Advanced Applications for e-ID Cards in Flanders

ADAPID Deliverable D2

Requirements Study

C. Diaz (Ed.), C. D'Halluin, B. De Decker, H. Dekeyser, S. Gevers, X. Huysmans, M. Layouni, S. Nikova, B. Preneel, X. Sun, S. Van Damme, H. Van Es, H. Vangheluwe, K. Verslype, and M. Zia

April 2006

Executive Summary

This report presents a requirements study for advanced e-ID cards and the applications that use e-ID card as identity token. The aspects taken into account include technical, legal and deployment issues.

We provide an outline of the current Belgian e-ID card. An overview is given of the most relevant legal provisions that apply to e-ID cards in Belgium.

We describe several e-ID use cases in the areas of e-health, e-government, trusted archival and financial applications. These use cases illustrate the possibilities of e-IDs and put into context the requirements.

The deliverable examines a wide range of requirements; namely functional, security, data protection, non-discrimination, electronic signatures, archiving, accountability, trust, e-ID cards and identity technologies, quality of service and interoperability requirements.

It is important that the advanced e-ID applications are compliant with the current legal framework. A requirement that is strictly necessary for applications making use of the e-ID is privacy. When people use the e-ID, their personal privacy should not be put at risk. We discuss the level of privacy protection that is provided by current e-ID cards and describe possible enhancements.

The current legal framework is a significant input for the development of advanced applications for the e-ID. Conversely, the research done in the ADAPID project may uncover areas where the law is ill suited to advanced e-ID applications and give an indication of how the law should be remodeled for the future.

List of Contributions

Introduction	COSIC, ICRI, DistriNet and McGill
Privacy-preserving digital credentials	McGill, DistriNet and COSIC
Anonymity metrics	COSIC
Anonymous communications	COSIC
Secure and privacy-enhanced storage	COSIC
Distribution of trust	COSIC
Policies and DRM	Distrinet
Legal aspects	ICRI
Conclusions	COSIC, ICRI, DistriNet and McGill
Editor	Claudia Diaz (COSIC)

List of Abbreviations

ACL	Access Control List
ADAPID	Advanced Applications for Electronic Identity Cards
AHC	Academic Health Centers
API	Application Programmers Interface
CA	Certification Authority
CDSS	Clinical Data Sharing System
CHUM	Centre Hospitalier de lUniversité de Montreal
CHUQ	Centres Hospitaliers affiliés Universitaires de la ville de Quebec
CIFS	Common Internet File System
CPU	Central Processing Unit
CSPA	Certification Service Providers Act
CRC	Cyclic Redundancy Check
CRL	Certificate Revocation List
CRU	Customer Replaceable Unit
CUSE	Centre Universitaire de Santé de lEstrie
DL	Data Loss
DPA	Differential Power Analysis
DPA	Belgian Data Protection Act
DRM	Digital Rights Management
DU	Data Unavailability
EBR	Event Based Retention
EHR	Electronic Health Record
e-ID	Electronic Identity Card
EMA	Electro-Magnetic Attack
EPAL	Enterprise Privacy Authorization Language
ERP	Entreprise Resource Planning
FRU	Field Replaceable Unit
GSM	Global System for Mobile Communications
IAC	Information Access Commission
ICT	Information and Communication Technologies
ID	Identity

IDA	Information Dispersal Algorithm
IDM	Identity Management
IOI	Item Of Interest
IP	Internet Protocol
IPO	Initial Public Offering
IQ	IRIS-Quebec
IRIS	Infrastructure de Recherche Integrée en Santé
MAC	Message Authentication Code
MD5	Message Digest 5
MUHC	McGill University Health Centre
MTTDL	Mean Time To Data Loss
MTTDU	Mean Time To Data Unavailability
MTTR	Mean Time To Repair
NDA	Non-Disclosure Agreement
NFS	Network File System
OCSP	Online Certificate Status Protocol
ODRL	Open Digital Rights Language
P3P	Platform for Privacy Preferences
PDF	Portable Document Format
PETs	Privacy Enhancing Technologies
PIN	Personal Identification Number
PIR	Private Information Retrieval
PKI	Public Key Infrastructure
PPDM	Privacy-Preserving Database Matching
PUK	Personal Unblocking Key
RAM	Random Access Memory
RAMQ	Regie de l'Assurance Maladie du Quebec
RBAC	Role Based Access Control
RFID	Radio Frequency Identification
ROM	Read Only Memory
RSA	Rivest-Shamir-Adleman
RIZIV	Rijksinstituut voor Ziekte en Invaliditeitsverzekering
SIS	Social Identification System
SNMP	Simple Network Management Protocol
SPOF	Single Point Of Failure
SSL	Secure Sockets Layer
TAS	Trusted Archival Service
TCO	Total Cost of Ownership
TCP	Transport Control Protocol
TTP	Trusted Third Party
URL	Uniform Resource Locator
XAM	Extensible Access Method

Contents

Chapter 1

Introduction

1.1 Background

The ADAPID project is a project of the Flemish government (IWT-Vlaanderen) aimed at:

- developing a framework for secure and privacy-preserving applications based on the Belgian e-ID card, focussing mainly on e-government, e-health and trusted archiving applications, and taking into account both technical and legal aspects; and
- investigating technologies for future enhanced generations of the e-ID card.

As first step in this project, we present in this report a set of requirements for e-ID cards and the three selected applications (e-health, e-government and trusted archival services), to serve as basis for future work in this project.

We have analyzed the requirements for e-IDs and applications making use of them, both from legal and technical perspectives. We describe a few use case scenarios in order to put the requirements into context and illustrate the need for them.

1.2 Goal

The goal of this deliverable is to develop a preliminary requirement study on the e-ID card and the protocols and applications that make use of it. We indicate the relevant issues to be taken into account and discuss legal, technical and deployment aspects. We note that some of these requirements may be difficult to combine. For example, combining accountability and privacy requirements may be complex, and tradeoffs need to be found. Here, we aim at the widest possible range of requirements, without limiting *a priori* the list of requirements.

We have gone beyond the capabilities of the e-ID cards being currently issued and explored all the desirable properties that e-ID cards could have. This requirement study will serve as basis for future work within the ADAPID project, that will conduct research intended to develop technologies and legal recommendations that implement these requirements.

1.3 Summary of contents

1.3.1 Chapter 2: Outline of the Belgian e-ID Card

This chapter gives an outline of the Belgian e-ID card. We present the purposes of introducing electronic ID cards and the legal framework that defines the functions of the card. Both the data printed on the card and the data contained in the chip are regulated by law. The chapter describes which data should be included in the Belgian e-ID card. We also give an overview on the card format, language and the procedures for issuing, renewing and returning the card. Finally, the chapter gives a list of links where more information on the Belgian e-ID card can be found.

1.3.2 Chapter 3: Use Cases

The third chapter describes use cases for the e-ID card in the following domains:

- **E-health.** It is very likely that future generations of the e-ID card will integrate health card functionalities. We have considered two types of e-health applications: Electronic Health Record Management and Clinical Data Mining for research purposes.

- **E-government.** One of the main motivations for introducing e-ID cards is to extend e-government services, making the interactions between the citizens and the public administration more convenient. We present two basic use cases for deploying e-government services, namely inquiries (requests) and submission of documents.

- **Trusted archiving.** A trustworthy archival that preserves electronic documents for an extended period of time is an essential building block for implementing an infrastructure that can support e-health, e-government or e-business services. We present three use cases that introduce trusted archival services.

- **Financial applications.** It is expected that the e-ID card will foster the development of e-business applications, by providing electronic means to sign contracts. We briefly describe use scenarios of the e-ID in financial and business applications.

We motivate the usage scenarios, analyze the flow of actions that take place and briefly describe the requirements that must be met in order to deploy these services using the e-ID card as identity token. The goal of this chapter is to illustrate the potential of e-IDs as basis to build applications.

1.3.3 Chapter 4: Requirements

In this chapter we analyze a wide range of requirements that should be met. The chapter is structured as follows:

- **Functional Requirements.** We first describe the main functionalities of the e-ID card.

- **Security Requirements.** We analyze in this section the security requirements that the e-ID card should fulfill in order to provide a secure and privacy-enhanced framework for developing applications.

- **Data Protection Requirements.** The handling of personal data (such as the one contained in the e-ID card) is regulated by the laws on data protection. This section describes the requirements imposed by these laws.

- **Non Discrimination Requirements.** The right to non discrimination is laid down in various national and international regulations. This section describes the principle of non discrimination and its implications when applied to e-ID cards.

- **Electronic Signatures Requirements.** The e-ID card provides electronic signature functionalities. This section analyzes the requirements that electronic signatures should comply with in order to be legally valid.

- **Archiving Requirements.** We present here a wide range of requirements needed to implement trusted archival services.

- **Accountability and Enforcement Requirements.** Some mechanism is needed in order to prevent abuse of the e-ID card. This section studies the requirements that enable enforcement and accountability in cases of abuse or dispute.

- **Trust Requirements.** We analyze in this section the requirements needed to make the e-ID system trustworthy, an essential property in order to ensure the wide use of e-IDs.

- **Physical Card Requirements.** In this section we present several technologies that can support e-IDs, and analyze their properties.

- **Quality of Service Requirements.** This section presents general requirements related to the usability and quality of service for e-ID cards and the applications that use them.

- **Interoperability Requirements.** As the mobility of people in Europe increases, it is important to take into account interoperability requirements that enable the access to services by foreigners or expatriates. This section explores the international interoperability requirements.

1.3.4 Chapter 5: Conclusions

The last chapter of this report presents the conclusions of the requirements study.

Chapter 2

Outline of the Belgian eID Card

2.1 Purpose

2.1.1 Part of an e-government project

The World Bank defines e-government as the use by government agencies of information technologies (such as Wide Area Networks, the Internet, and mobile computing) that have the ability to transform relations with citizens, businesses, and other arms of government. These technologies can serve a variety of different ends: better delivery of government services to citizens, improved interactions with business and industry, citizen empowerment through access to information, or more efficient government management. [1]

In Belgium it is Fedict, the Federal Public Service for information and Communication Technology, that leads and coordinates the national e-government initiatives. On the Fedict site, e-government is described as a fundamentally new, integrated and continuously adjusted way of providing services, using the potential of ICT to the greatest possible extent. [2]

For citizens, probably the most visible e-government initiative is the introduction of the e-ID, opening up a host of opportunities. After a successful pilot project in which the inhabitants of 11 municipalities were provided with their e-ID, the Council of Ministers gave the go-ahead for the national roll-out on 31 March 2004. By the end of 2009, 8 million Belgians over the age of 12 will possess an e-ID. [3]

[1] See `http://www1.worldbank.org/publicsector/egov/`

[2] See `http://www.fedict.be`

[3] L-SEC e-ID white paper 2005: e-ID beyond face value, `http://www.l-sec.be/whitepapers/e-IDpaper2005.pdf`; `http://www.godot.be`

With the e-ID, Belgium has created a card that allows the cardholder to identify and authenticate himself and to place a qualified electronic signature within the meaning of Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures. [4] In this way the e-ID is a very important means for efficient e-government applications. [5] The appearance of those applications combined with the legal recognition of the electronic signature will rapidly and safely replace a part of the paper documents by their electronic equivalent. [6] It helps to simplify the administration and to modernize the public services. It must be noticed that the e-ID is not only used in the relation with the public sector, but that citizens and private companies can also use the electronic identity card for the same purposes as part of their own relationships.

2.1.2 Functions of the e-ID

As mentioned above the present e-ID card has three functions: visual and electronic identification of the cardholder, electronic authentication of the cardholder using asymmetrical cryptography and PKI and generating a digital signature with legal force (non-repudiation). The Belgian e-ID card thus does not function as an electronic currency.

When it comes to visual identification, the card functions exactly like the traditional e-ID, as described in Art. 1 of the Royal Decree of 25 March 2003 concerning the identity cards. [7] Citizens must present their card:

- when they are required by legal authorities to provide proof of their identity,
- with every declaration or demand for official certificates, for instance when applying for specific documents at the municipality,
- when summons are delivered by the bailiff, and whenever individuals are asked to deliver proof of identity.

Checking the e-ID using electronic means is strictly regulated: persons or organizations can only check the e-ID electronically if they are allowed to do so by Royal Decree, as described in Art. 6 §4 of the Act of 19 July 1991 concerning the identity card. [8] At the moment there is still no such Royal Decree. Art. 19 of the Act of 25 March 2003 states that, as long

[4] Official Journal Nr. L 13, 19 January 2000, p. 12

[5] F.ROBBEN, E-government, 18, `http://www.law.kuleuven.ac.be/icri/frobben/publications/2004\%20-\%20E-government.pdf`

[6] See `http://eid.belgium.be`

[7] *Belgian State Gazette*, 28 March 2003

[8] *Belgian State Gazette*, 3 September 1991

as the identity cards are not renewed entirely, the current Royal Decrees concerning the use of the card continue to apply. This means that we have to take a look at the Royal Decree of 29 July 1985. [9] [10] Because Art. 1 of this Royal Decree is the same as Art. 1 in the Royal Decree of 25 March 2003, checking the e-ID with technical means at the moment is allowed in the same situations as when people have to present their e-ID for visual identification. Both with the visual and electronic identification it is necessary that the person performing the verification, has physical access to the card. For the visual identification it is sufficient that the card is shown, for the electronic identification it will be necessary that the card is handed over. [11]

For the authentication function as well as for the signature function, the e-ID will be used at a distance. Authentication refers to the process on the basis of which the origin and integrity of information are guaranteed. [12] The e-ID can for example be used to visit a website which uses client authentication. The e-ID can also be used to place a qualified electronic signature. Qualified electronic signatures are advanced electronic signatures based on a qualified certificate and created using a secure signature creation device. The qualified electronic signature is the only type of signature that will automatically be given the same value as a handwritten signature. [13] Important is that both functions are accomplished using the technique of the digital signature. It has to be noticed that both functions are optional. When he receives the card the cardholder can decide not to activate the functions. For minors the signature function is always deactivated.

2.2 Content

The Belgian e-ID takes the form of a processor chip card. On the one hand data are printed on the card, and on the other, data are stored on the cards processor chip. It is stipulated in the law which data will be placed on the card. [14] If in the future other data should be placed on the card, this will have to be provided by law.

[9] Belgian State Gazette, 7 September 1985

[10] J. DUMORTIER, Gegevensverwerking met de elektronische identiteitskaart: toegelaten of niet?, *Trends Business ICT*, November 2005, 20

[11] D. DE BOT, *Privacybescherming bij e-government in België*, Brugge, Vanden Broele, 2005, 361

[12] D. DE BOT, *Privacybescherming bij e-government in België*, Brugge, Vanden Broele, 2005, 347

[13] Art. 4 §5 of the Act of 9 July 2001, *Belgian State Gazette*, 29 September 2001

[14] Art. 6 §2 of the Act of 9 July 1991, *Belgian State Gazette* 3 September 1991

2.2.1 Visible data

The following data are printed on the card, and can thus be read visually: the cardholders single identification key (i.e., his national register number), the identity card number, the cardholders basic identification data (name, first names, gender, date and place of birth, nationality), a photograph of the cardholder, the handwritten signature of the cardholder and the municipality official, the cards period of validity and place of card issue.

Information that is likely to change, like marital status and address are no longer displayed, saving the replacement of 10% of the Belgian IDs each year.

2.2.2 Electronic data

The chip on the card, repeats the data displayed on the card and additionally stores the holders address, the authentication and signature keys, authentication and signature certificates, the certificate service provider, the information necessary for the authentication of the card, the information necessary for the protection of the electronically visible data that are encrypted on the card and the information necessary for the corresponding qualified certificates.

Digital key pairs can be used for various purposes, such as encryption of messages, authentication when consulting websites, placing qualified electronic signatures with legal force... In general however, it is argued, for security reasons that a key pair used to place an electronic signature with legal force should not also be used for authentication when accessing websites, nor for encryption purposes. [15] In the Belgian e-ID there are no encryption key pairs. There are only two key pairs, one for authentication and one for signing.

If key pairs are used to authenticate electronic communication, they are unambiguously linked to one or several certificates, on which the identity and/or one or several characteristics of the key holder are shown. In Belgium there is more and more consensus that including information on attributes in a certificate linked to key pairs used to place an electronic signature is sub-optimal because it restricts general use of the signature. For this reason the government has opted not to include attributes. [16] It is conceivable that this policy might change in the future. The use of the private keys and the corresponding certificates is secured by a PIN code. To place a qualified electronic signature, the PIN code must be entered each time a signature is to be placed. For authentication and to place an electronic signature,

[15] J. DEPREST en F. ROBBEN, E-government: the approach of the Belgian federal administration", 35: `http://ksz-bcss.fgov.be/documentation/fr/documentation/Presse/2003\%20-\%20E-government\%20paper\%20v\%201.0.pdf`

[16] D. DE BOT, *o.c.*, 357

no call is made to verify biometric properties (e.g., digital fingerprint, voice recognition, etc.). The use of biometry is not yet considered feasible on such a large scale, among other things because of the need for complicated and expensive ancillary equipment. [17]

No other data than those mentioned above are stored on the processor chip of the electronic identity card. A conscious decision has been made to use the electronic identity card only as means of identification, authentication and to place a qualified electronic signature, and not as a means of transmitting data. It is a deliberate choice to transmit data over networks, with the card as identification and authorization method to control access to data relating to the cardholder. Storage of data on the card itself would imply the cardholder needed to update those data whenever they changed. Electronic data exchange over a network relieves the cardholder from having to regularly update the card and offers the user of the data greater safeguards with regard to data availability and quality. [18]

2.3 Modalities

2.3.1 Form

The form of the e-ID is described in Art. 3 of the Royal Decree of 25 March 2003. [19] The e-ID card has the ID1-size, which is the same size as a bank card or a SIS-card. The card contains a microprocessor chip and is in conformity with all the current European standards.

