of Low, Substantial and High. Idensys will be classified as High, since both DigiD and eHerkenning fulfill all requirements.

Spain

The certificates of the eID card are valid for up to 30 months. After this period, the certificates must be renewed at the police station. The identity of the cardholder is verified by his fingerprints and that listed on the card and in the population register. After this, the cardholder is able to use the electronic capabilities again.

When the card is stolen, lost or broken the rightful owner must go to the police station to request a replacement eID card. The identity of the person is verified with the population register and the certificates will be blocked. It is not possible to reactivate the eID card, since a replacement eID card is produced directly. The validity dates of this replacement eID card is the same as the old card unless the card was in the last 90 days of his term. In that case a new card will be issued. The requirements of this replacement are the same as the first application as for a renewal.

Cardholders have the possibility to revoke the eID card in a timely manner when the card is stolen, lost or broken. The identity is verified at the police station to prevent unauthorized revocation. Even though it is not possible to reactivate eID cards Spain does meet all requirements. Moreover, the replacement card is immediately produced, so it is not necessary to reactivate the certificates. Spain is thus classified as High.

Results Suspension, revocation and reactivation

The countries with eID cards have similar processes to revoke or reactivate the eID card. Revocation occurs when a card is stolen, lost or broken. The identity of the cardholder is verified with the information in the population register. When matched, the card will be blocked. In some Member States it is not possible to reactivate the card, but a new card must be issued. In the Netherlands, at DigiD users must call the help desk in order to block the account. The help desk will ask for personal information to prevent unauthorized revocation. The help desk will determine if the account needs be deactivated immediately or at a later moment. The results of the classification of the category suspension, revocation and reactivation of the authentication means are listed in the table below.

Table 5.5: Results Suspension, revocation and reactivation

Country	**Low**	**Substantial**	**High**
Belgium			x
Estonia			x
Germany			x
Spain			x
The Netherlands			x

5.6 Renewal and replacement

The category renewal and replacement concerns the requirements of the renewal and replacement of the authentication means of authentication. Figure 5.6.1 describes the requirements associated with the LoAs.

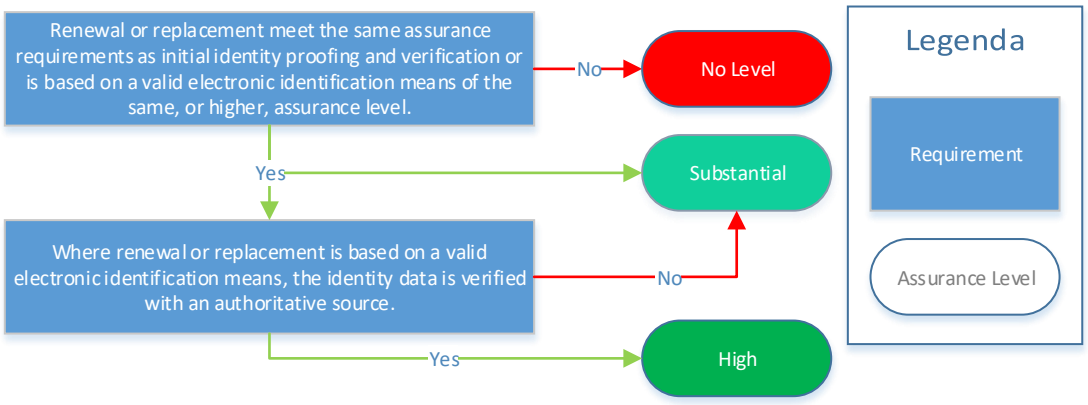

Figure 5.6.1: Flowchart Renewal and replacement

Belgium

A resident receives an envelope when the validity dates of the eID card will expire. The same steps are taken as during the initial application. The only difference is that the resident provides a valid eID card. The data provided is checked by the civil servant with that in the population register. When the card is stolen, it must reported to the police as discussed in Section 5.5. Belgium fulfills the requirements of Low, Substantial and High, since the same requirements are met as the initial application and the renewal is based on a valid eID card that is checked with the population register. Belgium is therefore classified as High LoA. The data and used coding for this classification are listed in Appendix C.7.

Estonia

When the card is about to expire or is lost, broken or stolen, the resident needs to go to the town hall to get a new card. The same procedures are followed as during the initial application. The validity of the eID card is checked with the population register by the civil servant when the card needs to be renewed. If no card is presented, the identity of the applicant compared with the information in the population register. Estonia fulfills the requirements of Low, Substantial and High and thus will be classified as High.

Germany

If the card has to be renewed, the holder must make an appointment at the town hall. When renewing, he must bring the old valid eID card with him and new resembling photos. At the town hall, the identity of the user and the validity of the card will be checked with the information in the population register. If the data are verified, the new card will be produced. Upon issuance, the identity is verified again and the old card is taken in to be destroyed. Thus, renewing the eID card will follow the same steps as the initial application. Germany is thus classified as at High.

The Netherlands

In DigiD there is no renewal, as the account does not expire. Moreover, there is no replacement, unless the account is blocked. Then the steps are taken described in Section 5.5. The requirements of the first application will apply at this replacement. It is not possible to renew an account based on another authentication means, thus this requirement can be left out. DigiD will therefore be classified to High.

The duration of validity of the authentication means varies by authentication service at eHerkenning. The minimum term at each authentication service is one year. At some services, there is the possibility to opt for a term of three or five years. An authentication means is not automatically renewed. The user will be notified that the validity of the authentication means expires and must be renewed. A price must be paid for renewing. The same requirements need to be met as the initial application. Therefore, eHerkenning fulfills the requirements of Low, Substantial and High. Idensys will be classified as High, as both DigiD and eHerkenning fulfill the requirements of all levels.