2.3.2 Language

Art. 6 § 1 of the Act of 19 July 1991 concerning the identity card [20] declares that the words België en identiteitskaart , verblijfskaart voor vreemdeling of identiteitskaart voor vreemdeling, will be first put on the card in the language of the municipality that issues the document. In the municipalities that are mentioned in the articles 6 to 8 of the Act of 18 July 1966, [21], the cardholder can choose one of the languages of which the use is allowed in those municipalities. Subsequently, these words are put in the two other official languages and in English. The titles of the headings under which the personal data of the cardholder are put, will firstly be in the language of the municipality that issues the card or in the language the cardholder chooses (in the municipalities where this is possible) and subsequently in English.

[17] J. DEPREST en F. ROBBEN, *l.c.*, 37

[18] J. DEPREST en F. ROBBEN, *l.c.*, 37-38; `http://eid.belgium.be`

[19] *Belgian State Gazette*, 28 March 2003

[20] *Belgian State Gazette*, 3 September 1991

[21] *Belgian State Gazette*, 18 August 1966

2.3.3 Issuing procedure

The e-ID card is issued to every Belgian citizen that has the age of 12. The issuing procedure is very complex and a lot of parties are involved. The municipality serves as registration authority. Certipost, [22] a joint venture of the Belgian Post Group and Belgacom, is the supplier of the Belgian e-ID certificates. Zetes [23] is responsible for the production of the card (physical integration of the card components), the personalization (putting the correct data on the card and in the chip), for the activation of the card and for the distribution to the municipalities. Now we will try to explain the whole issuing procedure.

When the citizen receives a convocation letter, [24] the citizen goes to the competent municipality with the necessary documents, under which a passport photo. The civil servant of the municipality prints out an official document which is filled in by the citizen. The document contains the basic identification data and the main residence of the person concerned. The citizen indicates on the document whether or not he/she wishes to use the e-ID for electronic authentication and to place qualified electronic signatures, and signs the document. The civil servant certifies the accuracy of the data comparing them against the data held on the municipality population register, adheres the passport photo to the form and signs it. Then the application form is sent to the National Register.

The National Register registers the data in the Register of Identity Cards and sends them to Zetes. [25] Zetes issues a card and personalizes it by burning the data that are shown visually onto the card. Zetes then initializes the processor chip with the file containing the data that are to be stored on the card electronically and generates three key pairs in the processor chip which will be used in the future to authenticate the card, authenticate the cardholder and enable the cardholder to place a qualified electronic signature (the private key of the three key pairs should not leave the card). Zetes sends the public keys of the key pairs to the National Register, as well as the file stored in the cards processor chip and the data needed to identify the processor chip. The National Register checks that the public keys are unique, verifies that the file stored in the processor chip is correct and generates serial numbers for the two certificates.

The National Register instructs the certification authority to issue the two certificates. The accredited certification authority generates, after validation of the request, the qualified certificates and sends them to the National Register. The National Register then verifies the information in the

[22] `http://www.certipost.be/`

[23] `http://www.zetes.com/`

[24] The citizen does not have to wait for this letter, he can also take the initiative to get himself an e-ID

[25] Which is, as mentioned above, the card producer, initializer and personalizer

certificate and the digital signature in the certificate and sends them to the Card Initializer (Zetes) if the information is correct. If the citizen has indicated that he/she does not wish to use the e-ID for electronic authentication and to place qualified electronic signatures, the National Register keeps the two certificates in a database.

The Initializer stores the certificates on the card, generates a PIN code and two unblocking keys (PUK1 and PUK2) at random, and blocks the e-ID.

The finished e-ID is sent to the municipality where the citizen lives. The PUK1 code and - if the citizen has indicated that he/she wishes to use the e-ID for electronic authentication and to place a qualified electronic signature the PIN code are sent by the service provider to the citizen. The National Register sends the protected PUK2 code to the competent civil servant of the municipality.

After the citizen has received his invitation to pick up his e-ID, he goes with his/her PUK1 code and, if necessary, his/her PIN code to the municipality. The municipality official enters the PUK2 code he/she has received from the National Register and the citizen enters the PUK1 code to activate the card. If the citizen has indicated that she/he wishes to use the electronic identity card for electronic authentication and to place qualified electronic signatures, he/she can test those functions.

2.3.4 Renewal and return

The renewal, return and expiration of the e-ID are described in the Royal Decree of 25 March 2003. [26]

2.3.4.1 Renewal

The e-ID will be renewed (Art. 5 Royal Decree):

- after the expiration of the legal validity period, which is five years;
- when the cardholder wishes a card in an other language than the one it was issued as far as he/she lives in a municipality that is authorized to issue a card in the chosen language;
- when the photograph of the cardholder is no longer resembling;
- when the card is damaged;
- when the cardholder changes his name or first name;
- when the holder changes his sex

[26] *Belgian State Gazette*, 28 March 2003

2.3.4.2 Return

The e-ID card must be returned in the following situations:

- in case of renewal;
- when the Belgian nationality is lost;
- when the cardholder is deceased

2.3.5 Loss, theft or destruction

Art. 6 of the Act of 19 July 1991 [27] makes a distinction whether an e-ID is lost, stolen or destroyed during office hours or outside these hours. During office hours the holder has to declare the loss, theft or destruction immediately to the municipality. When a card is stolen, the cardholder may also go to the police. The municipal authorities hand over a certificate of loss, theft or destruction and order, via the National Register, the certificate authority to suspend the electronic functionalities of the card in order to avoid abuse of the e-ID. In case of loss, theft or destruction outside office hours the cardholder has to declare the loss, theft or destruction to the help desk of the National Register. The help desk suspends the electronic functionality of the card. If the card is recovered within 7 days after the suspension, the e-ID can be reactivated. If the card cannot be recovered within 7 days after the suspension, the renewal procedure is started. The old card is revoked and invalidated forever. If the card is recovered after it has been revoked, it must be returned to the municipality for immediate destruction.

2.3.6 Protection

Taking into account the risks involved in the use of the card it is necessary that the data on the card are protected in an appropriate way. This obligation can be found in the data protection act of 8 December 1992. [28] In order to have an appropriate protection, one has to consider the nature of the data and the potential risks. Considering that the National Register number is on the card, it is necessary to have a high level protection. [29]

2.4 More Information about the Belgian e-ID

Sites of the federal authorities:

[27] *Belgian State Gazette*, 3 September 1991

[28] *Belgian State Gazette*, 18 March 1993

[29] D. DE BOT, *o.c.*, 377

- http://www.fedict.be
- http://www.registrenational.fgov.be
- http://www.eid.belgium.be

Sites concerning the certificates:

- http://repository.eid.belgium.be
- http://status.eid.belgium.be
- http://certs.eid.belgium.be
- http://crl.eid.belgium.be

Other sites about the e-ID:

- http://www.godot.be
- http://ksz-bcss.fgov.be/documentation/fr/documentation/Presse/2003\%20-\%20E-government\%20paper\%20v\%201.0.pdf
- http://www.l-sec.be/whitepapers/e-IDpaper2005.pdf

Books and periodicals:

- D. DE BOT, *Privacybescherming bij e-government in België*, Brugge, Vanden Broele, 2005, 322-390
- J. DUMORTIER, Gegevensverwerking met de elektronische identiteitskaart: toegelaten of niet?, *Trends Business ICT*, November 2005, 20
- M. CARLY, De elektronische identiteitskaart, *Waarvan Akte* 2004, 13-17

Chapter 3

Use Cases

3.1 E-Health Use Cases

3.1.1 Introduction

E-health addresses the problem of improving the quality and efficiency of health care, as well as the reduction of corresponding costs, through the innovation of information and communication technologies. These advances all rely on the development of central information systems, which store patient related information. These electronic data warehouses aid in addressing the many sides to health care. On the one hand, having a repository of patient records will permit care givers to access the medical history of a patient and aid them in administering more appropriate treatments. On the other hand, if mining of these clinical datahouses is allowed, then research will allow the discovery of new causes of disease, or will investigate the impact of health care policies on access to care and quality of care. Such research will benefit care givers, in that medical research breakthroughs and knowledge will be available to them, but will also identify more effective means of improving the quality of life for citizens. These two aspects of e-health differ both on the time scale on which they are applied, the interaction with the system, the purpose for accessing the data records, and the way in which access is granted.

In this section, we will address the two outlined sides of the e-health problem. Whereas section 3.1.2 examines the health record management aspect, and the involvement of doctors, patients and pharmacists as actors, section 3.1.3 examines the data mining aspect of the e-health problem, where the actor in play is a researcher.

3.1.2 Electronic Health Records Management

In this section we give an introduction to health record management in the past, the present and the future as we see it, taking into account the possibilities opened by the use of the e-ID card while the anonymity of different parties is guaranteed.

In the past, the health records of a patient where distributed across several doctors' archives. Transferring one's records from one doctor to another was not easy, especially when the patient wanted to switch from one doctor to another. Due to the distributed character of the health records, the doctors never got to see the complete picture.

In order to counter this shortcoming, Electronic Health Records (EHRs) were introduced, which allow new usage scenarios. In this model, a central system stores all the health records of the patients. This centralized architecture poses severe security and privacy risks, given that the patients do not have any control on who is accessing their data. Ideally, a doctor should not be able to access a patient's record unless explicit authorization is given by the data subject. Similarly, a pharmacist does not need to know the identity of the person who is buying a drug prescribed by a doctor (as is the case in the current model).

Moreover, people do not trust systems where a central authority can access all EHRs of specific persons, due to the intrinsic vulnerabilities of this model towards malicious insiders or security breaches at the central database.

We thus want to protect the privacy of the different parties as much as possible and to avoid leakage of sensitive personal data by insiders (e.g., by pharmacists or employees in charge of maintaining the central EHR system) or due to successful attacks against computer systems (e.g., the pharmacist's computer or the central EHR system).

On the other hand, emergency doctors must have immediate access to the EHRs of a patient at risk without explicit consent, as there may be scenarios where the patient is not capable of giving this consent. Nevertheless, mechanisms to detect abuse of this right must be implemented.

3.1.2.1 The Future of Electronic Health Records Management

An advanced e-ID card enabled for e-health services may substantially change the present picture. We present here a story that illustrates several interactions between a hypothetical patient called *John* and the health services.

John feels sick and decides to visit a doctor. First, John and the doctor authenticate each other by using their e-ID card. The doctor also proves some qualifications with his e-ID card. The doctor then wants to see the electronic health records of John. Therefore, John authorizes the doctor to do this. The doctor logs in to the system using his e-ID card and looks at

John's records.

After the examination, the doctor adds some health records to the system. He also generates a cost reimbursement statement and a prescription. A cost reimbursement statements enables the patient to recuperate the amount of money he/she paid to the doctor by showing the reimbursement statement to his/her health insurance fund. The doctor signs both the cost reimbursement statement and the prescription with his e-ID card to achieve integrity and non-repudiation. The signature is generated in such a way that the doctor's identity is not revealed by the signature. This way, linkage of the health records with the doctor by the system by verifying the signature becomes impossible. However, it is possible to check that a certified doctor has generated the signature. In case of misuse it must also be possible to deanonymize the signature.

John goes to the pharmacist to get the medicines the doctor prescribed. After the pharmacist has shown his pharmacists' accreditation, the patient shows his prescription in an anonymous way: nor the patient's identity, nor the doctor's identity is revealed. The patient also proves his social security status (widow, married, etc.). The patient and pharmacist agree on the cost statement that enables the pharmacists to get fully compensated by the RIZIV for the issuance of medicines.

After getting his medicines, John goes to the health insurance fund to request partial repayment of the costs he had. The health insurance fund verifies the payment proofs issued by the doctor and the pharmacist and pays back John's medical costs. Everything is shown in such a way that only the necessary information is leaked.

After a few days, John gets sicker. He decides to go to the counseling service of a hospital. This is a free service which can be accessed anonymously. The counseling service investigates the case and advises John to visit his doctor again.

John, however, does not fully trust his doctor anymore. He decides to visit another doctor for a second opinion. He authorizes the doctor to access his health records for one-time only. The new doctor examines John and sees there is something wrong with John's treatment. He asks John to do a blood test.

John therefore goes to a laboratory. John doesn't reveal his identity to the laboratory doctor. Instead he uses a pseudonym. He also gives the name of his second doctor where the results of the test will be sent to. When the second doctor receives the results of the test, he adds them to John's health records. John wants the possibility to hide the existence of this advice from the first doctor because this could worsen the relation between John and the first doctor. When looking at the results, the second doctor concludes that John's first doctor has made some severe errors. It seems that John's health is in extreme danger.

The doctor corrects John's electronic health records and sends a complaint to the RIZIV. John has lost his trust in the first doctor. He decides to revoke the doctor's rights to see his health records. He also authorizes his new doctor to have full access to his health records. After thorough investigation considering the complaint, the RIZIV decides to suspend the doctor. The doctor's qualifications are revoked. That way he cannot convince patients anymore that he is a qualified doctor.

A few days later John gets a brain haemorrhage. The ambulance brings him to the emergency service. An emergency doctor is called. Since John is unconscious, he is not able to give his consent for the doctor to access his health records. In case of emergency, however, this consent should not be necessary. The emergency doctor shows an emergency credential to the system. By doing this he has immediate access to John's health records.

It seems that John needs to stay a couple of weeks in the hospital. He has to follow a care path. A care path is a plan that outlines the sequence and timing of medical activities. In each step of the care path some person of the medical staff has to perform some activities. This person can change during the care path. The medical staff only needs access to John's health records when they have to perform an activity from the care path. When the activity is finished they should not be allowed anymore to watch the patient's health records.

The daily care of patients is mostly done by nurses. These people also need access to the health records of the patient. Therefore it must be possible for a doctor to delegate his access rights to nurses. The e-ID card can be used to hold a person's access rights in a secure way. That way improper access can be avoided.

After a few days in hospital it seems that John's left leg became paralyzed. John receives a medical certificate on his e-ID card containing this information. That way John can prove his paralysis to get some special services (e.g., special help on a train).

Because John is still weak when he leaves the hospital he receives a monitoring device to measure his blood pressure. When this pressure exceeds a critical level, John and an emergency doctor are warned. Furthermore, the measurements are sent to the system to log John's health situation.

To control his blood pressure, John received a prescription for some medicines. Because of his disability, however, John is not able anymore to go to the pharmacy. He asks a friend to do this for him. To do this, John must sign a proof by which he authorizes the friend to get his medicines.

Because of all the mistakes that happened, John became very suspicious of medical services. He wants to see which persons have been treating him the last months and which information they passed around about him. With a doctor next to him, he uses his e-ID card to log in the system and look at all the accesses to his health records. He looks at his health records and asks the doctor to explain things he does not understand. That way John can be assured his health records are not abused by anyone. He can also see that all information about him is correct.

3.1.3 Clinical Data Mining

In this section, we address the problem of mining personal health information i a privacy-friendly way. The mining of aggregate health data provides valuable information to the health care system. For instance, it considerably increases scientists' ability to discover new causes of health problems and to investigate the impact of new health care policies. Due to the sensitive nature of the information contained in those health records, the mining operation should protect the privacy of those patients owning the data.

An attempt to solve the private data mining problem for health care records has been undertaken by the *"Infrastructure de Recherche Intégrée en Santé du Québec "* (IRIS-Québec), who is developing a secure innovative research infrastructure to facilitate clinical and population studies. We refer to this work to perform a requirements analysis for the usage of e-IDs in such an infrastructure.

3.1.3.1 The IRIS-Québec example

IRIS-Québec is a consortium for health and health care research involving the Québec government (RAMQ: medical insurance ministry of Québec) and the four Québec academic health centers[1] (AHCs), and their affiliated universities and faculties of medecine. Their goal is to strategically implement new information technologies in such a way as to simultaneously support health care and research. This will allow the latest advances in knowledge to be immediately available to the practitioner, and pertinent real-time clinical and population information to be available to the researcher.

IRIS-Québec will link both administrative databases and databases containing denominalized (anonymized) clinical information from Québec's four AHCs. The development and implementation of IRIS-Québec will require a careful balancing between the right to confidentiality of individuals and the privileged access to health data by researchers. The implementation of this infostructure will be coordinated with the development of data security policies and the creation of an ethico-legal observatory.

The architecture proposed by IRIS-Québec of the following four building blocks:

Clinical data acquisition systems: the clinical information systems will have a complete electronic health record by integrating all clinical services (pharmacy, laboratory, radiology, electronic medical records,

[1] McGill University Health Centre (MUHC), Centre Hospitalier de l'Universite de Montreal (CHUM), Centre universitaire de sante de l'Estrie (CUSE), Centres hospitaliers affilies universitaires de la ville de Québec (CHA, CHUQ, Laval).

order entry, admissions and discharges, nursing and health professional notes). These information systems are implanted in the four AHCs. Individual-level information (i.e., data relating to an individual person) about care received within a given institution will be stored only in the local clinical information systems and the clinical data repositories.

Clinical data repositories in the AHCs: a denominalized clinical data repository will be implemented and maintained to allow data transfer operations from the clinical information systems in the AHCs, and researcher access to the centralized clinical data.

Provincial administrative data repository: will house population-level (i.e., data relating to a group or population of persons) health care utilization and administrative data (e.g., air pollution, water quality) that can be integrated on a project-by-project basis. This repository will store both population-level health care utilization data information and individual-level information that is essential for the long-term follow-up.

Research toolkit: allows the linkage of the clinical data with the administrative data. It also provides researchers with the following functionalities:

- Integration of clinical data from individual repositories;
- Integration between clinical and RAMQ warehouses;
- User authentication and access rights;
- Encryption and anonymization software;
- Custom research functionalities;
- Evidence-based alerts and reminders;
- E-trials and non-experimental cohorts;
- Data quality management tools;
- Search engine.

For the purpose of requirements gathering, we will base our case studies on a more generalized study of a Clinical Data Sharing System (CDSS). This CDSS will closely follow the model developed by IRIS-Québec, and will involve data mining on affiliated hospital center (AHC) data repositories as well as an administrative data repository.

3.1.3.2 The Future of Clinical Data Mining

We present here a story which illustrates how Jean-Luc, a hypothetical researcher, would interact with the CDSS using his e-ID. The scenario also illustrates how an advanced e-ID card can enable updates of the clinical data repositories by hospital staff.

Jean-Luc is a diabetes researcher at McGill University. He wants to study the effects of small injections of native INGAP peptides on type 2 diabetics. INGAP is a protein that's responsible for the formation of new insulin-producing beta-cells. Jean-Luc needs some clinical information about the population of Québec type 2 diabetics who have been hospitalized in the past 5 years for kidney failure following their initial prescription of such injections. More specifically, he needs to know when the prescription was made, and for how long the injections were performed before any signs of kidney failure were detected.[2]

Jean-Luc has heard about the CDSS research interface. This interface provides researchers with access to medico-administrative databases across the province through an online web interface. He decides to fill out the online registration form found on the website. His application is forwarded to the "Information Access Commission" (IAC). The IAC is a commission who decides who may and may not get access to information. IAC performs a check on Jean-Luc, and finds out that he is a researcher at the MUHC, conducting studies on diabetes. Furthermore, he has a record of good academic conduct, so the CAI decides to grant Jean-Luc access to the CDSS system. First, IAC asks Jean-Luc to sign a confidentiality and privacy agreement, whereby he is not allowed to share his access with any other individual or group, nor is he allowed to divulge or share the information gained by this access to any third party. The system and the information may only be used by him, in his studies, for the purpose of his research project. Then, the IAC adds a record for Jean-Luc in its administrative database, grants his access, and issues him an electronic researcher accreditation certificate.

Jean-Luc then logs-on to the CDSS web-interface to make his query. In order to do so, he is asked to authenticate himself with his e-ID researcher accreditation certificate. Once authenticated, Jean-Luc submits his query, and receives a confirmation that his query was accepted by the system, and that it will be processed.

Meanwhile, Dr. Ruth at CUSE just admitted a 55 year-old type 2 diabetic man into the hospital. The man undergoes some laboratory tests, the results of which Dr. Ruth has just received. After completing her rounds at the emergency room and receiving the man's consent to update his electronic record, she goes back to her office to update the CUSE clinical information system. She logs-on to the IQ web-interface, and is asked to authenticate herself with her e-ID doctor's license. Once her identity is verified, Dr. Ruth is allowed access to the CUSE clinical data repository, and updates the patient's electronic health record by integrating his admission record and his laboratory tests and results.

[2] It is important to note that this research is purely fictional in nature.

A few days later, Jean-Luc receives notification that his query was processed and is given instructions on how to retrieve the results. Again, he is asked to authenticate himself with the system through his e-ID. Once authenticated, Jean-Luc is able to retrieve the results of his query, and use them for his study.

3.1.4 Outline on E-Health cases

We give a typical usage scenario and elaborate on two Health Record Management use cases (visiting a doctor and visiting a pharmacist), and one Clinical Data Mining use case (collecting data through a "Clinical Data Sharing System"). For each use case, the functional, security and privacy requirements are described in Sect. 3.1.8.

3.1.5 E-Health Case 1: Visiting your doctor

3.1.5.1 Actors

- User as patient
- Doctor

3.1.5.2 Stakeholders

- Patient: needs treatment or consultation
- Doctor: needs access to all the patient's health records
- Health insurance fund of the patient: has to reimburse the patient and sometimes the doctor
- RIZIV: is responsible for the qualifications of the doctors
- Pharmacist: only accepts valid prescriptions

3.1.5.3 Description

A sick or wounded patient visits a doctor to get better. The patient identifies himself to the doctor using his e-ID card. The doctor proves his qualifications with his e-ID card. The patient authorizes with his e-ID card the doctor to access his health records. The doctor is then able to access the health records of this patient. He examines the patient, adds health records, gives a prescription to the patient and generates a cost reimbursement. Both patient and doctor remain anonymous to the system to enhance privacy with respect to the system manager and other people who could have access to the health records.

3.1.5.4 Main flow

1. The patient goes to the doctor in order to get cured
2. The patient identifies himself (e-ID card authentication) to establish a relation of trust between doctor and patient
3. The doctor checks the user identification
4. The patient asks the doctor to prove his/her qualifications to get assured about the doctor's capabilities
5. The doctor shows the patient his/her doctor's credential (e-ID card authentication with doctor's certificates)
6. The patient verifies the validity of the doctor's credential
7. The patient authorizes the doctor to access his health records (e-ID card digital signature)
8. The doctor contacts the system and tries to access the health records of that person (e-ID card authentication with user issued certificate)
9. The system sends the health records to the doctor
10. The doctor examines the person and makes a diagnosis
11. The doctor adds new health records of this patient to the system (e-ID card digital signature)
12. The doctor possibly updates previous health records (e-ID card digital signature)
13. The system accepts the new/updated health records
14. The doctor finally prescribes medication or treatment by issuing a prescription to the patient (e-ID card digital signature on the prescription). The doctor also generates a medical cost reimbursement statement which is given to the patient (e-ID card digital signature on the reimbursement statement)
15. The patient receives the prescription and the medical cost reimbursement statement

3.1.5.5 Alternative flow

2a. The patient chooses to remain anonymous to the doctor

1. The patient goes to the doctor
2. The patient asks the doctor to prove his/her qualifications

2b. The patient identification fails

1. The doctor can choose to continue the consultation or not

6b. The verification fails (e.g., some qualifications are revoked) or the qualification does not satisfy the patient

1. The patient leaves and can contact a controlling organization

3.1.6 E-Health Case 2: Visiting your pharmacist

3.1.6.1 Actors

- User as patient
- Pharmacist

3.1.6.2 Stakeholders

- Patient: wants his medication at the prescription charges.
- Pharmacist: wants to get compensated for difference between the retail price and the prescription charges.

3.1.6.3 Description

When the patient receives a prescription from a doctor, he goes to the pharmacist to get his medicines. The pharmacist shows his pharmacist's recognition using his e-ID card. The patient shows his prescription in an anonymous way: neither the patient's identity, nor the doctor's identity is revealed. The patient also proves his social security status using his e-ID card. Furthermore, the patient shows that he is entitled to get the medicine (i.e., he possesses a prescription in his name, or he is authorized to fetch the medicines by the patient, to which the drugs were prescribed). The patient and pharmacist both sign the cost statement that enables the pharmacist to get fully compensated by the RIZIV for the difference between the retail price and the prescription charges.

3.1.6.4 Main flow

1. The patient goes to the pharmacist
2. The user asks the pharmacist to prove he/she is an accredited pharmacist in order to assess the pharmacist's capabilities
3. The pharmacist gives a proof (e-ID authentication with pharmacist's accreditation certificate issued by RIZIV)

4. The patient gives the prescription to the pharmacist
5. The pharmacist verifies the validity of the prescription
6. The patient proves his social security status: widow, married, etc. (e-ID card authentication with certificate containing the social security status). This determines the prescription charges the patient will have to pay to the pharmacist
7. The pharmacist verifies the social security status proof. Now, he can determine the prescription charges
8. The pharmacist generates a cost statement for the social security (e-ID card digital signature)
9. The patient agrees with the prescription charges and signs the cost statement for the social security (e-ID card digital signature). The cost statement enables the pharmacist to get fully compensated for the difference between the retail price and the prescription charges
10. The pharmacist gives the patient the necessary medication
11. The patient accepts the medication and leaves the pharmacy

3.1.6.5 Alternative flow

3a. Invalid proof

1. The user leaves the pharmacy and can contact a controlling organization

5a. the prescription is invalid (e.g., has been tampered with or has been successfully used in past)

1. The verification of the prescription by the pharmacist failed. The pharmacist can contact a controlling organization is fraud is likely

5b. Valid prescription, but it contains suspicious/doubtful content data (e.g., a deadly dose of pills)

1. After valid verification of the prescription, the pharmacist sees suspicious/doubtful content and must be able to contact that doctor to verify the data

7a. The patient does not agree with the prescription charges

1. Stop use case

3.1.7 E-Health Case 3: Collecting data through a "Clinical Data Sharing System"

3.1.7.1 Actors:

- User as researcher

3.1.7.2 Stakeholders:

- Researcher: needs to conduct research/population studies, and intends to gather clinical and statistical data.

3.1.7.3 Description:

Researchers do not interact with the system directly; instead, all interactions go through the "Clinical Data Sharing System" (CDSS) web interface, and the CDSS coordinates the activities between the researcher and the Affiliated Hospital Centres (AHCs). To gain access to the interface, the researcher must register with the CDSS by first going through a mandatory screening by the "Information Access Commission" (IAC).

The intention of the researcher is to gain access to the Clinical Data Sharing infrastructure for the duration of his/her research project. Many researchers may be registering multiple projects with the CDSS at any given time. A researcher intends to gather data from the AHCs for a specific project by submitting a query. Many researchers may be submitting queries at any given time.

Researchers do not interact with the system directly; instead, all interactions go through the CDSS web interface. The activities between a researcher, the AHCs, and their data repositories are coordinated by the CDSS. To get access to the CDSS, a person must prove their researcher credentials to the IAC. Once access is issued, the researcher must show his researcher recognition, using his e-ID card, every time he wants to submit a query. Upon completion of the research project, or in case of fraudulent behaviour, the researcher's recognition is revoked.[3]

3.1.7.4 Main flow

1. The researcher contacts the IAC about a specific research project in order to get access to the CDSS.

2. The IAC performs a background check on the researcher, and his/her project, to prove he/she is an accredited researcher before granting system access.

[3] This generalized use case is inspired by the real-life application currently being implemented by by the IRIS-Québec research group in Montreal, Canada.

3. The IAC acknowledges the researcher's credentials, and issues a researcher accreditation certificate.

4. The researcher logs on to the CDSS web interface and is asked to identify him/herself and to prove his approved researcher status. The researcher proves his accreditation with e-ID authentication (with the researcher accreditation certificate issued by IAC).

5. The researcher submits a query.

6. The CDSS coordinates the processing of the query by remotely invoking methods on the AHC data repository systems as well as the administrative repository.

7. The AHCs sequentially process the query, passing it on to the next partner in the chain, as well as the results obtained which will be integrated with the next partner's processed results. Once all the AHCs have processed the query, the CDSS coordinates the passing of the integrated results and the query to the administrative repository system (referred to as the last participant).

8. The last participant completes processing of the query, the results of which are are integrated with all previously gathered results.

9. The query results are anonymized.[4]

10. The researcher is notified that the query has been processed by all partners involved. The results of the query have been saved on the server of the last participant.

11. The researcher establishes a secure connection with the last participant. He is asked to authenticate himself using the researcher accreditation certificate of his e-ID card.

12. Query results are transferred to the researcher.

13. The researcher accepts the results, and logs off the web interface.

3.1.7.5 Alternative flow

2a. IAC ascertains bad record/background of the researcher.

1. IAC rejects the researcher's registration. The use case ends in failure.

[4] The anonymizing software ensures that the data batch resulting from the query satisfies certain anonymity constraints.

4a. The researcher identification fails

1. The researcher is not denied access to the system. Use case ends in failure.

9a. Query has resulted in a data batch which cannot be anonymized:

1. The CDSS notifies the researcher and rejects the query. The researcher does not receive results. The use case ends in failure.

3.1.8 Requirements for E-Health Use Cases

For the previous use cases, the following requirements concerning the e-health application domain can be distinguished.

3.1.8.1 Prescription

Only qualified doctors can issue prescriptions, even to patients who want to remain anonymous to the doctor. When a prescription is shown to a pharmacist, the pharmacist must be convinced that the show is done by the subject of the prescription (i.e., the patient) or one of his/her delegates (authorization). This avoids prescriptions from being stolen and used by another person, something that could happen especially in case of prescription-only drugs.

Both the pharmacist and the patient can verify the integrity of the prescription (in order to detect tampering) and the fact that it has been issued by a qualified doctor (authentication). In normal situations, the pharmacist is unable to identify the patient or the doctor who issued the prescription. By enforcing patient anonymity, the pharmacist is unable to profile the patients using database and data-mining techniques. However, the pharmacist must still be able to contact the doctor (direct or indirect) to verify a possibly lethal dose (conditional anonymity).

Both patient and doctor remain anonymous to the system to avoid profiling and linking by the central system. This minimizes the trust put in the central system. Also, the leakage of sensitive information by the central system due to external attacks or internal misuse is minimized.

A patient must not be able to receive the prescribed medicines multiple times (single use property). Afterwards, when abuse committed by a doctor is detected by the RIZIV for instance, the doctor can be held accountable. The doctor can thus not repudiate having issued a certain prescription. A prescription must also contain an expiry date to avoid that medicines are obtained long after the patient has recovered.

3.1.8.2 Doctor's license

The doctor must be able to prove his recognition as a doctor and his specialties (authentication) to convince the patient of his capabilities. This is done by showing a doctor's license. This license is issued by the RIZIV. A doctor's license must be revocable (by the RIZIV) in case unacceptable behaviour is observed. This overrules the doctor's capability to access EHRs. Existing EHRs inserted by the revoked doctor can be marked as untrustworthy. Of course, these licenses must be integrity protected to avoid tampering by the doctor.

3.1.8.3 Pharmacist's credential

The pharmacist also needs a pharmacist's credential to prove his pharmacist accreditation (authentication). This credential may also be revoked in case abuse or incapability by the pharmacist is proven. The integrity must be protected in order to avoid tampering. Only the owner of the pharmacist's credential may be able to show it (authorization).

3.1.8.4 EHR access rights

The patient must be able to grant a doctor access rights to to the patient's electronic health records (authorization). The doctor proves ownership of these rights to the system (authentication) in order to view or update existing e-health records, add new health records (authorization). The patient issues these rights but can also revoke them. For example, he must be able to switch to another GP. When a patient wants to contact another doctor (not his/her GP), the patient can issue a one-time access permission to his/her e-health records without his/her regular GP being able to know this (authorization) to avoid a deterioration of the relationship with his/her GP. The doctor however should not be able to link that patient to other transactions both inside the e-health system (e.g., pharmacist visits etc.) and outside (e.g., financial or governmental etc.)

3.1.8.5 Medical advice

As a result, this "second doctor" can give advice that is both integrity protected and confidential such that tampering is impossible and only the patient can see it or enable another doctor to see the advice. Still, the second doctor can be held accountable for the given advice. The patient can contact an on-line counseling service. This should happen anonymously to reduce trust put in the counseling service and to minimize leakage of sensitive date in case of an attack. The given advice must remain confidential as described by law.

3.1.8.6 Emergency access

In case of an emergency, the emergency doctor needs immediate access to the EHRs of the patient, without first having the explicit authorization of that patient (authorization), who may be in a state unable to grant access to his EHRs. Because every emergency doctor has access to all EHRs of each patient, abuse has to be detectable and the emergency doctor must be held accountable in that situation (accountability).

3.1.8.7 Electronic health Records (EHRs)

A central concept in e-health is the electronic health record (EHR). The doctor must be able to view all the medical records of the patient consulting him/her in order to put the right diagnosis. In order to update the patient's health status, the doctor must be able to submit new EHRs to the system after being authorized to do so. The doctor is not able to remove EHRs to prevent destruction of potentially valuable EHRs or evidence (e.g., in case of accountability). The EHRs must be integrity protected such that no one can tamper with these. The confidentiality of the EHRs must be preserved such that only authorized doctors are able to view these. The anonymity of both the doctor as the patient involved in the EHRs must be preserved to minimize trust and to avoid data leakage in case of attacks. However, when wrong EHRs are submitted, the doctor must not be able to repudiate he submitted the EHRs and the doctor must be held accountable for his/her actions. In this situation, it might be necessary to reveal the identity of the doctor (conditional anonymity). Only a recognized doctor can access the EHRs to prevent non qualified doctor's having access to EHRs. The health records must be available when the doctor wants to view them.