Spain

In the case of the renewal of the eID card the same procedures must be followed as during the first application. Applicants must be in possession of a new birth certificate and two resembling photos. The only difference from the initial application is that the person must bring the current eID card. Data from this card, the birth certificate, the resembling photos and the data in the population register are checked with the person's identity. If it matches the new card is produced and issued to the applicant. Spain fulfills all requirements and is thus classified as High.

Results Renewal and replacement

In all Member States the same procedures of the initial application are followed at renewing the authentication means. DigiD does not have a renewing process, since the account does not expire. In case of, for example, identity theft the account could be suspended and a replacement needs to be requested. The same procedures will take place as the first initial application. Therefore, all these situations do not differ from each other. All Member States are therefore classified to High. The results of the classification of the category renewal and replacement of the authentication means are listed in the table below.

Table 5.6: Results Renewal and replacement

Country	**Low**	**Substantial**	**High**
Belgium			x
Estonia			x
Germany			x
The Netherlands			x
Spain			x

6. Conclusion

This thesis investigated whether the new Dutch system, Idensys, is the best eID system. Therefore we compared Idensys with the systems of other Member States of the EU. The comparison was based on the Regulation 910/2014 and the Implementation Regulation 2015/1502 of the EC, since these regulations are a legal act that becomes immediately enforceable as law in all member states. The main objective of these regulations is *'to enhance trust in electronic transactions in the internal market by providing a common foundation for secure electronic interaction between citizens, businesses and public authorities, thereby increasing the effectiveness of public and private online services, electronic business and electronic commerce in the Union'* [51]. The Implementation Regulation 2015/1502 set out the minimal (technical) requirements for the eID systems of the Member States. These requirements form the basis for the comparison of this research.

6.1 Classification

The results of the classification show most systems meet the requirements of the LoAs, but the Dutch system under-performs. In the categories 'Application and Registration', 'Suspension, Reactivation and Registration' and 'Renewal and Replacement' all systems meet the requirements of the levels Low, Substantial and High. In the categories 'Identity proofing and verification', 'Electronic identification means characteristics and design' and 'Issuance, delivery and activation' only the Netherlands does not meet all requirements. The reason for under-performing lies in the use of DigiD in Idensys. The main focus of the Regulations lies on proofing the identities of users. The Member States using a eID card perform well on these LoAs since the identity of an issuer is verified on multiple moments by bio-metric identification in the process from issuing to authentication. DigiD, and thus Idensys, does not have a comparable verification, thus performing poorly in the classification. Furthermore DigiD often uses one authentication factor (user name/password). Using more authentication factors reduces the risk of identity theft/fraud, since abducting both a possession (eID card) and knowledge (user name/password) factor is more difficult than abducting only one. The first conclusion we can draw is that Idensys is not the best system at this moment. Furthermore, the other systems meet the same requirements and it is not possible to conclude which system is best. We will discuss this further in the section Implementation Regulation.

The reason why Idensys still has the possibility to be the best system with the adjustments the Dutch Goverment is going to make in 2018. For online authentication in 2018 they start with producing identity cards and driving licenses including a chip for online authentication[28], just like other Member States. With this improvement Idensys will meet the highest requirements of

[28] Tweede Kamer der Staten-Generaal Verslag van een algemeen overleg. 2016. https://www.tweedekamer.nl/downloads/document?id=a7b8c021-5caa-4129-a893-91c8bc46f1ba&title=Verslagvaneenalgemeenoverleggehoudenop29September2016overeID.pdf

the LoAs. Furthermore the use of pseudonyms and data minimization will improve the privacy of users and the security of the system. The main question of this system is what the extent of the role of the authentication services will be. At this moment it seems that the role of the authentication services becomes so large that they can see exactly when users use which service. This is what Hoepman rightly mentioned in his blog[29]. With the uprising demand for more security and privacy in systems the role of the service providers will become too large. At the moment of writing there is not a proper solution for this problem.

6.2 Implementation Regulation

The main goal of the implementation regulation is to enhance trust by providing a common foundation for secure electronic interaction between citizens. They want to create the foundation by creating minimal requirements to comply with. This research shows that most systems meet the requirements of all LoAs, but meeting the requirements does not ensure that the systems are secure. The requirements are to minimal to conclude that. In practice, there are differences between the systems, but with these requirements they are not brought to the surface. Thus, the Regulation does not give a clear distinction between systems. Furthermore, the categories of the Regulation focus on procedural measures. There are only a few technical measures in this Regulation. The requirements do not give a valuable insight into whether a system is safe or secure. For the requirements to be useful, the requirements need to more specific and should address more aspect of the systems.

6.3 Method

We used inductive coding to gather and group data. With inductive coding the coding is not based on previous research, but based on observation to determine patterns and regularities in this research . The basis for the coding was the implementation regulation of the EC, since this is the common basis for the European systems. Using inductive coding available data is gathered based on the the various aspects from the implementation in a structured manner. Goal of this method is to remove all subjectivity when the systems are being classified. Furthermore it is systematic, so it is repeatable by other researchers. Creating and adjusting the codes was an ongoing process during the gathering of the data. When the codes or data could not answer the requirements the codes were adjusted.

The last conclusion of this research is the used methodology was very useful for classifying the systems. With the used method the available data is gathered on a structured manner. The requirements form the basis for the codes being used to structure the available data. Furthermore the codes are adjusted during the gathering process to improve the classification later on. The flowcharts used during classification give a step-by-step visualization of when the system complies with a LoA. With this method systems could be classified in a systematic, consistent and repeatable manner to avoid subjective discrimination/interpretation.

[29] De authenticatiepooier onder de loep
`http://blog.xot.nl/2016/02/10/de-authenticatie-pooier-onder-de-loep/`

7. Discussion & Future Research

After comparing all systems, a number of conclusions have been drawn. For example, it became evident that the Dutch system is not the best system at the moment. Furthermore, this study shows that the Regulations do not make a sufficiently distinction between the eID systems of the EU Member States. In this chapter we will discuss all other concerns of this research.