3.1.8.8 Medical cost statement

When visiting a pharmacy, a medical cost statement is made. The patient only pays the prescription charges to the pharmacist. A medical cost statement is a proof of having offered certain services and/or medicines to a patient and will be shown by the pharmacist to the RIZIV in order to get fully compensated for the difference between the retail price and the prescription charges. This medical cost statement needs to be integrity protected to avoid tampering (by e.g., the pharmacist to obtain higher compensations). Such a cost statement may only be used once (to avoid double compensations). The cost statement must be accompanied by a valid prescription. In principle, it is not necessary for the RIZIV to know the patient identity. The patient can thus remain anonymous with respect to the RIZIV but must still be held accountable when e.g., illegal deals with the pharmacist are made. Thus, when abuse is detected, the patient and/or pharmacist must be held accountable.

To be able to determine the prescription charges, the patient needs to prove health insurance fund membership (authentication) and his/her social status (married, widow, etc.). The health insurance membership statement and the social status must be integrity protected to avoid tampering and may only be shown by the patient who owns it (authorization). Both can be shown using a digital identity card.

Because the patient wants to have the ability to remain anonymous to the pharmacist, the medical cost statement must not reveal the identity of the patient nor the identity of the health insurance fund, nor the identity of the issuing patient (anonymity). The membership statement will typically expire after one year. Memberships can in some circumstances be revoked beforehand (e.g., change of health insurance fund by the patient).

3.1.8.9 Reimbursements statement

After consulting a doctor, the doctor issues a reimbursement statement to the patient to enable the patient to recuperate (part of) the amount of money he/she paid to the doctor (authorization) by showing the reimbursement statement to his/her health insurance fund. This statement must be integrity protected and the health insurance fund of the patient and maybe the RIZIV are the only entities who must be able to read it (confidentiality) in order to compensate the patient, although the patient may show it to others. A doctor must be held accountable when reimbursement statements are issued illegally. In some situations, the patient can also be held accountable (non-repudiation). The reimbursement statement can only be shown by the patient who legally owns it (authorization). A patient can only be paid back once for each reimbursement statement (single use). Typically, a reimbursement statement will have an expiry date.

3.1.8.10 Patient's identity

To subscribe to a health insurance fund or when visiting a doctor, the patient needs to prove his/her identity (authentication).

The integrity (to avoid tampering) and confidentiality (to protect the patient's identity) need to be protected and the identity can only be shown by the person corresponding to that identity.

3.1.8.11 Medical certificates

Medical certificates issued by a doctor (or another medical instance) to a patient can be shown by this patient to other parties to prove, for example, certain disabilities (authentication). These medical certificates must be integrity protected, confidential (not everyone needs to know these disabilities).

The anonymity of the patients needs to be preserved: for instance, to use a parking place reserved for disabled people, one does not need the identity of the patient. The issuing doctor should also remain anonymous in a credential show to keep the anonymity set as large as possible. Maybe not all the information in the medical certificate needs to be shown. Therefore, selective disclosure of information is useful (confidentiality). On the other hand, some information must not be hidden. For example, when one wants to obtain a driving license, it must not be possible to hide disabilities, treatments, or other conditions which prohibit driving a car. The medical certificates must be bound to the patient such that no one else can use these. Revocability is necessary because not all disabilities, treatments, or special conditions are permanent. For the same reason, an expiry date is needed. In case the issuing entity commits fraud by issuing medical certificates wrongfully, he/she must be held accountable (non repudiation) and the certificates involved revoked.

3.1.8.12 Medical surveillance

Medical surveillance on distance must be possible. The system receives pseudonymous data at regular intervals. When critical values or dangerous patterns are detected, the location of the patient is determined. This enables the system to contact the closest available (emergency) doctor. This doctor must be able to access the EHRs of the patient and must be able to locate him/her quickly. The monitoring data must be integrity protected by the monitoring device and authenticated as generated by that device. Confidentiality must also be preserved such that only the controlling entity is able to view the data. Only in dangerous situations, the anonymity of the patient may be revealed to the closest emergency doctor or the patient's GP (conditional anonymity).

3.1.8.13 Data mining

Researchers and the government want to data mine on the clinical data contained in the EHRs. First, permission by the Information Access Commission (IAC) has to be obtained (authorization). The researcher needs to prove his research credentials and accreditation (authentication). If the IAC is satisfied with these credentials, it issues a researcher accreditation certificate. Only the owner of the certificate may be able to use it (authorization), and must do so every time he/she want to access the Clinical Data Sharing System (CDSS). This certificate must be revoked in case of abuse or unacceptable behaviour is observed. The certificate must be integrity protected.

The data must respect the anonymity of the different parties involved (mainly patients). Patients must remain anonymous to the system and to the researchers. That is, even if data collected through several projects and queries is integrated, individual patients may never be identifiable. The result of data mining queries must maintain integrity and confidentiality for obvious reasons.

The privacy and confidentiality of medical records and anonymized data to unauthorized parties (i.e., CDSS) must be maintained: the CDSS must never be in possession of private data.

Transfer of data between Affiliated Health Centers and the researcher must be secured against external attacks.

3.1.8.14 Access right delegation

During a treatment in a hospital, access to a subset of the information in the EHRs must be delegated to the nurses for the daily care of the patient. This can only be done by a doctor who has access to the patient's EHRs (authorization). This doctor must be held accountable in case far too much info is given to the nurses. These partial access rights must be revocable and expire after a given time.

During every interaction with the RIZIV or a health insurance fund, these entities must authenticate themselves.

3.2 E-Government Use Cases

3.2.1 Introduction

One of the main goals of deploying electronic ID cards at a national level is create an infrastructure to support e-government applications. The migration from paper to electronic administration opens a whole range of possibilities for e-governments services:

- Citizens will be able to request and submit information electronically (this covers many of the interactions between citizens and the public administration)
- Citizens may vote electronically in electronic elections
- Tax declarations may be done on-line
- On-line access may extend the modalities and possibilities of social services (e.g., attention to handicapped people may be partially done electronically)
- Local services, such as parking cards, garbage collection, etc.

In this report, we have selected inquiry and submission of information as use cases, given that most services imply in one way or another the request or submission of data.

In the next two sections, we study in detail these two use cases. At the end of the chapter we analyze the requirements that must be fulfilled by e-government applications.

3.2.2 E-Government Case 1: Inquiry

In this section, we describe how the e-ID could be used by citizens to request information from the government. We first outline the different kinds of inquiry and then we describe the basic steps of the transaction. The requirements such a system should comply with are discussed at the end of the chapter.

3.2.2.1 Types of inquiry

Citizen's demands for information from public offices can have various aims. We can distinguish three types of inquiries according to the level of identification and authentication required:

- **Type I: Access to public information.** When citizens request information which is publicly available (i.e., which fall into the Freedom of Information Acts), there is no need for identification of the requester.

- **Type II: Access to own data.** Citizens have the right to access their personal data processed by other parties according to the Data Protection Acts. In this case, only the owner of the data should be able to access it.

- **Type III: Access to registers.** The access to registers such as the Land, Trade or Residents' Register may be restricted to certain professional groups (e.g., notaries). In these cases, requesters may be required to identify themselves and prove they belong to a specific professional group.

In all three kinds of inquiry, there may be third parties whose interests are affected. In some cases, these third parties can prevent the information or the permission for the examination of data.

3.2.2.2 Flow

In order to describe the flow of these transactions in a general way, we use the following terminology:

- User: citizen which initiates the inquiry
- Server: portal that serves as interface for e-government services
- Database: repository where the information of interest is stored
- Third parties: entities which have legitimate interests that may put conditions on the transaction

3.2.2.3 Inquiry Type I

1. The user challenges the server to prove that it is an authentic server
2. The server proves that it is an authentic server
3. The user sends the request to the server
4. The server checks if the information can be made available (i.e., if there are no legitimate restrictions on the information established by third parties)
5. The server forwards the request to the database
6. The database responds to the server with the requested information
7. The server forwards the information to the user

3.2.2.4 Inquiry Type II

1. The user challenges the server to prove that it is an authentic server
2. The server proves that it is an authentic server
3. The user sends the request to the server
4. The server challenges the user to prove that he/she is the owner of the data
5. The user proves that he/she is the owner of the data
6. The server checks if the information can be made available (i.e., if there are no legitimate restrictions on the information established by third parties)
7. The server forwards the request to the database
8. The database responds to the server with the requested information
9. The server forwards the information to the user

3.2.2.5 Inquiry Type III

1. The user challenges the server to prove that it is an authentic server
2. The server proves that it is an authentic server
3. The user sends the request to the server
4. The server challenges the user to prove that he/she is authorized to access the data
5. The user proves that he/she is authorized to access the data
6. The server checks if the information can be made available (i.e., if there are no legitimate restrictions on the information established by third parties)
7. The server forwards the request to the database
8. The database responds to the server with the requested information
9. The server forwards the information to the user

3.2.3 E-Government Case 2: Submission of data

When interacting with e-government services, citizens often need to submit data. In this section, we outline the different kinds of submissions and we describe the basic steps of each type of transaction. The requirements of this e-government service are discussed in the following section.

3.2.3.1 Types of submissions

Citizen's can submit different type of data to the public offices. We can distinguish four types of submissions according to the level of identification and authentication required:

- **Type I: Anonymous submission of data.** Certain e-government services may benefit from providing anonymous submission of data. These range from on-line help services (for victims of violence, people with drug addictions, people who want to suicide, etc.), to whistle blowing or collection of citizens' opinions on a particular policy.
- **Type II: Anonymous submission of data only from citizens that fulfill certain attributes.** In some cases, the e-government service may be aimed at a certain subset of citizens. This could be a professional group, people within a certain age range, residents of a locality, etc. In this case, the citizens may be required to prove they posses the required attribute(s) before they are allowed to submit the data.

- **Type III: Authenticated submission of anonymous data.** Applications such as e-voting have strong security requirements that concern the fairness and correctness of the election tally (one person, one vote). At the same time, they require that the votes cast by citizens remain secret. Therefore, citizens must authenticate (this authentication may be based on a unique identifier or on a securely generated pseudonym), but the data they submit must remain anonymous and unlinkable to their identity.

- **Type IV: Authenticated submission of authenticated data.** Citizens must often submit authenticated data when accessing e-government services (e.g., Declaration, Registration or Enrolment). In this case, the citizen must prove his identity (which can be based on a unique identifier or on a secure pseudonym) and sign the data.

3.2.3.2 Flow

In order to describe the flow of these transactions in a general way, we use the following terminology:

- User: citizen who submits the data

- Server: portal that serves as interface for e-government services

- Database: repository where the information is stored

3.2.3.3 Submission Type I

1. The user challenges the server to prove that it is an authentic server

2. The server proves that it is an authentic server

3. The user submits the data to the server (e.g. using a web based form)

4. The server forwards the submitted data to the database

5. The database stores the submitted information

3.2.3.4 Submission Type II

1. The user challenges the server to prove that it is an authentic server

2. The server proves that it is an authentic server

3. The server challenges the user to prove that he/she fulfills the required attributes

4. The user proves that he/she fulfills the attributes

5. The server gives the user access to the specific web based form
6. The user submits the data to the server
7. The server forwards the submitted data to the database
8. The database stores the submitted information

3.2.3.5 Submission Type III

1. The user challenges the server to prove that it is an authentic server
2. The server proves that it is an authentic server
3. The server challenges the user to prove his identity (could be pseudonymous)
4. The user sends authentication information (could be pseudonymous)
5. The server gives the user access to the system
6. The user submits the anonymized data to the server (e.g., in such a way that the data cannot be linked to the user's (identity) authentication data)
7. The server forwards the anonymized data to the database
8. The database stores the submitted information

3.2.3.6 Submission Type IV

1. The user challenges the server to prove that it is an authentic server
2. The server proves that it is an authentic server
3. The server challenges the user to authenticate himself (could be pseudonymous)
4. The user sends authentication information (could be pseudonymous)
5. The server gives the user access to the system
6. The user submits authenticated (signed) data to the server
7. The server forwards the submitted data to the database
8. The database stores the submitted information
9. The server returns a (signed) receipt to the user that he has received the signed data and that the registration/declaration has been accepted

3.2.4 Requirements E-government Use Cases

Many of the requirements that inquiry and submission services must fulfill are common to most e-government applications. First of all, the goal of any electronic service is to be used, it is thus important that the service is usable for non-expert users. Usability aspects include a good quality of service in terms of performance and availability of the service, as well as the ease of use for the average citizen.

E-government services should also be affordable in order to be deployed. And, given the large amount of citizens expected to access these services, they should also be scalable with the number of users.

These systems should also provide digital evidence to law enforcement in order to deal with unauthorized accesses and cases of identity theft.

The security is particularly important to prevent the possibilities of abuse and enhance trust in the system. The confidentiality of the information should be protected, so that unauthorized third parties are not capable of eavesdropping on the communication between the citizen and the e-government service. Maintaining the integrity of the information is of crucial importance, as otherwise malicious entities could modify this information and either present to the e-government server to the user with manipulated data. As the user may be obtaining official statements with legal value, it should not be possible for the server to deny having produced the document. Therefore, the server may have to produce some signature on the information in order to ensure non repudiation properties.

While inquiries type I and submission of type I do not require authentication because any citizen has the right to access this information or anonymously express their opinions, users performing inquiries type II should prove that the data they are requesting is their own, and users performing submissions of type II must prove certain attributes. Submissions of type III and IV as well as inquiries type III require that the user authenticates before accessing or submitting the data.

When only users who fulfill certain conditions, like belonging to a specific professional group, are authorized to access data, the server is responsible for implementing the necessary access control mechanisms.

In order to preserve the privacy of users, the level of identification should be the lowest necessary to ensure that the security and legal requirements are fulfilled. Inquiries type I and can be made anonymously, as the information being requested is public. Inquiries type II can be made pseudonymously, as the server needs to be convinced that the requester of data is the owner of it, but does not need to know his identity. Inquiries type III may require identification for legal reasons, although in some cases it may be enough if the requester of the information is known by a pseudonym to the server and capable of proving that he has certain attributes that authorize him to access the requested data.

Submissions type I and II can be made anonymously. Submissions of type III should be done is such a way that the server should not be able to link the data with the identity of the authenticated user, i.e. the data should be first anonymized. Submissions type IV require authentication of the citizen and the data submitted.

Entities who do not participate in the protocol should not be able to determine that the user is accessing the service. In order to achieve this, the user should have an anonymous communication channel that prevents other entities from learning about the access. This may be particularly important in cases in which the fact of accessing the information leaks sensitive data of the use; e.g., accessing information on government programs to rehabilitate people with drug addictions or in case of e-voting, when it should not be possible to link the identity of the voter with his vote.

Another threat to privacy appears when all the actions of the user can be linked together, as the information accumulated by combining all of the users' actions (either at the communication or at the data layers) may enable a very sophisticated profiling of the user. Therefore, whenever possible the actions of the user should be unlinkable to each other. In our case, subsequent inquiries of type I and type II and submissions of type I, II and III should be unlinkable to each other.

3.3 Trusted Archival Use Cases

3.3.1 Introduction

We require a large-scale high-availability disaster-proof archive for many of the ADAPID use cases. This archive can be used for archiving requirements such as transaction data, banking data, medical data, CRL lists, etc. Our first use case *Criminal Records for Road Hogs* discusses the storage and retrieval of digital pictures of traffic speed infringements. We discuss at great length the properties of the archive.

The archive must offer a high service level. Data must be retrievable fast and from everywhere, regardless of the client device. Also, there must be very strict policies on how data can be removed from the archive. These are called retention policies. The second use case *Personal Medical Information* discusses the storage, retrieval and retention of personal medical information.

Finally we need a 'trusted' archive. Digital signatures do not have the strength to provide non-repudiation over decades. Therefore, they must be completed with a trusted archive. Our third use case *Long-Term Archival of Digitally Signed Documents* is all about longevity. How can we store digitally signed documents for decades, yet keep them readable and accessible all the time, and provide non-repudiation over such a long period of time.

In the next section, we describe three use cases. In the first use case Criminal Records for Road Hogs we discover many aspects of a Trusted Archival Service (TAS). We try to highlight the concerns of the various parties involved. These are both technical and operational. In the second use case Personal Medical Records we focus on the compliance legislation and Event-Based Retention (EBR). In the third use case Longevity of Digitally Archived Documents we focus on the more tricky aspects of data longevity.

3.3.2 TAS Case 1: Criminal Records for Road Hogs

Assume a system on which all information about traffic speed infringements is stored. This includes date, time, location, traffic and weather information, type of speed camera, proof of calibration of the speed camera, one or more photos of the infringement, vehicle type, license plate, identification of the driver, traffic fine, date of payment, digital (or digitized) signatures of the police officer issuing the traffic fine, digital (or digitized) acknowledgment of the driver that he drove too fast, and possibly many other legal documents and information.

The system must be capable of storing the information related to millions of speed infringements. This will involve managing several million individual documents, with complex relations between the documents. The scale of the system can grow to several Petabytes. Since the TAS is used for government data, it might be required to store data for several decades, up to a century. Longevity of legal data is a key aspect, which is solved in the analog world by expensive paper or microfilm archives. A cheaper and more reliable alternative is desirable.

Under intense usage, hardware typically does not survive more than 5 years. The so-called bath-tub curve shows an exponential increase in component failure rate after the component lifetime, especially if the hardware has to be cheap. This means that huge disk-based archives will have disk failures every week or almost daily. It is key that the system can protect its data without waiting for the storage administrator to replace failed hardware parts. Instead, the system should start self-healing the unprotected data immediately. Later, the administrator can replace broken hardware parts without downtime.

It is also required that the storage admin can purchase extra hardware as needed; i.e., that no gigantic upfront investment is required. Scaling up the size and capacity of the TAS should go seamless, and should not result in difficult reconfiguration of the TAS and its clients, nor should it result lower system performance or availability.

Finally, hardware and software errors will be detected in the TAS hence upgrades will be required regularly. In order to make these as painless as possible, both software and hardware upgrades must be non-disruptive; i.e., no data unavailability or reduced performance during upgrade.

The system must be affordable. The Total Cost of Ownership (TCO) must be reasonably low. This includes both the one-time purchase cost, and the recurring costs such as support, administration, electricity, floor space, cooling, etc.

The system must provide a high degree of reliability and availability. Reading and writing data must be permanently possible at an acceptable performance. The system must not have a Single Point of Failure (SPOF), which is possible by introducing redundancy in the system (network, CPUs, RAM) and by protecting the data (e.g., by storing two instances of every file). Data Loss / Data Unavailability (DU/DL) must be avoided in case of hardware failures (solid state memory/disk/tape, processing unit, network interfaces and switch, power supply, cooling systems, etc.) or in case of software errors.

The combination of one or more hardware or software failures might be bring the data in an unprotected state. The data redundancy level must be restored as quickly as possible. Ideally, the system should start re-protecting the data immediately, and should not wait for replacement of the broken hardware parts. This self-healing should involve as little human interaction as possible, in order to minimize cost. For example it is not preferred that the storage administrator has to come and replace a broken disk on Friday night, but also it is undesirable that the data is vulnerable to a catastrophic failure during the entire weekend.

In the event of a fire, storm, earthquake, flooding, or terrorism, the full TAS system might be destroyed. In order to restore the data availability, a disaster recovery scheme must be deployed. This can involve cheap techniques such as backup and restore. During the restore period, which can take several days or weeks, the data is unavailable on the production system, and the TAS is not usable. At the other end of the spectrum there are expensive techniques such as multi-site synchronous replication, which requires deploying multiple TAS systems at several geographically scattered locations.

A very strict access control system consisting of both authentication and authorization must allow the data to be retrieved/viewed by authorized persons only. In order to maximize the usability of the system, it is important that one does not have to be physically close to the storage system, in order to get authorized to the data. Authentication using the e-ID card is very desirable as it uniquely identifies a citizen.

A very granular authorization scheme (e.g., access rights per file) might be required, but one should not forget the complexity to manage access rights for millions of users (citizens) and many millions of files. A more dynamic as-needed authorization scheme might be required, based on policies (e.g., all traffic infringements in 2005, or all traffic infringements in the Center of Brussels, all traffic infringements committed by a certain citizen). We might take a look at ODRL (Open Digital Rights Language) concepts and primitives to build a scalable authorization scheme.

The TAS must support a high level of confidentiality. Preferably, data is not sent over the wire in cleartext, but instead it is encrypted before leaving the TAS. Even better is to encrypt all data on the system. The typical example is the cleaning lady who can steal a disk or a tape from the storage system, and this way gain access to some of the data stored on the system. This would violate the access control and confidentiality we want to impose on the information.

If all data is encrypted on the system, then the key management must be organized properly and securely. This problem is a huge technical, organizational and legal challenge. Solutions might depend a lot on local legislation. For example key escrow might be forbidden in one country, yet be a requirement in another country. The complexity of this problem is one of the reasons why the e-ID card does not contain an encryption key.

It is important that one cannot tamper with data on the system. For example, it is not acceptable that the measured speed can be changed, or that the vehicle license plate can be changed. All parties (e.g., driver and police) should agree upon the authenticity of the pictures, speed information, environmental information etc and it should not be possible for parties to repudiate the facts after they first have acknowledged them. Data integrity and non-repudiation are important requirements.

The legislation will state how long data has to be retained. The storage system must make it impossible for all parties to delete data that is under retention. There will be several retention periods. For example, the law could stipulate that the evidential photographs have to be retained for 2 years, but that the digital signatures have to be retained for 10 years.

Suppose that the law stipulates that after 10 years, the speed infringement has to disappear from the criminal record of the road hog citizen. It is in the interest of the citizen that the government can no longer refer to this speed infringement in future legal disputes. Therefore, the citizen wants the data to disappear as soon as it is allowed. This is called data expiration. This is also beneficial for the government, since deleting data might allow some storage capacity to be reclaimed, driving down deployment costs of the storage system.

The citizen wants to be assured that the government has forgiven his sins and can no longer retrieve information about his prescribed infringement. In the analog world, this could involve shredding or burning paper documents, photos and negatives, microfilm or magnetic tapes. For magnetic or solid state storage, there are several digital shredding methods to achieve the same goals.

3.3.3 Personal Medical Information

Assume a system with the full medical history of all citizens. The archive contains medical interventions, results of analysis, X-ray and other medical images, insurance information, health information about relatives, etc.

The archive can be consulted by doctors, hospitals, insurance agencies and patients. Very strict access control is required since all parties have different objectives and the information must be kept very confidential.

The full medical history will allow citizens to change doctors as they wish. They will not run the risk of losing their medical history or getting difficult access to it.

In case of an accident or an emergency, the medical information of the patient could be available to the emergency workers within seconds. This would greatly improve the medical service offered in case of an accident, for example by avoiding shocks due to an allergic reaction. Note that at this point the patient might himself not be able to offer biometrical identification or password. Possibly, that e-ID card of the patient could be used, together with strong authentication of the emergency worker, as to gain access to the confidential records.

The records themselves have to be stored on the TAS for very long periods of time (multiple decades up to a century). For example, legislation dictates how long after the death of a patient, a hospital has to archive X-ray images and MR scans taken during the patients lifetime. This is called event-based retention: based on an event (death of a patient), data is put under retention for X years (e.g., 7 years).

If the hospital is sued by relatives of the deceased, then data might be put under litigation. No party is allowed to delete the data while the litigation hold is on the data. The TAS has to enforce this, since the TAS needs to protect the interests of the patient, relatives, hospital, insurance company etc. In order to establish trust in the TAS system, probably some government involvement in the TAS deployment will be desirable (e.g., certification).

Storing medical records for all citizens for multiple decades, will cause huge scalability and deployment issues, since billions of individual files and documents have to be protected.

The access control is very tricky. The authentication and authorization to the documents will involve a lot of potential identities, which are not necessarily known by the organization who owns the data. We need to find out how to deal with this in an efficient manner. A central authority managing all authentication and authorization is probably not scalable. On the other, a decentralized model will require trust management. We can learn a lot from the deployment issues encountered with large scale PKI systems. We should not make the same mistakes. The various parties and roles should be very clear from the beginning.

3.3.4 Long-Term Archival of Digitally Signed Documents

Envision a Trusted Archive on which digitally signed annual account statements for millions of companies are stored. This is a public repository, which is used by suppliers, customers and investors to evaluate the financial and commercial state of those companies.

Today, this role is fulfilled by the National Bank of Belgium.

First of all, the TAS shall not lose data. It is a fact that all information carriers (CD, DVD, disk, tape, paper) wear out and age, and that information gets lost after anything between a few years and a few centuries. The physical longevity of the information carrier is critical. The TAS system must introduce redundancy and self-healing on its system such that individual events of information loss or corruption does not result in a system level event of losing data.

Next, the TAS system has to be used for many decades. In the past we have seen many technologies come and go (e.g., Minidisk). Even more important, the formatting of the data is important and the visualization technology (e.g., WordPerfect on Windows 3.1) has to survive several decades. Virtualization techniques and decent data migration capabilities are critical for technological longevity of the TAS.

Next, the TAS system lifespan might be larger than the lifespan of the company selling the TAS hardware and software. Also, even if the technology would last for a long time, the operator of the TAS still needs to be able to find employees or consultants having an adequate level of technological knowledge to operate the TAS. This might be a problem for old technology. We call this requirement the business longevity.

Finally, the TAS system needs to guarantee integrity and authenticity of the documents it stores. The TAS is a critical component in order to ensure trust longevity. The TAS is an essential part in the trust chain which is validated to verify that a document that was digitally signed decades ago, was valid at that point in time. This is a largely unsolved technical, organizational and legal challenge.

3.4 Financial Use Cases

3.4.1 Introduction

Financial institutions and applications will benefit as one of the best from the electronic ID card projects. They have intensive need to authenticate persons, to copy a proof of their identity, or to let them sign documents or agreements. One possible appliance, that is already widespread, is the case of internet banking.

However, in this section we want to discuss some more advanced use cases, where people can perform daily financial and/or business requirements using their ID card credentials. These appliances will become more useful as they are understood and accepted better by a wider range of the public. As an example we can point to the different trusted third party services, who will each perform one clear task. For example in the contract negotiations example below, the trusted third party is used as an neutral third party. Our use cases are (some of them will be elaborated further):

3.4.1.1 Buy shares from an IPO

A private person wants to order shares from the IPO (Initial Public Offering) of his favorite company. The person will execute the transaction over the internet. The data is send over publicly available lines, and has to be encrypted. The person has to authenticate himself, and it must be able to proof that the person has put the order afterwards. Also, the private person must have proof that he put that order.

3.4.1.2 Authentication on a bank website

A public bank offers a website service. Both private persons and bank persons are able to log into this service. The authentication has to be 'bullet-proof'. The clients can use an e-ID card to log in. The web server generates a challenge, that is first verified and then signed by the client using a registered e-ID card and the corresponding pin code and fingerprint. The signed challenge is send back and the web site opens the SSL connection.

3.4.1.3 Contract negotiations over the public web

Company A and company B engage in discussions about a possible contract. Company A can start by sending a signed NDA (Non-disclosure agreement) in pdf form over the internet. A qualified person of company B uses his/her e-ID card to verify the first signature and sign the NDA in return. The NDA is send back. Both companies have an NDA PDF file that is signed by both companies. This can serve as legal proof in court.

3.4.1.4 ERP system automated orders

Company A has installed an ERP system (Enterprize Resource Planning system) to manage the resources and the stock. If a stock runs below a specified level or if the system foresees a shortage of a specific resource, it will generate an automatic order. This order can be in html format, and can be signed by a credential that is furnished by a trusted third party (TTP). The TTP has furnished this credential for a maximum liability of 10,000 euros, in return for a signature of the e-ID card of a qualified person of the company A. The TTP requires every month a new e-ID signature with the registered e-ID card to extend the duration of validity of the credential.

3.4.1.5 Contract negotiations B

Company A has installed an ERP system (Enterprise Resource Planning system) to manage the resources and the stock. If a stock runs below a specified level or if the system foresees a shortage of a specific resource, it will generate an automatic order. This order can be in html format, and can be signed by a credential that is furnished by a trusted third party (TTP). The TTP has furnished this credential for a maximum liability of 10,000 euros, in return for a signature of the e-ID card of a qualified person of the company A. The TTP requires every month a new e-ID signature with the registered e-ID card to extend the duration of validity of the credential.

In the following section, three use cases will be described in detail. We have chosen the following scenarios for a more in depth discussion:

1. Bank transaction - Buy shares from an IPO,
2. Commercial business scenario - Contract negotiations and
3. Financial business process - ERP system automated orders

3.4.2 Bank transaction Buy shares from an IPO

3.4.2.1 Context

The process of an IPO (Initial public offering) is already a complex one at the moment. It is the first time that company shares will be distributed among public shareholders, and will be tradeable on a stock market. All the organization requirements for a successful IPO need to remain in place. This transaction can also be seen as a financial transaction over the public web. Is it possible to perform an IPO fully digitally, however still implementing the law requirements. The e-ID card can open up this possibility. Liability and non-repudiation are very important factors here.

3.4.2.2 Actors

The different actors in this scenario are:

- Interested parties. Users that would like to subscribe (the 'user')
- The financial consortium that manages the IPO (the 'IPO manager')
- The company that is the subject of the IPO (the 'IPO subject')

Each actor can have a responsible natural person assigned to be the end responsible for this actor. (Also for users, when a user is a legal entity)

3.4.2.3 Flow

1. The user authenticates on the private website
2. The digital ID card can be used to make a digital 'copy' of your e-ID card. This can then be signed by the user, replacing the need for a paper copy of the e-ID/ID card
3. IPO documents are presented to the authenticated user over a secure web interface. The user is able to read and download legal information, prospect and additional documents on which he or she can base the investment decision.
4. User can use ID card to put legally valid digital signature, stating that the user will buy the shares on a specific day, and stating the number of shares that the user wants to subscribe to
5. User enters signature PIN code. The user can see the first 4 letters of the hash on the screen of his smart card reader and on the screen of his desktop and is therefore more sure that what he signs is indeed what is shown in the application.
6. The signature and the digital copy of the e-ID card can be anonymized and sent to the 'IPO manager' Anomyzation is an extra guarantee for a fair distribution process. The anonymization should happen in a way that can be rolled back by the 'IPO manager' (to check the legitimately of the subscription), and afterwards, when the share distribution is done (to assign the shares)
7. A separated entity (Trusted Third Party linked to the IPO Manager) TTP removes all non-legitimate subscriptions
8. The 'IPO manager' manages all the inscriptions, and makes a final price and distribution based on the anonymous data
9. The 'IPO subject' will review the final price/distribution on the management site and put a digital signature to approve the transaction
10. Users are de-anonymized and notified in an encrypted way about their assigned shares
11. The IPO can start without any problems

3.4.3 Commercial business scenario - Contract negotiations

3.4.3.1 Context

Commercial businesses are done mostly by the use of contracts. The contract negotiation process is usually an extensive process where the contract travels a lot between different parties. It would be very useful to be able to do this online using an online contract negotiation scenario. We believe the e-ID card is suited to make this scenario usable in the real world. For the following scenario, we will consider the case where a commercial company wants to sign a contract with a partner company.

3.4.3.2 Actors

The different actors in this scenario are:

- Commercial company A ('company A')
- Commercial company B ('company B')
- Trusted Third Party ('TTP')

Each actor can have a responsible natural person assigned to be the end responsible for this actor.

3.4.3.3 Description / Flow / Basic

A basic scenario is described first:

- Company A sends NDA (Non disclosure agreement) in signed PDF over email line. Company B signs the document and sends it back over email. Both companies now have the mutually signed document. However, the risk exists that one of the companies stops the process and at that time is in possession of a signed contract by the other party only.
- No signing of multiple copies is required and after contract negotiations, the same basic flow is executed for the contract.

3.4.3.4 Description / Flow / Extensive

To make the process more secure, an alternative advanced scenario is described in the following:

1. Company A logs in on trusted third party (TTP). The authentication can be done using an e-ID card, or a credential that has been distributed to the company before.

2. Trusted third party holds the documents. Both the non signed, and the signed documents. If an adaptation is made to the contract during the course of the negotiation, the process is started over.
3. Company A signs NDA (non-disclosure agreement), and uploads it to TTP. Alternatively, the NDA is first uploaded or is provided as a standard NDA by the TTP.
4. Company B logs in to TTP, and signs the NDA using the e-ID card or the company credential received.
5. At this time (the NDA is mutually signed), the TTP will notify both parties that the NDA is legally binding, and both parties will receive a mutually signed version
6. The TTP will retain an archive of the NDA/contracts, and both companies can be hold liable for the contract. After NDA negotiations, the same flow is executed for the contract negotiations.

3.4.4 Financial business process - ERP system automated orders

3.4.4.1 Context

A lot of companies organize their business logic around their resources. This can be done by using an 'Enterprize Resource Planning' system, that will, among other things, take care for them that resources are always available to manage the current tasks. The aim of this scenario is to investigate how ERP packages can be authorized in a legal way to generate and send out automated orders. This scenario will make use of the e-ID card to accomplish this.

3.4.4.2 Actors

The different actors in this scenario are:

- Commercial company A ('company A')
- Commercial company B ('supplier')
- Trusted Third Party ('TTP')

Each actor can have a responsible natural person assigned to be the end responsible for this actor.

3.4.4.3 Flow

1. A trusted third party is visited by the product manager of company A. This step can be done online, if the product manager is able to authenticate himself and to put a legally valid signature. During this step, the following actions will be performed: -Product manager signs a note for 10,000 euro using his card. This step can be done online too, providing the product manager uses a qualified certificate to sign (e.g., e-ID card). The trusted third party deploys a credential X, that is good for 10,000 euro in transactions.
2. Product manager uploads the credential in the ERP server. From now on, the approval of the product manager is not required for every order of the ERP system.
3. The ERP server makes automated orders for over 9,000 euro during a certain amount of time. The product manager has to make sure this timespan is workable. The Trusted third party however will try to keep this timespan as short as possible to limit liabilities. The exact timespan will thus be a result of negotiations.
4. The ERP server makes a note to the product manager to update the credential. The credential is only valid for 10,000 euro and there is only 1000 euro left. The product manager has some time to revalue the credential.
5. The suppliers have a contract with the trusted third party, and they receive their money from the trusted third party.

3.4.5 Requirements of the Financial Use Cases

In this section, we will give a summary of the requirements for successful financial scenarios using the e-ID card. We will base ourselves on the three developed scenarios, but also other financial scenarios will be seen to have the same requirements.

Usability. It is very important that a system is usable and does not require too complex or too many tasks to perform a simple basic transaction. Some of the underlying requirements are: stability, response time, visibility.