Available literature

This thesis is based on the available literature on the selected eID systems. Most of the literature available is several years old. The IT keeps evolving continuously and it could occur the information is already outdated. There is a possibility that an information gap would arise. To fill this gap, documents given by the governments itself are used. The first example where this could occur is at the available literature for Spain. Just a few papers were available. For this research it would have been better if there were more papers available to gather information from multiple perspectives. The second example was the available literature for eHerkenning. There was no literature available except the papers given by the government itself. The research could have used more recent literature as evidence for classifying, but this would not change the outcome.

Classification Requirements

What we already addressed before is that the requirements of the Regulations are to minimal. This results in the appearance that the systems do not differ much from each other, while this is not the case. These criteria need to be more specific and stricter to be more useful in future research. A few examples of requirements that are too general: '*After issuance, the electronic identification means is delivered via a mechanism by which it can be assumed to reach only the intended person.*' and *Ensure the applicant is aware of the terms and conditions related to the use of the electronic identification means.* These requirements leave a lot of room for interpretation. Since it is not clear when the applicant is actually aware of the terms and conditions. In classification this should be avoided. By specifying the requirements and establishing stricter requirements a better distinction between system is made. Furthermore, there should be more technical requirements to give insight in the security of a system, since most requirements are primarily organizational. ISO/IEC 29115:201 [33] would be a great addition to these requirements, since this framework includes technical requirements and measures that can be taken when requirements are not met.

In this research we did not use the category 'Authentication Mechanism'. In this category there are three requirements regarding the attack potential (enhanced-basic, moderate and high). These attack potentials are based on the Common Criteria. In this document the attack potential is based on six categories; elapsed time to attack, the expertise of the attacker, the knowledge of the system, the access to the system, the used equipment and the used samples. To calculate

the attack potential *"the evaluator has to estimate the value of the factors"*[30]. In this research we want to reduce the subjectivity and presumptions of the researcher. This category would just increase this. Furthermore, we needed to examine the systems ourselves to give a good answer on this category. This would take too much time and thus we decided to not include this category.

Future Research

For future research the method could be used where similar situations are compared. Furthermore, it could be used for automatic verification in IT-systems.

The method is intentionally set up universally so it is applicable to different situations. In further researches the method should be used where similar situations are compared and classified based on available literature, besides classifying IT-systems to check whether the method is usable. For example, classifying process optimizing theories to improve business processes would a perfect situation to test this method.

Furthermore, the method could used to translate requirements or new theories into decision trees for formal verification/validation to proof the correctness of IT-systems. The method used in this research should be applicable to different situations where requirements/theories from literature are gathered and translated to a formal verification/validation.

[30] Application of Attack Potential to Smartcards
`https://www.commoncriteriaportal.org/files/supdocs/CCDB-2013-05-002.pdf`

Bibliography

[1] S. Ahlswede, J. Gaab, B. Speyer, S. Kaiser, and T. Mayer. eids in europe. *Deutsche Bank Research, Tech. Rep*, 2010.

[2] S. Arteaga and J. Ignacio Criado. Public promotion and social use of the spanish eid card. ICEGOV '11, pages 385–386. ACM, 2011.

[3] Margraf M. Bender J., Kügler D. and Naumann I. Privacy-friendly revocation management without unique chip identifiers for the german national id card. *Computer Fraud and Security*, 2010(9):14 – 17, 2010.

[4] B. Berelson. Content analysis in communication research. *New York: Hafner*, 1952.

[5] Bud P Bruegger, Detlef Hühnlein, and Michael Kreutzer. Towards global eid-interoperability. In *BIOSIG*, pages 127–140. Citeseer, 2007.

[6] A. Bryman. *Social research methods*, volume 3. Oxford University Press, 2008.

[7] B. Bud, A. Garcia, T. Gross, G. André, H. Moritz, D. Houdeau, C. Rodriguez, and S. Grzegorz. Survey and analysis of existing eid and credential systems, 2013. `http://www.futureid.eu/data/deliverables/year1/Public/FutureID_D32.1_WP32_v1.0_Survey%20of%20existing%20eID%20and%20credential%20systems.pdf`.

[8] Bundesdruckerei. Faqs - new german id card.

[9] Certipost. Citizen ca certification practice statement, 2004.

[10] R. Cimander and H. Kubicek. eid in estonia. good practice case. interoperability at local and regional level., 2006.

[11] Danny Cock, Karel Wouters, and Bart Preneel. Introduction to the belgian eid card. In *Public Key Infrastructure*. 2004.

[12] European Commission. i2010 egovernment action plan, 2006.

[13] European Commission. The european egovernment action plan 2011-2015: Harnessing ict to promote smart, sustainable & innovative government-com (2010) 743, 2010.

[14] European Commission. *Further Steps Towards the Consolidation of the Internal Market for Electronic Communications*, volume 3. Publications Office, 2010.

[15] European Commission. egovernment in spain, 2016.

[16] D. De Cock. Belgian eid card technicalities, 2006.

[17] D. De Cock, C. Wolf, and B. Preneel. The belgian electronic identity card (overview). In *Sicherheit*, volume 77, pages 298–301, 2006.

[18] B. De Decker, V. Naessens, J. Lapon, and P. Verhaeghe. Kritische beoordeling van het gebruik van de belgische eid kaart. *CW Reports*, 2008.

[19] Ministerio del Interior. Declaración de prácticas y politicas de certificación (dpc), 2016.

[20] Bundesministerium des Innern. Einführung des elektronischen personalausweises in deutschland, 2008.

[21] EU Signature Directive. Directive 1999/93/ec of the european parliament and of the council on a community framework for electronic signatures. *Official Journal L*, 13, 1999.