Confidentiality. As we have seen in practically all the scenarios, confidentiality is a very important aspect in financial transactions. Note that in contract negotiations it is essential that no other party knows about the content of the contracts.

Integrity. For financial transactions like payments, orders, financial states, etc., it is very important that the data cannot be altered. Also that can be verified that it was not altered, and that it was send by the right instance.

Anonymity. In some cases, anonymity of the applier can be important (e.g., the example for the IPO scenario). In most cases also unlinkability is important and must be ensured by the network or the data layer. Pseudonymity can be a way to implement the anonymity required.

Legally valid signatures. An important factor for financial transactions are legally valid signatures. A signature must be legally valid, and it must also be possible to verify that a signature is legally valid. A good archival service is essential to keep record of the legally valid signatures that have been issued.

Liability. In almost every case the person who signs something (order form, contract, etc.) is liable for his actions. This liability must be enforceable.

Legal identification. An extra requirement for financial transactions, that we did not find back in other use case categories is the need for 'legal identification'. Before the digital age, and still in use until now, this was done by making a paper copy of the ID document. In the scenario descriptions here, we proposed an alternative for this by using a digital copy, or a digitally signed scan of the document. Another alternative would be to provide proofs of identity that do not reveal personal data (pseudonymous credentials). It is essential for most of the scenarios above to be useful that this form of legal identification is accepted by law.

Chapter 4

Requirements

4.1 Functional Requirements

Traditional ID cards have been used for the identification of citizens in a variety of contexts (transactions with the administration, private contracts, etc.). The use of traditional IDs, however, was bound to the physical presence of the card owner. The authentication was performed by visual check of the picture on the card and comparison with the face of the holder. Alternatively (or complementarily), the card holder could be challenged to produce a signature that would be compared to the one visible in the card.

The migration from paper-based to electronic ID cards enables extended functionalities. Personal data stored in the e-ID can be read much more efficiently when a citizen uses it to identify in person. But now the card can also be used for identification and authentication in online applications. Citizens may use the card to sign online contracts, access to e-government services, e-health services, or trusted archives, among other applications. We discuss below these functionalities more in detail.

The rest of this chapter studies all the other requirements that the e-ID should comply with. It is organized as follows:

- One of the essential aspects of e-ID cards is their security. If the card is not secure, it will not generate the necessary trust to serve as identification and identity management token. We describe the security requirements in Sect. 4.2.

- As the e-ID card contains personal information (such as name, birth date, gender, etc.), it is subject to regulations on Privacy and Data Protection, which are studied in Sect. 4.3. As we explain in Sect. 4.4, data gathered from or though interaction with the e-ID card should not serve as basis for any sort of discrimination.

- One of the main functionalities of electronic e-ID cards is to provide the necessary infrastructure to enable electronic signatures. The requirements for electronic signatures are described in Sect. 4.5.
- Electronic ID cards are issued by and form part of the national administrative infrastructure. While the traditional administration used to function based on paper documents, the introduction of electronic technologies has enabled the use of electronic documents. As these documents need to be kept securely for long periods of time, there are strong requirements on the way they are stored. The requirements for secure, long term archives are presented in Sect. 4.6.
- Accountability mechanisms have to be put in place in order to deal with abuse, crime and identity theft problems. We analyze in Sect. 4.7 the requirements for allow law enforcement to deal with abuse cases.
- The goal of the e-ID card is to provide trusted means for online transactions. In Sect. 4.8, we analyze the concept of trust, its legal implications, and the different trust models that can be implemented.
- The requirements of the physical card, the technologies for e-ID cards, and the contents of the card are discussed in Sect. 4.9.
- There are important practical aspects related to the usability, quality of service and cost of deployment of the e-ID infrastructure. We have analyzed in Sect. 4.10 the affordability and usability requirements.
- Finally, and taking into account the increased cross-border mobility of citizens, it is important to take into account the requirements for international interoperability. These issues are studied in Sect. 4.11.

4.1.1 Identification

The e-ID card, just as traditional ID cards do, serves as identification token when shown by a citizen who is physically present. Moreover, e-ID holders may identify themselves in online applications.

4.1.2 Data extraction

Interactions with the administration often imply filling forms with personal data: name, birthdate, address, etc. These data are kept in the e-ID chip, and they are electronically readable. Capturing the data directly from the card reduces the time needed to complete the transaction, and eliminates the risks of transcription mistakes.

4.1.3 Electronic signatures

The development of e-business requires a common understanding of what constitutes an electronic signature amongst the parties involved. In practice a wide variety of technologies is in use, from very simple to highly sophisticated.

The e-ID card provides secure electronic signature functionalities, being the public key certificate backed by the national administration.

The generation of an electronic signature on a document requires the e-ID holder to introduce a PIN.

4.1.4 E-government services

Traditionally, users were required to physically go to government offices in order to perform transactions (request of travel documents, tax declaration, request for social benefits, etc.).

There is an increasing interest in offering the possibility of online E-Government services. This would increase the convenience for citizens as well as reduce the costs of operation for the pubic administration.

4.1.5 E-health services

Containing all necessary credentials to authenticate a patient, a doctor, a nurse, or a pharmacist, the e-ID card would play an essential role in any transaction the electronic health-care system might offer. In addition, by using an appropriate user-centric architecture, as well as the "right" cryptographic techniques, it is possible to make the system secure, accountable, and yet privacy-friendly with respect to the patient. More specific e-health requirements can be found in Sect. 3.1.8.

4.1.6 Trusted storage services

There is a variety of information to be stored in an e-ID enabled application. One can think of digitally signed official documents, medical records, personal tax sheets, etc. They all need to be stored in a reliable, performant, secure, forward compatible and affordable Trusted Archive. The panoply of requirements for a TAS (Trusted Archival Service) can be found in Sect. 4.6.

4.2 Security Requirements

4.2.1 Confidentiality

4.2.1.1 Definition

Confidentiality refers to the state of keeping the content of information secret from all entities but those authorized to have access to it.

There are numerous approaches for providing confidentiality ranging from physical protection to mathematical algorithms which render data unintelligible.

4.2.1.2 Reference to use cases

Keeping information secret towards entities that do not have any need or legitimate interest on it, is an effective measure to prevent illegitimate use of the data. Confidentiality is particularly relevant when sensitive data (such as health related information) is concerned.

The confidentiality of the information should be protected, so that unauthorized third parties are not capable of eavesdropping on the communication between the citizen and the e-government service or e-health services. In case of e-health the confidentiality of the health records must be maintained.

4.2.1.3 Technical issues

There are two types of encryption algorithms that can be used for achieving confidentiality, which are symmetric-key and public-key encryption schemes [MvOV96].

A symmetric encryption scheme may be used as follows. Two parties Alice and Bob first secretly choose a key k. At a subsequent point in time, if Alice wishes to send a message m to Bob, she computes $c = E_k(m)$ and transmits this to Bob. Upon receiving c, Bob computes $D_k(c) = m$ and hence recovers the original message m.

A public-key encryption scheme may be used as follows. Alice has a key pair (d_A, e_A) of private and public keys. Bob also has a key pair (d_B, e_B). The public keys e_A and e_B are published. At a subsequent point in time, if Alice wishes to send a message m to Bob, she uses the public key of Bob and computes $c = E_{e_B}(m)$ and transmits this to Bob. Upon receiving c, Bob computes using his private key $D_{d_B}(c) = m$ and hence recovers the original message m.

4.2.1.4 Legal issues

An obligation of confidentiality may find its basis in an agreement or be imposed directly by law. In some cases, a breach of confidentiality is a criminal offence, for instance in the health care sector. More generally, the regulation on data protection [1] provides that personal data must be treated as confidential by the data controller.

Applications should be able to distinguish between confidential and non-confidential data. Confidentiality is never absolute but relative to the person requesting access, thus there must be some way of determining who may have access to data under which circumstances. This may vary over time, for instance after the death of the data subject.

4.2.1.5 Deployment

There are many available cryptographic algorithms that provide confidentiality. However, the current version of the e-ID does not provide encryption/decryption functionalities. One of the main problems of storing encryption/decryption keys in the e-ID card is that the card may get lost, making it impossible to decrypt data. In order to solve this problem, some back-up or key escrow mechanism needs to be implemented.

4.2.2 Integrity

4.2.2.1 Definition

Integrity is the quality of the items of interest (facts, data, attributes etc.) indicating that they have not been subject to manipulation (insertion, deletion, substitution etc.).

Definition of the term integrity according to archival science: "The quality of being whole and unaltered through loss, tampering, or corruption."

4.2.2.2 Reference to use cases

For example, in the e-government use case "Inquiry" maintaining the integrity of the information is of crucial importance, as otherwise malicious entities could modify this information and either present to the e-government server a different request or provide incorrect data to the user. For e-health: The integrity of the prescriptions must be guaranteed as well as the integrity of the health records. A medical cost reimbursement statement must be also integrity protected.

[1] Act of 8 December 1992, *Belgian State Gazette*, 18 March 1993

4.2.2.3 Technical issues

The cryptographic primitives that are used for achieving data integrity are message authentication codes (MACs) and digital signatures [MvOV96]. Hash functions are used for data integrity in conjunction with digital signature schemes, where for several reasons a message is typically hashed first, and then the hash-value, as a representative of the message, is signed in place of the original message. A distinct class of hash functions, called message authentication codes (MACs), allows message authentication by symmetric techniques. MAC algorithms may be viewed as hash functions which take two functionally distinct inputs, a message and a secret key, and produce a fixed-size output, with the design intent that it will be infeasible in practice to produce the same output without knowledge of the key. MACs can be used to provide data integrity and symmetric data origin authentication. A digital signatures is a data string which associates a message with some originating entity.

A typical usage of (unkeyed) hash functions for data integrity is as follows. The hash-value corresponding to a particular message x is computed at time T1. The integrity of this hash-value (but not the message itself) is protected in some manner. At a subsequent time T2, the following test is carried out to determine whether the message has been altered, i.e., whether a message x' is the same as the original message. The hash-value of x' is computed and compared to the protected hash-value; if they are equal, one accepts that the inputs are also equal, and thus that the message has not been altered. The problem of preserving the integrity of a potentially large message is thus reduced to that of a small fixed-size hash value. Since the existence of collisions is guaranteed in many-to-one mappings, the unique association between inputs and hash-values can, at best, be in the computational sense. A hash-value should be uniquely identifiable with a single input in practice, and collisions should be computationally difficult to find (essentially never occurring in practice).

4.2.2.4 Legal issues

Integrity plays a significant role in the evaluation of evidence. However it is in the first place the integrity of the content that counts, and not that of a particular bitstream.

The data protection act [2] imposes an obligation on data controllers to protect the personal data in their care against unauthorized modification or destruction.

[2] Act of 8 December 1992, *Belgian State Gazette*, 18 March 1993

4.2.2.5 Deployment

The integrity of the data contained in the chip is protected by a digital signature generated by the card issuer (the government). Anybody who has access to the card can read out the information it contains: public key certificates, personal data of the card owner, etc. However, only the card issuer can modify the contents of the card.

The current version of the e-ID card does provide integrity protection of statements generated by the card owner through digital signatures.

In the case of the role-certificate authentication, then the information is integrity-protected with MACs. The MACs are calculated using a session key agreed on during the role-certificate authentication.

4.2.3 Non-repudiation of origin

4.2.3.1 Definition

Non-repudiation is the concept of ensuring that an action cannot later be denied by one of the entities involved.

With regard to digital security, non-repudiation means that it can be verified that the sender and the recipient were, in fact, the parties who claimed to send or receive the message, respectively. In other words, non-repudiation of origin proves that data has been sent, and non-repudiation of delivery proves it has been received.

Non-repudiation of origin and delivery are very important for assuring legal effectiveness to actions done in a digital context (e.g., signing a contract).

In Europe, electronic signatures which are based on a qualified certificate and created by a secure-signature-creation device enjoy a particularly privileged legal status. The EU e-Signatures directive provides that such qualified electronic signatures must be awarded the same legal effectiveness as a handwritten signature in the entire EU. This does not prevent the use of other technologies to fulfill a non-repudiation function.

When disputes arise due to an entity denying that certain actions were taken, a means to resolve the situation is necessary.

4.2.3.2 Reference to use cases

As the user may obtain official statements with legal value, it should not be possible for the server to deny having produced the document. Therefore, the server may have to produce some signature on the information in order to ensure non repudiation properties. In e-health applications the doctor should not be able to deny that he has changed the health records. The patient should not be able to deny that he/she has been consulted by a doctor. A doctor cannot deny having written a prescription to the patient.

4.2.3.3 Technical issues

Non-repudiation is achieved in the current e-ID version by using digital signatures [MvOV96].

4.2.3.4 Legal issues

¿From a legal point of view, non-repudiability is a consequence of the availability of reliable evidence. The general rule is that all evidence is admissible in court and that the judge assigns legal value to it as he sees fit. In some cases, the law limits what kind of evidence is admissible, which in turn impacts the technologies that may be used to ensure non-repudiability. A prime example of this is the role reserved for signed written evidence in civil law, as explained in Sect. 4.5.

4.2.3.5 Deployment

The current version of the e-ID provides non-repudiation by using digital (qualified) signatures.

4.2.4 Authentication

4.2.4.1 Definition

Authentication is the corroboration of a claimed set of attributes or facts with a specified, or understood, level of confidence. Authentication serves to demonstrate the integrity and origin of what is being pretended.

Authentication may be used during any IDM process. The security and reliability of authentication mechanisms may vary dependant on the desired authentication level. The stronger the authentication, the higher the confidence that an entity corresponds with the claimed set of attributes.

During the authentication process, one makes often use of credentials.

Authentication is typically subdivided into two separate classes: data authentication and entity authentication. For this reason, autonomous use of the term authentication (without specifying the type of authentication) should be avoided, as it is subject to (mis)interpretation. Authentication can be unilateral or mutual. Unilateral authentication provides assurance of the identity of only one entity, where mutual authentication provides assurance of the identities of both entities.

This function applies to both entities and information itself. Two parties entering into a communication should identify each other. Information delivered over a channel should be authenticated as to origin, date of origin, data content, time sent, etc. For these reason there are two types of authentication: entity authentication and data origin authentication. Data origin authentication implicitly provides data integrity (e.g., if a message is modified, the source has changed.)

Entity authentication is the process whereby one party is assured (through acquisition of corroborative evidence) of the identity of a second party involved in a protocol, and that the second has actually participated (i.e., is active at, or immediately prior to, the time the evidence is acquired).

Data origin authentication or message authentication techniques provide one party which receives a message assurance of the identity of the party, which originated the message. Data origin authentication implicitly provides data integrity since if the message was modified during transmission, the sender would no longer be the originator.

4.2.4.2 Reference to use cases

Authentication is required in most of the e-government and health scenarios. Nevertheless there are services providing information which is publicly available (e.g. type I of e-government use case "Inquiry") that do not require authentication because any citizen has the right to access this information. But for example users performing inquiries type II of the same e-government use case should prove that the data they are requesting is their own. Inquiries type III require that the user proves that he is authorized to access the data. This authorization is granted to users who fulfill certain conditions, like belonging to a specific professional group. In an e-health scenario patients and doctors must be able to authenticate each other.

4.2.4.3 Technical issues

Authentication serves to demonstrate the integrity and origin of what is being pretended (the claimed information) [MvOV96]. The security and reliability of authentication mechanisms may vary dependent on the desired authentication level. The stronger the authentication, the higher the confidence that an entity corresponds to the claimed set of attributes.

Authentication can be provided by digital signatures or MACs. There is a major difference between entity authentication and message authentication. Message authentication itself provides no timeliness guarantees with respect to when a message was created, whereas entity authentication involves corroboration of a claimants identity through actual communications with an associated verifier during execution of the protocol itself (i.e., in real-time, while the verifying entity awaits). Conversely, entity authentication typically involves no meaningful message other than the claim of being a particular entity, whereas message authentication does.

4.2.4.4 Legal issues

The Certification Service Providers Act (CSPA) [3] regulates the provision of qualified certificates. The e-ID certificates contain the National Registry Number of the citizen, use of which is regulated. Authentication will often entail the processing of personal data and must therefor happen in compliance with the data protection act.

4.2.4.5 Deployment

Authentication is often achieved by proving something you know (e.g., PIN or password), something you have (e-ID) and/or something you are (biometrics). In the case of the e-ID, authentication in the current version is performed by "something you have" (i.e., the physical e-ID card) and "something you know" (the PIN to the card).

The citizen authentication works in four steps:

1. Prepare the card for a particular signature (either qualified signature or authentication signature)
2. Verify the citizen PIN
3. Send the hash-to-be-signed to the card
4. Collect the signature

Before accepting modifications in the data contained in the chip of the e-ID card, the card authenticates the entity trying to make the modification through role-certificate authentication. Only the National Registry is entitled to perform such modifications.

The role-certificate authentication works in five steps:

1. Collect a random challenge from the e-ID card
2. Digitally sign the challenge (by the external party)
3. Send the signature back to the e-ID card
4. e-ID card verifies the signature using the genuine copy of the role certificate's issuer to verify the role certificate
5. Send the commands to the card that require particular roles

[3] Act of 9 July 2001, *Belgian State Gazette*, 29 September 2001

4.2.5 Access control - Authorization

4.2.5.1 Definition

Authorization refers to:

1. the permission of an authenticated entity to perform a defined action or to use a defined service/resource;
2. the process of determining, by evaluation of applicable permissions, whether an authenticated entity is allowed to have access to a particular resource.