[22] Stuurgroep EID. Masterplan eid, 2014.

[23] A. Fairchild. The evolution of the e-id card in belgium: Data privacy and multi-application usage. In *Sixth International Conference on Digital Society*, 2012.

[24] Federal Office for Information Security (BSI). Innovations for an eid architecture in germany, 2010.

[25] A. Fullana and M. Iglesias. E-commerce and digital content.

[26] B. Gedrojc, M. Hueck, H. Hoogstraten, M. Koek, and S. Resink. Rapportage advisering toelaatbaarheid internetstemvoorziening waterschappen. fox-it, 2008.

[27] Rop Gonggrijp, Willem-Jan Hengeveld, Eelco Hotting, Sebastian Schmidt, and Frederik Weidemann. Ries-rijnland internet election system: A cursory study of published source code. In *E-Voting and Identity*, pages 157–171. Springer, 2009.

[28] H. Graux and J. Dumortier. Report on the state of pan-european eidm initatives. *European Network and Information Security Agency. ENISA. Abgerufen am*, 2(07):14, 2009.

[29] H. Harmannij, E. Verheul, and J. van Dijk. Polymorphic pseudonymization in educational identity federations, 2016.

[30] A. Heichlinger and P. Gallego. A new e-id card and online authentication in spain. *Identity in the Information Society*, 3(1):43–64, 2010.

[31] G. Hornung and A. Roßnagel. An id card for the internet – the new german id card with "electronic proof of identity". *Computer Law and Security Review*, 26(2):151 – 157, 2010.

[32] B. Hulsebosch, G. Lenzini, and H. Eertink. Deliverable d2.3 - stork quality authenticator scheme. Technical report, Technical report, STORK eID Consortium, 2009.

[33] ISO/IEC. Information technology – security techniques – entity authentication assurance framework. technical report iso/iec 29115:2013, 2013. `http://www.iso.org/iso/catalogue_detail.htm?csnumber=45138`.

[34] B. Jacobs. De overheid als verschaffer en beschermer van digitale identiteiten, 2015.

[35] B. Jacobs and W. Pieters. Electronic voting in the netherlands: from early adoption to early abolishment. In *Foundations of security analysis and design V*, pages 121–144. Springer, 2009.

[36] M. Jochems. Digid en privacy. Master's thesis, Radboud University, 2007.

[37] D. Jones and B. Simons. *Broken Ballots: Will Your Vote Count?* CSLI Publications, 2012.

[38] A. Kalja, A. Reitsakas, and N. Saard. egovernment in estonia: Best practices. *Technology Management: A Unifying Discipline for Melting the Boundaries*, pages 500–506, 2005.

[39] Tweede Kamer. Verslag van een algemene vergadering. In *Informatie- en communicatietechnologie (ICT)*, 2016/2017. Kamerstuk: 26 643. Nr. 423.

[40] K. Krippendorff. *Content analysis: An introduction to its methodology.* Sage, 2004.

[41] H. Kubicek and T. Noack. The path dependency of national electronic identities. *Identity in the Information Society*, 3(1):111–153, 2010.

[42] P. Laud and M. Roos. Formal analysis of the estonian mobile-id protocol. In *Identity and Privacy in the Internet Age*, pages 271–286. Springer, 2009.

[43] H. Leitold, A. Lioy, and C. Ribeiro. Stork 2.0: Breaking new grounds on eid and mandates, 2015.

[44] E. Maaten. Towards remote e-voting: Estonian case. *Electronic Voting in Europe*, 47:83–100, 2004.

[45] M. Margraf. *The New German ID Card*, pages 367–373. Vieweg+Teubner, Wiesbaden, 2011.

[46] T. Martens. Electronic identity management in estonia between market and state governance. *Identity in the Information Society*, 3(1):213–233, 2010.

[47] J.H. Matto and H. van der Wel. Privacy impact assessment, 2014.

[48] V. Naessens, J. Lapon, B. Verdegem, B. De Decker, and P. Verhaeghe. Developing secure applications using the belgian eid technology, 2009.

[49] I. Naumann and G. Hogben. Privacy features of european eid card specifications. *Network Security*, 2008(8):9–13, 2008.

[50] T. Noack and H. Kubicek. The introduction of online authentication as part of the new electronic national identity card in germany. *Identity in the Information Society*, 3(1):87–110, 2010.

[51] Council of European Union. Council regulation (EU) no 910/2014, 2014. `http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32014R0910&qid=1445249378336`.

[52] Council of European Union. Council implementing regulation (EU) no 2015/1502, 2015. `http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:JOL_2015_235_R_0002`.

[53] Architectuur Elektronische Overheid. Actieprogramma 'andere overheid'. *The Hague: Andere Overheid*, 2003.

[54] PBLQ. Internationale vergelijking eid-middelen, 2014. `https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/rapporten/2015/02/09/internationale-vergelijking-eid-middelen/internationale-vergelijking-eid-middelen-v1-0.pdf`.

[55] PBLQ. International comparison eid means, 2015.

[56] A. Poller, U. Waldmann, S. Vowé, and S. Türpe. Electronic identity cards for user authentication-promise and practice. *IEEE Security and Privacy*, 10(1):46–54, 2012.

[57] V. Reible and A. Braunmandl. The eid function of the npa within the european stork infrastructure. In N Pohlmann, H Reimer, and W Schneider, editors, *ISSE 2010 Securing Electronic Business Processes*, pages 392–398. Vieweg+Teubner, 2011.

[58] AS Sertifitseerimiskeskus. The estonian id card and digital signature concept principles and solutions. *White Paper*, 5, 2003.

[59] D. Springall, T. Finkenauer, Z. Durumeric, J. Kitcat, H. Hursti, M. MacAlpine, and J. Halderman. Security analysis of the estonian internet voting system. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, pages 703–715. ACM, 2014.