Access control is restricting access to resources to privileged entities.

Access control works at a number of levels: There are access control mechanisms that work at application level and for the user they are expressed as a very reach and complex security policy. The applications may be written on top of middleware (such as a database management system), which enforces a number of protection properties. The middleware will use facilities provided by the underlying operating system. As this constructs resources such as files and communication ports from lower-level components, it acquires the responsibility for providing access ways to control access to them. Finally, the operating system access controls will usually rely on hardware features provided by the processor or by associated memory management hardware.

4.2.5.2 Reference to use cases

The server is responsible for implementing the necessary access control mechanisms that ensure that information is only made available to those entitled to access it. There are different access control techniques (see technical aspects). In use case “Inquiry” type II can be used user based access control, whereas in type III role based access control is more suitable.

In E-health applications a patient need to be able to authorize the doctor to access his/her health records. Different categories of doctors should have different access rights to the system, e.g. ER doctors should have access to the patient medical records not necessarily after the patient’s authorization (e.g. in case of emergency). This will not apply to GP doctors or doctors - specialists.

4.2.5.3 Technical issues

One type of Access Control is the so called Role Based Access Control [MvOV96]. The basic concept of Role Based Access Control is that users are assigned to roles, permissions are assigned to roles, and users acquire permissions by being members of roles. Core RBAC includes requirements that user-role and permission-role assignment can be many-to-many. Thus the same user can be assigned to many roles and a single role can have many users. Similarly, for permissions, a single permission can be assigned to many roles and a single role can be assigned to many permissions. Core RBAC includes requirements for user-role review whereby the roles assigned to a specific user can be determined as well as users assigned to a specific role. A similar requirement for permission-role review is imposed as an advanced review function. Core RBAC also includes the concept of user sessions, which allows selective activation and deactivation of roles.

Usually, authorization is used in the context of authentication. Permission is granted or denied based on the result of data or entity authentication, and on the allowed activities, as defined within the system. Once an entity is authenticated, it may be authorized to perform different types of access, each of which is referred as a role.

4.2.5.4 Legal issues

The data protection act's provisions on fully automated decisions may apply to access control mechanisms, insofar as certain criteria are met. In numerous cases, the law specifies who may have access to certain data or systems. The data protection act gives every data subject a limited right of access to his personal data.

Failure to correctly enforce access control may lead to a breach of confidentiality, which may give rise to civil or even criminal liability.

4.2.5.5 Deployment

The e-ID card does not implement access control mechanisms to read the personal data and public key certificates stored in the card. The private keys used to generate signatures cannot be exported from the e-ID card.

Concerning the write access, the citizen-related files (identity and address files, citizen photo, certificates, etc.) can only be updated by the government (i.e., national register). The national register uses for that purpose role-based certificates. The task of "updating an address file" corresponds to a certain role, creating a new directory in the card's file structure corresponds to another role, etc.

After a successful authentication with a role-certificate, the card will accept all the commands that correspond to the roles mentioned in that certificate. The e-ID card holds a genuine copy of the public key of the CA issuing the role certificates which is used for verification purposes.

4.2.6 Anonymity, Pseudonymity, Unlinkability and Unobservability

The use of identity data by default in electronic transactions enables serious risks for the privacy of e-ID holders. In most cases, identity data is not necessary to carry on secure transactions, where all parties are ensured that their requirements are met. The identity data is stored along with transactions that may reveal sensitive personal information (e.g., sexual orientation or religious beliefs). As the security of the databases storing this information cannot be one hundred per cent guaranteed, there is the possibility of these data being used for illegitimate purposes. Moreover, if data gathered by databases in different domains contain common identifiers (such as the national ID number), the possibilities of aggregating huge amounts of data on all users of the e-ID card grow dramatically. The possession of such extensive information on large amounts of people would enable very sophisticated profiles that could be used for criminal purposes such as identity theft, or for unfair commercial practices, such as price discrimination. In scenarios where human rights and legal guarantees are not respected, this information could also be abused for undermining civil liberties or exercising discrimination on minorities.

These risks can be greatly reduced by implementing security mechanisms that rely on anonymous or pseudonymous authentication and access control technologies. Pseudonyms belonging to unrelated domains can be unlinkable to each other, and to identity data that could lead to the physical person who owns the e-ID card. This reduces the risk of constructing multi-domain profiles that can be related to physical people. In cases where the user only reads information, there is often no need to maintain a permanent identity of (pseudonym) of users. In these services, the access can be made anonymously and subsequent transactions can be unlikable to each other. There are contexts where the mere fact of communicating may already threaten the privacy of a user (for example, in certain countries with undemocratic regimes, the access to anonymous communication networks is censored as soon as it is detected). In these cases, the user may need to use an unobservable channel for the communication.

We now describe more in detail anonymity, pseudonymity, unlinkability and unobservability. We first define these terms; then, we link them to the context of the use cases presented in the previous chapter; we describe the technologies that have been developed to provide the described properties; we discuss their legal implications; and finally we address some deployment issues.

4.2.6.1 Definitions

The definitions provided by Pfitzmann, Hansen *et al.* in [PH01] have a wide consensus and have been adopted in several identity management projects. We reproduce here these definitions:

Anonymity. To enable anonymity of a subject, there always has to be an appropriate set of subjects with potentially the same attributes. Anonymity is thus defined as *the state of being not identifiable within a set of subjects, the anonymity set.*

The *anonymity set* is the set of all possible subjects. With respect to acting entities, the anonymity set consists of the subjects who might cause an action. With respect to addressees, the anonymity set consists of the subjects who might be addressed. Both anonymity sets may be disjoint, be the same, or they may overlap. The anonymity sets may vary over time.

Unlinkablity. As there is no legal definition of unlinkability, yet, we only give a technological definition, taken from [ISO15408 1999]: "[Unlinkability] ensures that a user may make multiple uses of resources or services without others being able to link these uses together. [...] Unlinkability requires that users and/or subjects are unable to determine whether the same user caused certain specific operations in the system."

We may differentiate between "absolute unlinkability" (as in the given definition; i.e., "no determination of a link between uses") and "relative unlinkability" (i.e., "no change of knowledge about a link between uses"), where "relative unlinkability" could be defined as follows:

Unlinkability of two or more items of interest (IOIs, e.g., subjects, messages, events, actions, ...) means that within the system (comprising these and possibly other items), from the attackers perspective, these items of interest are no more and no less related after his observation than they are related concerning his a-priori knowledge.

This means that the probability of those items being related from the attackers perspective stays the same before (a-priori knowledge) and after the attackers observation (a-posteriori knowledge of the attacker). Roughly speaking, unlinkability of items means that the ability of the attacker to relate these items does not increase by observing the system.

Unobservability. In contrast to anonymity and unlinkability, where not the IOI, but only its relationship to IDs or other IOIs is protected, for unobservability, the IOIs are protected as such. *Unobservability is the state of items of interest (IOIs) being indistinguishable from any IOI (of the same type) at all.*

This means that messages are not discernible from e.g. random noise. As we had anonymity sets of subjects with respect to anonymity, we have unobservability sets of subjects with respect to unobservability. Sender unobservability then means that it is not noticeable whether any sender within the unobservability set sends. Recipient unobservability then means that it is not noticeable whether any recipient within the unobservability set receives. Relationship unobservability then means that it is not noticeable whether anything is sent out of a set of could-be senders to a set of could-be recipients. In other words, it is not noticeable whether within the relationship unobservability set of all possible sender-recipient-pairs, a message is exchanged in any relationship.

Pseudonymity. Pseudonyms are identifiers of subjects. We can generalize pseudonyms to be identifiers of sets of subjects. The subject which the pseudonym refers to is the holder of the pseudonym.

Being pseudonymous is the state of using a pseudonym as ID.

We assume that each pseudonym refers to exactly one holder, invariant over time, being not transferred to other subjects. Specific kinds of pseudonyms may extend this setting: A group pseudonym refers to a set of holders, i.e. it may refer to multiple holders; a transferable pseudonym can be transferred from one holder to another subject becoming its holder. Such a group pseudonym may induce an anonymity set: Using the information provided by the pseudonym only, an attacker cannot decide whether an action was performed by a specific person within the set.

Defining the process of preparing for the use of pseudonyms, e.g., by establishing certain rules how to identify holders of pseudonyms, leads to the more general notion of pseudonymity:

Pseudonymity is the use of pseudonyms as IDs.

An advantage of pseudonymity technologies is that accountability for misbehaviour can be enforced [CH02, CL01].

4.2.6.2 Reference to Use Cases.

The need for anonymity, pseudonymity and unlinkability can be clearly seen in the use cases presented in the previous chapter.

Certain inquiries are made to access public information. In these cases, there is no need to identify the users accessing the information. The maximum privacy protection is granted when the requests made by a user are anonymous and unlinkable to each other. In other cases, there is a need of maintaining a permanent identity for users in subsequent accesses. Users can be known to the server by secure pseudonyms, generated from a secret stored in the e-ID card, and to which attributes for access control can be linked. Pseudonyms maintained by the user with unrelated servers should be unlinkable to each other.

E-health applications deal with extremely sensitive data that, if linkable to the physical identities of patients, could pose a serious threat to privacy if the security of the databases is compromised. Moreover, these applications can be securely implemented using pseudonyms to identify patients. The substitution of identity data by pseudonyms lowers the privacy risks for patients and the liability of database managers. For example, the pharmacist of the use case presented in Sect. 3.1.6 needs to check that the prescription has been issued by a certified doctor, and that it was prescribed to the patient who intends to get it. Identity data is not needed to securely perform the transaction, and carries additional risks to patients' privacy if the security of the pharmacist's computer is compromised.

Unobservability requirements apply to scenarios in which the fact of observing activity leaks relevant information. For example, unobservable access could be required in a service where citizens can provide to law enforcement relevant information for criminal investigations. If the access is not unobservable, criminal organizations could monitor the activity at the server and determine if law enforcement is getting little or much information.

4.2.6.3 Technical Issues

Several Privacy Enhancing Technologies (PETs) have been developed to provide anonymity, pseudonymity, unlinkability and unobservability properties. We introduce here three PETs which are relevant to electronic ID applications. These technologies enable privacy-enhanced communication, identity management and database access.

Anonymous Communication Networks. Data communication networks use IP addresses to route information. Anyone who can listen to the communication lines sees the origin and destination of the information traveling in the network. As the IP address is a unique identifier which appears in all communication of a user, it enables linkability of all the user's transactions. If the IP address can be linked (even if only in one transaction) to a physical identity, the privacy of that user could be seriously compromised.

Anonymizing the communication layer is thus a necessary measure to protect the privacy of users. The implementation of anonymity mechanisms at the application layer may be rendered useless if transactions can be linked through IP addresses. Several technologies have been proposed to provide anonymous communication channels.

DC-nets [Cha88, WP90] and mix networks [DMS04, JAP, PPW91, RSG98] implement anonymous communication channels. The technique consists is having a large number of users who communicate through the system. The anonymous communication nodes perform certain operations on the data being transmitted such that the two ends of the communication are not easily linked. Unobservability of communication can be achieved in these networks by requiring communicating entities to constantly transmit traffic [PPW91].

There are also several proposals for anonymous communication networks based on peer-to-peer anonymizing network. Examples in the literature include systems such as Crowds [RR98], Tarzan [FM02], MorphMix [RP04], P^5 [SBS02], Cebolla [Bro02] or Herbivore [GRPS03].

In general, a mechanism to achieve some kind of anonymity appropriately combined with cover traffic yields the corresponding kind of unobservability. Cover traffic alone can be used to make the number and/or length of sent messages unobservable by everybody except for the recipients; respectively, it can be used to make the number and/or length of received messages unobservable by everybody except for the senders. Steganography and spread spectrum are other well-known unobservability mechanisms.

Pseudonymous Credentials. Pseudonymous credentials [CE87, Cha90, Bra99, Che95, LRSW99, CL01, CH02] are a privacy-enhanced alternative to public key certificates. Users are known by pseudonyms to the entities they interact with. The pseudonyms cannot be linked, but are formed in such a way that a user can prove to one entity a statement about his relationship with another. Such statement is called a credential.

Users are motivated not to share their identity by an *all or nothing* transferability mechanism. Users maintain a root secret in a secure, tamper-resistant storage device (such as the e-ID card). All pseudonyms of a user are generated using this root secret. Assuming that the e-ID card is used as a basis for a wide range of secure applications, a user sharing his root secret with somebody to use his health insurance would also give that person access to his bank account.

Pseudonymous credentials allow for optional recovery of their owners' identity. This mechanism can be implemented in applications where users may be held accountable for abusing the system for illegal purposes.

Private Information Retrieval and Private Filters. Private Information Retrieval (PIR) [CGKS95] schemes enable a user to access one or more servers that hold copies of a database and privately retrieve parts of the data stored in the database. The queries give each individual database no partial information (in the information theoretic or computational sense) on the identity of the item retrieved by the user.

Private filters [OS05] enable searching for documents under a secret criteria (such as presence or absence of a hidden combination of hidden keywords) under various cryptographic assumptions. The filter does neither learn the keywords provided by the user nor the documents that contain these keywords.

Privacy-Preserving Database matching. Privacy-Preserving Database Matching [FNP04, KM05, KS05] is a class of protocols that allow two or more parties holding private databases to compute the intersection of their databases without revealing any information beyond that. For instance, in the context electronic health-care, in order to detect instances of fraud, insurance companies, hospitals, and pharmacies do not have to share their patients' data (and possibly their corporate data with it) with each others, or with other parties. Instead, they can use Privacy-Preserving Database Matching (PPDM) protocols to detect irregularities (e.g., multiple reimbursement claims for the same treatment, multiple fulfillment of the same prescription...). Similar uses of PPDM protocols can be thought of in the context of homeland security, tax evasion, and welfare fraud investigations. There are few other variants of PPDM protocols. For instance, instead of having the parties learn the content of their databases intersection, at the end of the execution, we may have them only learn the size of the intersection, or the answer to the question of whether the size of the intersection is greater than a certain threshold. In the case where one of the databases is a singleton, the problem reduces to a membership proof. This private membership proof problem is also referred to sometimes as the blacklisting or whitelisting problem.

Public key encryption with keyword search. Public key encryption with keyword search [SWP00, BCOP04] is an encryption primitive that allows a party B to perform ”specific” keyword search operations on data that has been encrypted using a party A's public key. To enable this, party A has to give party B a ”specific” trapdoor information which will allow B to perform those specific search operations on A's encrypted data. Party B should not be able to learn anything else about the content of A's encrypted data, or to search for keywords other than those explicitly allowed by A's trapdoor information. This could be useful in the context of credentials, because if we can find a way to make a user provably show that his encrypted credential data is correctly formed, then the user only needs to provide a trapdoor information to the verifier (party B) for a term or a research pattern of interest. The verifier uses that trapdoor information to scan the encrypted data for the keyword or pattern in question. Depending on the application's context, a match may mean that the user is on whitelist (or on a blacklist) and is therefore (not) allowed to gain access to a service.

4.2.6.4 Legal Issues

The data protection act [4] applies to pseudonymous data. Unlinkability and unobservability are technological means to limit the amount of data processing occurring and the risks of data leakage or harvesting (unauthorized processing of data).

[4] Act of 8 December 1992, *Belgian State Gazette*, 18 March 1993

The e-ID contains the citizen's National Registry Number. This unique identifier could be abused by otherwise unconnected data controllers to effectively combine the personal data they own separately. Use of the National Registry Number is regulated by law, as is processing of personal data to create profiles. Such abuse by data controllers is easy to do, but hard to detect, therefore the risk is non-negligible. Databases which contain citizen certificates in some way may become attractive targets for hackers. Insofar as this risk is foreseeable, data controllers must invest in sufficient security measures to prevent unauthorized access. Data controllers are liable for the confidentiality of the data in their possession.

The enforcement of contractual or legal rights through the court system is only possible if the parties involved can all be fully identified. Faced with this reality, the parties to an agreement can avail themselves of alternative dispute resolution mechanisms, if any exist that do not require full identification as well, or include a clause stipulating that each party will give his identity into escrow.

Service providers that issue pseudonymous credentials to users may have an interest in also providing an identity escrow service. Where identity escrow is provided, law enforcement agents may attempt to take advantage of this to unveil the physical identity of the pseudonymous user. It should be researched firstly under which circumstances identity escrow must be provided and secondly under which circumstances the identity must be revealed. Notably the impact of the EU Directive on data retention must be examined

4.2.6.5 Deployment

Theoretical anonymous communication networks which resist powerful adversaries present feasibility problems, as the overhead imposed to protect the users identity renders the system unusable [Cha88, Dai96]. Two working implementations of real-time, by-directional anonymous communication networks are currently available [DMS04, JAP]. These low-latency networks protect the user against local adversaries (who do not have access to both the entry and the exit of the network). However, these systems are vulnerable to a series of traffic analysis attacks involving more powerful adversaries.

Protocols involving pseudonymous credentials are based on zero-knowledge proofs. These protocols involve computationally intensive computations that may introduce intolerable latencies for some transactions. The use of pseudonymous credentials instead of public key certificates would impose new requirements on the contents of the card and its capabilities.

Private information retrieval and private filters also involve complex operations and impose significant storage and communication overheads in order to achieve effective privacy protection.