[60] Forum Standaardisatie. Betrouwbaarheidsniveaus voor authenticatie bij elektronische overheidsdiensten, 2014.

[61] Forum Standaardisatie. Betrouwbaarheidsniveaus voor digitale dienstverlening - een handreiking voor overheidsorganisaties, 2016.

[62] J. Tepandi, I. Tšahhirov, and S. Vassiljev. Wireless pki security and mobile voting. *Computer*, 6:54–60, 2009.

[63] Minister van Binnenlandse Zaken en Koninkrijkrelaties. Kamerbrief over eid stelsel en digidkaart, 2013.

[64] Ministerie van Binnenlandse Zaken en Koninkrijkrelaties. Evaluatie van het experiment internetstemmen tweede kamerverkiezingen 2006, 2007.

[65] Ministerie van Binnenlandse Zaken en Koninkrijkrelaties. Ontwerp op hoofdlijnen van de werking van het eid stelsel nl, 2013.

[66] Ministerie van Binnenlandse Zaken en Koninkrijkrelaties. Polymorphic pseudonymization scheme 091, 2014.

[67] Ministerie van Binnenlandse Zaken en Koninkrijkrelaties. Werking van het eid stelsel, 2014.

[68] Minster Plasterk van Binnenlandse Zaken en Koninkrijksrelaties. Kamerbrief over test met internetstemmen kiezers buitenland, 2015.

[69] Klooster Verdonck and Associaties. Onderzoek internetstemmen voor kiezers in het buitenland, 2014.

[70] P. Verhaeghe, J. Lapon, B. De Decker, V. Naessens, and K. Verslype. Security and privacy improvements for the belgian eid technology. In *Emerging Challenges for Security, Privacy and Trust*, pages 237–247. Springer, 2009.

[71] Pieter Verhaeghe, Jorn Lapon, Vincent Naessens, Bart De Decker, Kristof Verslype, and Girma Enideg Nigusse. Security and privacy threats of the belgian electronic identity card and middleware. 2008.

[72] E. Verheul. Privacy protection in electronic education based on polymorphic pseudonymization. *See eprint. iacr. org/2015/1228*, 2015.

[73] Adviesommissie Inrichting Verkiezingsproces. Stemmen met vertrouwen, september 2007, 2007.

[74] H. Zwingelberg and M. Hansen. Privacy protection goals and their implications for eid systems. In Jan Camenisch, Bruno Crispo, Simone Fischer-Hübner, Ronald Leenes, and Giovanni Russello, editors, *Privacy and Identity Management for Life*, volume 375 of *IFIP Advances in Information and Communication Technology*, pages 245–260. Springer Berlin Heidelberg, 2012.

A. Levels of Assurance

A.1 Application and Registration

Table A.1: Application and Registration

Assurance Level	**Elements Needed**
Low	1. The applicant is aware of the terms and conditions related to the use of the electronic identification means 2. The applicant is aware of recommended security precautions related to the electronic identification means 3. Collect the relevant identity data required for identity proofing and verification
Substantial	Same as low
High	Same as low

A.2 Identity proofing and verification of a natural person

Table A.2: Identity proofing and verification (natural person)

Assurance Level	Elements Needed
Low	1. The person can be assumed to be in possession of evidence recognized by the Member State in which the application for the electronic identity means is being made and representing the claimed identity. 2. The evidence can be assumed to be genuine. 3. It is known by an authoritative source that the claimed identity exists and it may be assumed that the person claiming the identity is one and the same.
Substantial	Level low, plus one of the alternatives listed in points 1 to 3 has to be met: 1. The person has been verified to be in possession of a genuine and valid evidence that is recognized by the member state and steps have been taken to minimize the risk that the person's identity is not the claimed identity. 2. An identity document is presented during a registration process in the member state where the document was issued and the document appears to relate to the person presenting it and steps have been taken to minimize the risk that the person's identity is not the claimed identity. 3. Where electronic identification means are issued on the basis of a valid notified electronic identification means having the assurance level substantial or high, and taking into account the risks of a change in the person identification data, it is not required to repeat the identity proofing and verification processes.

Table A.2 – continued from previous page

Assurance Level	Elements Needed
High	Requirements of either point 1 or 2 have to be met: 1. Level substantial, plus one of the alternatives listed in points (a) to (c) has to be met: (a) Where the person has been verified to be in possession of photo or biometric identification evidence recognized by the member state, the evidence is valid according to an authoritative source and the applicant is identified as the claimed identity through comparison of one or more physical characteristic. (b) Where electronic identification means are issued on the basis of a valid notified electronic identification means having the assurance level high, and taking into account the risks of a change in the person identification data, it is not required to repeat the identity proofing and verification processes. Where the electronic identification means serving as the basis has not been notified, the assurance level high must be confirmed by a conformity assessment body referred to in Article 2(13) of Regulation (EC) No 765/2008 or by an equivalent body and steps are taken to demonstrate that the results of this previous issuance procedure of a notified electronic identification means remain valid. 2. Where the applicant does not present any recognized photo or biometric identification evidence, the very same procedures used at the national level in the Member State of the entity responsible for registration to obtain such recognized photo or biometric identification evidence are applied.

A.3 Electronic identification means characteristics and design

Table A.3: Electronic identification means characteristics and design

Assurance Level	Elements Needed
Low	1. The electronic identification means utilises at least one authentication factor. 2. The electronic identification means is designed so that the issuer takes reasonable steps to check that it is used only under the control or possession of the person to whom it belongs.
Substantial	1. The electronic identification means utilises at least two authentication factors from different categories. 2. The electronic identification means is designed so that it can be assumed to be used only if under the control or possession of the person to whom it belongs.
High	Level substantial, plus: 1. The electronic identification means protects against duplication and tampering as well as against attackers with high attack potential. 2. The electronic identification means is designed so that it can be reliably protected by the person to whom it belongs against use by others.

A.4 Issuance, delivery and activation

Table A.4: Issuance, delivery and activation

Assurance Level	Elements Needed
Low	After issuance, the electronic identification means is delivered via a mechanism by which it can be assumed to reach only the intended person.
Substantial	After issuance, the electronic identification means is delivered via a mechanism by which it can be assumed that it is delivered only into the possession of the person to whom it belongs.
High	The activation process verifies that the electronic identification means was delivered only into the possession of the person to whom it belongs.

A.5 Suspension, revocation and reactivation

Table A.5: Suspension, revocation and reactivation

Assurance Level	Elements Needed
Low	1. It is possible to suspend and/or revoke an electronic identification means in a timely and effective manner. 2. The existence of measures taken to prevent unauthorized suspension, revocation and/or reactivation. 3. Reactivation shall take place only if the same assurance requirements as established before the suspension or revocation continue to be met.
Substantial	Same as level low
High	Same as level low

A.6 Renewal and replacement

Table A.6: Renewal and replacement

Assurance Level	**Elements Needed**
Low	Taking into account the risks of a change in the person identification data, renewal or replacement needs to meet the same assurance requirements as initial identity proofing and verification or is based on a valid electronic identification means of the same, or higher, assurance level
Substantial	Same as level low
High	Level low, plus: Where renewal or replacement is based on a valid electronic identification means, the identity data is verified with an authoritative source.

A.7 Authentication Mechanism

Table A.7: Authentication Mechanism

Assurance Level	Elements Needed
Low	1. The release of person identification data is preceded by reliable verification of the electronic identification means and its validity. 2. Where person identification data is stored as part of the authentication mechanism, that information is secured in order to protect against loss and against compromise, including analysis offline. 3. The authentication mechanism implements security controls for the verification of the electronic identification means, so that it is highly unlikely that activities such as guessing, eavesdropping, replay or manipulation of communication by an attacker with enhanced-basic attack potential can subvert the authentication mechanisms.
Substantial	Level low, plus: 1. The release of person identification data is preceded by reliable verification of the electronic identification means and its validity through a dynamic authentication. 2. The authentication mechanism implements security controls for the verification of the electronic identification means, so that it is highly unlikely that activities such as guessing, eavesdropping, replay or manipulation of communication by an attacker with moderate attack potential can subvert the authentication mechanisms.
High	Level substantial, plus: The authentication mechanism implements security controls for the verification of the electronic identification means, so that it is highly unlikely that activities such as guessing, eavesdropping, replay or manipulation of communication by an attacker with high attack potential can subvert the authentication mechanisms.

B. Quickscan

At the beginning of this reserach, a quickscan was done to compile a list of countries that we will investigate further. The purpose of the quickscan was to come with a list of countries that have different implementations of eID systems that give a complete picture of the systems in Europe without researching all systems. The results of this short study are based on the following documents [1, 2, 5, 7, 41, 49, 54, 55].

Table B.1: Quickscan

Land	Beschrijving redenatie
Austria	Austria citizens have no obligation to old an identity card. They can prove their identity with an ID card, a passport or another official document. The two cards being used mostly are the social security card and the bank cards.
Belgium	Belgium implemented the eID card early which resulted in that a very large part of the population has such card and is widely used.
Denmark	Denmark does have an mandatory identity card, but does not have an eID card. There is no plan to create one either.
Estonia	Estonia has introduced the eID card in the early years of '00. They can also vote via the internet using this card since 2005. Furthermore, Estonia does not only use an eID card but also Mobile ID. With the phone they can use the same services as the eID card.
France	France does not have a countrywide system implemented. They tried to implement an eID card, but this was rejected. They have a systems with username/password for some sectors, like a government portal.
Germany	Germany emphasized security and privacy when designing and implementing the eID. Germany is ahead of other countries on this area.
Portugal	Portugal has implemented an eID card and replaces five similar cards. Portugal has also implemented Mobile ID, just like Estonia.
The Netherlands	In the Netherlands DigiD is used as an authentication means for citizens. Organizations use eHerkenning for the government services. Currently, the Netherlands is developing a platform (Idensys) to link these systems. This implementation differs from the implementation of other countries
Spain	Spain has an eID card for a number of years. This is not the only system they use because the different regions also have their own system. Furthermore, this system has the ability to accept certificates from other CAs to use other services.
United Kingdom	The United Kingdom does not have an eID system. The public opinion was against such system. Privacy is a big theme in the UK and the public was against a system with one central database.

For this thesis we will investigate the countries Belgium, Germany, Estonia, The Netherlands and Spain further. The countries have a different implementation that gives a good idea of all implementations in the European Union. The systems highlight various aspects of possible implementations, such as privacy and security, but also the introduction of Internet voting and large scale implementations.

C. Coding

Below the coding that is being used to analyze the literature.

Table C.1: Coding

Category	Code	Description
Application and Registration	TermsConditions	Ensure awareness terms and conditions
	SecurityPrecautions	Ensure awareness recommended security precautions
	CollectData	Collecting relevant identity data
Identity Proofing	AssumedEvidence	Assumed Recognized evidence representing claimed identity
	EvidenceCorrespond	Represented evidence corresponds with entity
	GenuineEvidence	Represented evidence is genuine and valid
	IdentityDocument	Identity document is represented at registration
	OtherValidMeans	Other valid electronic identification means confirmed by conformity assessment
	OtherSameCriteria	Other valid electronic identification means conformity assessment same criteria that is confirmed by conformity assessment
	PhotoComparison	Photo or biometric identification comparison
	CollectPhoto	No photo or biometric identification evidence, then this will be collected by same procedures
Electronic identification means	OneFactor	Using one authentication factor
	TwoFactor	Using two authentication factors of different categories
	Duplication	Electronic identification means protects against duplication and tampering
	ProtectedUse	Designed to be reliably protected against use of others
	IssuerSteps	Issuer takes reasonable steps and can be assumed that it is only used or under control by person whom it belongs to

Table C.1 – continued from previous page

Category	Code	Description
Issuance and Delivery	IntendedPerson	Delivered by mechanism it can be assumed that it only reach the intended person
	Possesion	Mechanism that is can be assumed it is delivered only into possession of person whom it belongs to
	ActivationProcess	Activation process verifies it was delivered to the person it belongs to
Suspension, Revocation and Reactivation	PossibleSuspend	Possible to suspend, revoke in a timely manner
	Unauthorized	Measures are taken to prevent unauthorized revocation and reactivation
	ReactivationReq	Reactivation shall take place when same requirements are met as before
Renewal and Replacement	ProofingReq	Renewal or replacement meet the same requirements as at identity proofing
	VerifiedData	Identity data is verified by authoritative source when renewal or replacement is based on valid electronic identification means

C.1 Belgium

Table C.2: Belgium Application and Registration Coding

Code	Description
TermsConditions	Once the digital signature has been created by the signer, the signer cannot deny that this signature has been produced by his her EID card, provided that the signer's certificate was valid at the time when the signature was created.
SecurityPrecautions	In total, a Belgian eID card holds three different 1024-bit RSA private signing keys one to authenticate the citizen, one for non-repudiation signatures, and one to identify the card itself towards the Blegian government. The eID card is able to compute digital signatures with all three private keys. For the citizen's authentication key and non-repudiation signature key, this is only done after the card holder entered a PIN. This PIN must be entered by the citizen, preferable using some trusted hardware, e.g. a smart card reader with stand-alone key pad.
CollectData	The initial paper-based document included the following pieces of information on the citizen: name (family name, up to two given names, and the initial of a third name), address, title, nationality, place and date of birth, gender, and a photo of its holder.

Table C.2 – continued from previous page

Code	Description
CollectData	For the e-ID card, it is visually similar to the previous identity card and shows the same information as the paperbased document, except for the address. It also contains a hand written signature of its holder and also of the civil servant who issued the card
CollectData	Kids cards contain a unique safety feature to contact parents in case of emergency. This feature allows third parties to enter a list of preset phone numbers by way of a unique phone number and the child's RRN, both visible on the kids-ID card.
CollectData	The register also keeps track of current and past addresses and keeps a record of all the citizen's identity-related documents: passport, driving license and other relevant data. So citizens and residents cannot opt-out, but must carry the e-ID for identification and for service to be provided [4]. So choice is not part of our discussion.
CollectData	the citizen visits the municipality with his/her picture. Step 2: A civil servant validates the identity of the citizen based on the old ID card of the citizen, and starts the EID card production. The citizen then manually signs the official EID request form. The Card Personalizer will print this hand-written signature on the new EID card
CollectData	When all the digital information has been stored in the EID card (citizen's identity information, address, certificates, etc.), the Card Initializer de-activates the card and sends it to the municipality of the citizen, after which the National Register is informed of this

Table C.3: Belgium Identity Proofing Coding

Code	Description
AssumedEvidence, EvidenceCorresponds, GenuineEvidence, IdentityDocument	Civil servant validates the identity of the citizen based on the old ID card of the citizen.
IdentityDocument	The citizen receives a convocation letter with an invitation to obtain a new EID card.
PhotoComparison	The citizen visits the municipality with his/her picture. Step 2: A civil servant validates the identity of the citizen based on the old ID card of the citizen, and starts the EID card production.
PhotoComparison	Civil servant fetches the citizen's EID card, verifies the citizen's identity and starts the card's activation process

Table C.4: Belgium Electronic Identification means Coding

Code	Description
OneFactor	Two PIN-protected key pairs allow digital authentication and signing.
OneFactor, TwoFactor	After the new EID card has left the Card Initializer's premises, the Card Initializer sends a letter with the EID card holder's Personal Identification Number (PIN)
TwoFactor	When an application wants to authenticate or sign a document with the e-ID card, the middleware invites the user to enter the appropriate PIN code.
Duplication	The private keys are stored in a tamper-proof part of the chip and can only be activated (not read) with a PIN code.
Duplication, IssuerSteps	Moreover, certified card readers can have a keypad and a small screen. This way, users can enter their PIN code securely and do not longer need to trust the middleware on the PC. The screen on the card reader can display the hash value of the document that is to be signed or the personal data that will be released. This hash prevents malicious programs to sign another document than the one intended. To enforce that only certified card readers are used, the card readers should authenticate to the eID card.
ProtectedUse, IssuerSteps	In total, a Belgian eID card holds three different 1024-bit RSA private signing keys one to authenticate the citizen, one for non-repudiation signatures, and one to identify the card itself towards the Belgian government. The eID card is able to compute digital signatures with all three private keys. For the citizen's authentication key and non-repudiation signature key, this is only done after the card holder entered a PIN. This PIN must be entered by the citizen, preferable using some trusted hardware, e.g. a smart card reader with stand-alone key pad.
ProtectedUse, IssuerSteps	After the new EID card has left the Card Initializer's premises, the Card Initializer sends a letter with the EID card holder's Personal Identification Number (PIN) and activation code (PUK) to the citizen.

Table C.5: Belgium Issuance, Delivery and Activation Coding

Code	Description
IntendedPerson, Possesion	After the new EID card has left the Card Initializer's premises, the Card Initializer sends a letter with the EID card holder's Personal Identification Number (PIN) and activation code (PUK) to the citizen.

Table C.5 – continued from previous page

Code	Description
ActivationProcess	Step 11: When the citizen has received this letter, he/she can visit the municipality to activate and collect his/her EID card. Step 12: A civil servant fetches the citizen's EID card, verifies the citizen's identity and starts the card's activation process
Possesion	Carrying and identity card is a legal obligation in Belgium. Hence, the loss of such a card has to be ported swiftly, after which the corresponding certificate is suspende for up to 7 days.
ActivationProcess	A civil servant fetches the citizen's EID card, verifies the citizen's identity and starts the card's activation process (This requires the civil servant to log onto the National Register's server to access the Register's part of the activation code): the EID card is activated after the successful presentation of the activation code. Step 13: When the EID card has been activated, the civil servant witnesses that the citizen generates a digital signature with each signing key. If the digital signatures can be verified with the public keys certified in these certificates, the status of the two certificates for this citizen changes from "certificateOnHold" to "active." In practice, this means that the National Register commands the CA to remove the CRL items that correspond to these certificates as soon as the EID card has been activated.

Table C.6: Belgium Suspension, Revocation and Reactivation Coding

Code	Description
PossibleSuspend	Apart from revoking the use of an e-ID card's keys when it is stolen, card holders also have the possibility to have the electronic signature capability of an e-ID card revoked, even before using a card [8].
PossibleSuspend	In practice, this means that the National Register commands the CA to remove the CRL items that correspond to these certificates as soon as the EID card has been activated
PossibleSuspend	The major tasks of the Citizen CA consist of the issuance, suspension, activation and revocation of citizen certificates.
PossibleSuspend	The Citizen CA issues certificates on the request of the National Register. Each certificate which is issued is immediately suspended at creation, and will only be activated when the citizen presents him/herself at the municipality (cf. step 13 of Figure 3).
PossibleSuspend	The Citizen CA suspends certificates at the request of the National Register. A citizen can decide to have the certificates of his/her EID card suspended at all times.
PossibleSuspend	All certificates that have been suspended for over a week will automatically and irreversibly be revoked. Their status changes from "Suspended" to "Revoked."

Table C.6 – continued from previous page

Code	Description
PossibleSuspend	Suspension may last for a maximum of seven calendar days in order to establish the conditions that caused the request for suspension. Following negative evidence of such conditions a citizen may request to re-activate (un-suspension of) the Citizen Certificates on the following conditions:
PossibleSuspend	the citizen has ascertained without any doubt that his suspicion that there has been a loss, theft, modification, unauthorised disclosure, or other compromise of the private key of one or both of his Citizen Certificates was incorrect;
PossibleSuspend	The police, LRA or RA Helpdesk requests promptly the suspension of a pair of Citizen Certificates via the RA after: · Having received notice by the citizen that a suspicion exist that there has been a loss, theft, modification, unauthorised disclosure, or other compromise of the private key of one or both of his Citizen Certificates. · The performance of an obligation of the LRA under this CPS is delayed or prevented by a natural disaster, computer or communications failure, or other cause beyond the person's reasonable control, and as a result, there is a suspicion that another person's information is materially threatened or compromised. · Having received notice by the citizen that there has been a loss, theft, modification, unauthorised disclosure, or other compromise of the private key of one or both of his Citizen Certificates. · There has been a modification of the information contained in a Citizen Certificate. · The performance of an obligation of the RA under this CPS is delayed or prevented by a natural disaster, computer or communications failure, or other cause beyond the person's reasonable control, and as a result, another person's information is materially threatened or compromised. · Upon request from the RA or the CSP the CA suspends or revokes a pair of Citizen Certificates. · The RA revokes a pair of suspended certificates after a period of one week if it does not receive notification from the Citizen to un-suspend the certificate. · Under specific circumstances (e.g. circumvention of a disaster, a CA key comprise, a security breach, ...) , the CSP may request suspension and / or revocation of certificates
Unauthorized	To request the un-suspension of his Citizen Certificates, a citizen must present him self to his/her LRA (his/her municipalities of residence)

Table C.6 – continued from previous page

Code	Description
Unauthorized	the LRA request promptly the un-suspension of a pair of Citizen Certificates via the RA after: · Having received notice from the citizen that a suspicion that there has been a loss, theft, modification, unauthorised disclosure, or other compromise of the private key of one or both of his Citizen Certificates was undoubtedly incorrect; · The suspicion has proven undoubtedly incorrect that another person's information would be materially threatened or compromised due to the fact that the performance of an obligation of the RA under this CPS was delayed or prevented by a natural disaster, computer or communications failure, or other cause beyond the person's reasonable control. · Upon request from the RA, the CA suspends or revokes a pair of Citizen Certificate
ReactivationReq	To request the un-suspension of his Citizen Certificates, a citizen must present him self to his/her LRA (his/her municipalities of residence).

Table C.7: Belgium Renewal and Replacement Coding

Code	Description
ProofingReq	When a citizen has to receive an EID card (e.g., to replace an expired identity card), a complex process is triggered in which the National Register plays a central role.
ProofingReq, VerifiedData	The complete issuing procedure is depicted in Figure 3. If the citizen spontaneously asks for a new EID card, Step 0 is omitted: Step 0: The citizen receives a convocation letter with an invitation to obtain a new EID card. Step 1: The citizen visits the municipality with his/her picture. Step 2: A civil servant validates the identity of the citizen based on the old ID card of the citizen, and starts the EID card production. The citizen then manually signs the official EID request form. The Card Personalizer will print this hand-written signature on the new EID card.
VerifiedData	The National Register is a department of the federal government where all the identification information on the Belgian citizens is managed and monitored. All changes in the status of the EID card's production process are reflected in the National Register's databases. The municipalities act as an interface between the National Register and the citizens, and as a Registration
VerifiedData	A civil servant validates the identity of the citizen based on the old ID card of the citizen, and starts the EID card production. The citizen then manually signs the official EID request form. The Card Personalizer will print this hand-written signature on the new EID card.