In summary, there are a number of proposed privacy enhancing technologies which provide strong protection properties at a high cost. Current practical solutions offer an improvement of privacy protection towards weak adversaries. There are ahead many challenges to design robust practical systems for mass deployment that can be used in combination with the electronic identity card.

None of these technologies have been considered in the current version of the e-ID card.

4.3 Privacy and Data Protection Requirements

4.3.1 Belgian Law on privacy protection in relation to the processing of personal data (Act of 8 December 1992)

This law [5] (DPA) was modified by the law of 11 December 1998 implementing Directive 95/46/EC [6] and by the law of 26 February 2003. [7]

4.3.1.1 Processing of personal data

Personal data means any information relating to an identified or identifiable natural person. [8] The Royal Decree of 13 February 2001 implementing certain aspects of the Belgian Law on personal data protection [9] defines anonymous data as data which cannot be linked with an identified or identifiable person and consequently cannot be qualified as personal data. [10] Consequently, the rules on the processing of personal data are not applicable to anonymous data, as the latter are not or no longer considered as personal data. The Act does apply to pseudonymous data as well as the process of anonymizing personal data.

'Processing' shall mean any operation or set of operations that is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation, alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment, combination, as well as blocking, erasure or destruction of personal data. [11]

It is necessary to document whether an application processes personal data, the nature of these processes and the type of personal data involved.

[5] *Belgian State Gazette*, 18 March 1993

[6] *Belgian State Gazette*, 11 February 1999

[7] *Belgian State Gazette*, 26 June 2003

[8] Art. 1 §1 DPA

[9] *Belgian State Gazette*, 13 March 2001

[10] Art. 1, 5^o

[11] Art. 1 §2 DPA

4.3.1.2 Data controller

In the Belgian Law on privacy protection in relation to the processing of personal data (DPA) a data controller is defined as the natural or legal person, the factual association or public authority that alone or jointly with others determines the purposes and means of the processing of personal data. [12] The controller is the person with overall responsibility for the definition and implementation of processing. That is why the requirements that can be found in the law are in most cases addressed to him. Who exactly is the controller depends on the factual context. Therefore it will be very important to know who is determining the purposes and means of the processing of personal data. The e-ID card offers a range of opportunities to perform operations upon personal data. It will be important to determine who is in control of these operations. There will be several data controllers, so it is important to know who is responsible for which operation.

The data controller may not be confused with the processor. This is the natural or legal person, the factual association or public authority that processes personal data on behalf of the controller, except for the persons who, under the direct authority of the controller or processor, are authorized to process the data. [13]

4.3.1.3 Principles related to data quality

Art. 4 DPA lists several important principles relating to data quality.

Fair and lawful processing. Fair processing requires transparency. [14] [15] Transparency has to be guaranteed during each moment of the processing. The data subject must be made aware of the uses of data relating to him. In many cases, applications built upon the e-ID will necessitate transfer of personal data from one data controller to another. It is important to notice that these data flows must happen in a transparent way. The data subject has to be aware of what is happening with his personal data. Also it may be necessary to attach an acceptable use policy to transferred personal data.

Lawful processing requires compliance with all the national legal provisions

Finality. Personal data must be collected for specified, explicit and legitimate purposes and may not be further processed in a way incompatible with those purposes [16]. The purpose of the processing should thus be de-

[12] Art. 1 §4 DPA

[13] Art. 1 §5 DPA

[14] D. DE BOT, *Verwerking van persoonsgegevens*, Antwerpen, Kluwer, 2001,115

[15] Art. 4 §1, 1^o DPA

[16] Art. 4 §1, 2^o DPA

fined at the moment of the collection and the purposes of further processing should not be incompatible with the purposes initially defined. An initial purpose defined in very broad terms embraces a far wider range of secondary uses. [17] However, it may not be forgotten that the purpose must be sufficiently specified. For example when the e-ID card can be used to travel on public transport, subsequent use of the data coming from the card should, in principle, be limited to public transport applications.

Proportionality and data minimization. Personal data must be adequate, relevant and not excessive in relation to the purposes for which they are collected or further processed. [18] A legitimate and specified purpose does not in itself authorize use of any data. For each purpose specified, a sufficient connection must be established beyond doubt between the purpose and the data collected. [19] This embodiment of proportionality principle is also called data minimization as it requires that the least possible amount of data is processed about a data subject. Personal data should be disclosed on a need-to-know basis only. The idea of data minimization is reinforced by Art. 1 §4, 5^o DPA which adds that data should only be kept in a form that permits identification of data subject for no longer than is necessary for the purposes for which the data were collected or for which they are further processed.

In the context of ADAPID, data minimization requirement means that the e-ID card applications should always provide minimal amount of personal information about the card holder. For this reason pseudonym certificates should in principle be preferred above identity certificates. Technical tools should be available to contribute to the effective implementation of these requirements.

4.3.1.4 Criteria for making data processing legitimate

Personal data can only be processed in the following cases: [20]

- Unambiguous consent
- Necessity for the performance of a contract to which the data subject is/will be party
- Compliance with a legal obligation to which the controller is subject
- Protection of the vital interests of the data subject

[17] Cullen International, *A business guide to changes in European Data protection legislation*, The Hague, Kluwer Law International, 1999, 42

[18] Art. 1 §4, 3^o DPA

[19] CULLEN International, *o.c.*, 43

[20] Art. 5 DPA

- Pursuit of a task carried out in the public interest
- Processing necessary for the legitimate interest of the data controller provided that the interests or fundamental rights and freedoms of the data subject who has a claim to protection under the DPA, do not prevail.

Without any prejudice to other possibilities, the main guideline may be that within the e-ID concept it is most probable that private companies processing of personal data may be justified by consent of the data subject or by contractual relationships, whereas public agencies processing will be justified by legal requirements. In case of a medical emergency, the protection of the vital interests of the data subject will justify the data processing. [21]

The applicable grounds for legitimate data processing must be recorded in the appropriate way. For a number of applications it may suffice to mention this in the documentation. However, it may be necessary to record such information in much more detail, perhaps even on a per transaction basis.

4.3.1.5 Processing special categories of data

The articles 6, 7 and 8 of the DPA provide for particular guarantees concerning special categories of data. [22] Processing of certain data can by their very nature infringe fundamental rights or freedoms. The processing of such data is prohibited unless at least one of several specified exceptions applies. It is important to know that these data have to be treated differently. That is why it should be signaled when these special categories of data are processed in an appropriate way.

4.3.1.6 Transfer to non-EU countries

Transfer of personal data to countries outside of the EU is subject to specific rules. Because the regulation in the Belgian DPA is dependant on the European Directive for its application, these texts must be considered together. The Privacy directive only allows transfer if the third country in question ensures an adequate level of protection. The adequacy of the protection level of a country should be assessed by the Member States or by the European Commission. In order to permit the transfer of personal data from the European Union to third countries with a protection level that has not (yet) been assessed by the European Commission or by one of the Member

[21] Electronic identity white paper, version 1.0, June 2003, http://www.fineid.fi/vrk/fineid/files.nsf/files/2F38FAA842A30AE5C225703F00253DC/file/eID-WP-final-o.pdf

[22] Sensitive data, medical data and judicial data

States as being adequate, exporters of personal data have the possibility to include data protection rules into contracts with the recipients of the data in the third country. These contracts have to be made on the basis of models published by the European Commission.

Applications that transfer personal data to third countries must take these requirements into account. Filters may need to be developed to selectively block use of certain applications or transfer of personal data.

4.3.1.7 Confidentiality requirements

Art. 16 §3 DPA stipulates that any person acting under the authority of the controller or of the processor, as well as the processor himself having access to the personal data, may only process them on the instruction of the controller, except for the case of an obligation imposed by or by virtue of a law, decree or ordinance. The risks incurred by processing personal data are not only from external action by third parties, but equally from unauthorized use of or access to the data by persons acting under the control of the controller or the processor.

It is important that it is clearly defined who is responsible for the processing of the personal data and who is processing the data on behalf of the data controller. The risks associated with the multi-purpose e-ID applications have to be minimized. The data controller has to make sure that the necessary confidentiality agreements are in place. He will have to give detailed instructions. They need not, however, be given in writing except with regard to the processor. [23]

4.3.1.8 Security and organizational requirements

Art. 16 §4 DPA obliges the controller and the processor to take the appropriate organizational and technical measures that are necessary for the protection against accidental or unauthorized destruction, accidental loss, as well as against alteration of, access to and any other unauthorized processing of personal data. These measures shall ensure an appropriate level of security taking into account the state of the art in this field and the cost of implementing the measures on the one hand, and the nature of the data to be protected and the potential risks on the other hand.

In assessing the right level of technical security for e-ID applications it is necessary to assess all risks and the nature of personal data processed.

Taking into account the risks involved in the use of the e-ID it is necessary that the data involved is protected in an appropriate way.

[23] CULLEN International, *o.c.*, 77

4.3.1.9 Notification

Before carrying out any wholly or partly automatic processing operation or set of such operations intended to serve a single purpose or several related purposes the controller or, if such is the case, his representative, shall notify the Commission for the protection of privacy thereof. [24] The procedures for notifying the Commission are designed to ensure disclosure of the purposes and main features of any processing operation so as to enable the Commission to control compliance with the legal provisions. To avoid repetitive notifications when a controller operates a set of operations on personal data, he does not need to identify every one of them, providing that they all serve a single purpose or several related purposes.

4.3.1.10 Data subject rights

Generally, data controllers are required to give information to the data subjects whenever they process personal data, though a few exceptions exist. For each application it must be determined what information must be provided, at what time and in which form. It may be necessary to keep a record of how this requirement is fulfilled by the application at an appropriate level.

Other rights of the data subjects are: a right of access to personal data relating to him/her; a right to rectification of personal data that is shown to be inaccurate and the right to opt out of allowing their data to be used in certain circumstances (for example, for direct marketing purposes, without providing any specific reason). These requirements must be taken into account in the design of the e-ID applications.

Art. 6 §3 of the Act of 25 March 2003 [25] gives the bearer of the e-ID the possibility to access and correct the electronic data on the card and the data that can accessed via the card. He also has the right to access and correct the data in the local administration population register and in the National Register of Natural Persons. He can even see who, during the last six months, has accessed his data. [26] The use of the e-ID thus provides a way to increase the transparency of the data operation process. It is important that the e-ID really is used to increase transparency, increasing the consumers willingness for acceptance. The effect of these specific provisions on the design of public and private e-ID applications must be researched.

[24] Art. 17 DPA

[25] *Belgian State Gazette*, 28 March 2003

[26] except in the case of criminal investigation

4.3.1.11 Use of unique versus multiple identifiers

The use of a unique identifier has the advantage of assigning an identifier to an individual from birth to death, to ensure appropriate, accurate information exchange among the approved parties, prevent fraud and assure accurate linkage of information between different users. However, it also increases the risks involved, due to the ability of the identifier to act as a key to uncovering and linking a vast amount of information in order to create a complete personal profile. [27] That is why some scholars propose to use sector-based identifiers. The drawback is that accurate information exchange is made more difficult then. [28]

Belgium has de facto opted for a universal and unique personal identifier: the National Register Number. [29] This number is even placed four times on the e-ID. Use of this number is regulated by law: an authorization of the sectoral committee of the National Register is necessary. But of course it is still possible that this number is abused by otherwise unconnected data controllers to effectively combine the data they own separately.

Applications built upon the e-ID should where possible try to mitigate the risks of abuse.

4.3.1.12 Publicity given to a qualified certificate

A certificate means an electronic attestation which links signature verification data to a person and confirms the identity of that person.

A qualified certificate is a certificate which meets the requirements laid down in Annex I of the Act of 9 July 2001 [30] and is provided by a certification service provider who fulfils the requirements laid down in Annex II.

As mentioned above the data minimization principle requires that the least possible amount of data is processed about a data subject. This means that digital certificates should only be made public when this is absolutely necessary. [31] Annex II of the Act of 9 July 2001 stipulates that for qualified certificates this is only allowed when the certificate-holder's consent has been obtained. It is of course important that the receiver of a digital signature can verify that the certificate is still valid. That is why the certification service providers are obliged to make the revocation of a certificate public. [32]

[27] CULLEN International, *o.c.*, 79

[28] D. DE BOT, *Privacybescherming bij e-government in België*, Brugge, Vanden Broele, 2005, 61

[29] D. DE BOT, *Privacybescherming bij e-government in België*, Brugge, Vanden Broele, 2005, 69

[30] *Belgian State Gazette*, 29 September 2001

[31] J.A.G. VERMISSEN, *Sleutels van vertrouwen: TTP's, digitale cerificaten en privacy*, `http://www.cbpweb.nl/downloads_av/AV22.pdf`

[32] Art. 13 of the Act of 9 July 2001

4.3.1.13 Biometrics in e-ID cards

A wide and unrestricted use of biometrics raises concerns with regard to the protection of the privacy of individuals. Biometric data relates to the behavioral and physiological characteristics of an individual and may allow his or her unique identification.

Biometric data per definition is information relating to a natural person. In the context of biometrical identification, the person is generally identifiable, as the biometric data are used for identification or authentication/verification of the data subject. It follows that biometric data falls under the definition of personal data within the meaning of the DPA. Consequently, its processing must take place in accordance with the principles and procedures stipulated in the DPA.

4.3.2 Privacy and electronic communications

Directive 2002/58/EC [33] commonly referred to as the Directive on privacy and electronic communications particularizes and complements the principles of the general Directive 95/46/EC [34] into specific rules for the electronic communications sector. Its provisions apply to the processing of personal data in connection with the provision of publicly available electronic communications services in public communication networks in the Community. This directive has been implemented in Belgian law: in the Act of 11 March 2003 concerning certain judicial aspects of the information society services [35] and in the Electronic Communications Act of 13 June 2005. [36]

Because this directive could be relevant for some e-ID applications, we will have look at the most important requirements. Note that the technical aspects of these legal requirements are presented in Sect. 4.2.

4.3.2.1 Security

Pursuant to Article 114 of the Electronic Communications Act, providers of publicly available electronic communications services must take appropriate technical and organizational measures to safeguard security of their services, if necessary in conjunction with the providers of the public communications networks with respect to network security. Having regard to the state of the

[33] Directive 2002/58/EC of 12 July 2002, concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communication), O.J. L 201/37, 31 July 2002

[34] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, O.J. L 281, 23 November 1995

[35] *Belgian State Gazette*, 17 March 2003

[36] *Belgian State Gazette*, 20 June 2005

art and the cost of their implementation, these measures have to ensure a level of security appropriate to the risk presented. This provision extends the security obligation that was already included in the Data Protection Act. Security is no longer only legally required for the processing of personal data but also for electronic communications in the framework of publicly available services on public networks.

4.3.2.2 Confidentiality

The Directive further aims to protect the confidentiality of communications. Member States must through national legislation ensure the confidentiality of communications (and the relevant traffic data) by means of public communications network and publicly available electronic communication services. In particular, listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned and except when legally authorized to do so is prohibited. However, the Directive provides for an important exception from the principle: legal authorization for the monitoring of electronic communications is possible when it constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security, defense, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorized use of the communications system.

Belgium took the necessary measures in the articles 124 and 125 of Electronic Communications Act. A Royal Decree will determine the identifying, the tracking, localizing, listening, tapping and storage of electronic communication.

4.3.2.3 Data retention

Traffic data are the data that are processed for transmitting communication via an electronic communications network or for billing such a communication. Location data means any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service; Law enforcement authorities claim that traffic and location data are essential to effectively trace perpetrators of all types of crimes involving the use of communications networks, but also crimes that are not strictly related to, neither automatically associated with computer networks, including fraud, drug trafficking, human smuggling, blackmail, harassment, defamation and terrorism. Their claims have been taken into account and reflected in the provisions of directive 2002/58/EC. Its Article 15 authorizes Member States to retain data when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security, defense, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorized use of the electronic communication system. For those, quite broadly defined, purposes Member States may render the retention data mandatory for a limited period of time.

Recently, on 14 December 2005, the European Parliament adopted the Data Retention Directive [37]. The directive applies to providers of publicly available electronic communications services or of public communications networks. Traffic and location data are envisaged. It sets mandatory requirements for the collection, retention and retrieval of communication records. The following data have to be retained:

- data necessary to trace and identify the source of a communication
- data necessary to identify the destination of a communication
- data necessary to identify the time, date and duration of a communication
- data necessary to identify the type of communication
- data necessary to identify users' communication equipment or what purports to be their equipment
- data necessary to identify the location of mobile communication equipment

Note that only information about the transaction must be logged, not the content of it.

The data have to be retained for a minimum of 6 months and for a maximum of 24 months. The Member States have 18 months to implement the directive into national law.

In Belgium, Art. 126 of the Electronic Communications Act regulates data retention. The necessary Royal Decree still has not been published. A decision on this matter cab be expected with the implementation of the Data Retention Directive.

It should be researched under which circumstances and to what extent these rules apply to the e-ID applications considered in the ADAPID project.

4.4 Non Discrimination Requirements

The right of equality and non-discrimination is generally and internationally recognized. The right not to be discriminated is a basic right in a democratic society. The right is laid down in various national and international regulations. In the Belgian Constitution, the following articles can be found:

[37] The directive is not yet published in the Official Journal

Article 10: There are no class distinctions in the State. Belgians are equal before the law; they are the only ones eligible for civil and military service, but for the exceptions that could be made by law for special cases.

Article 11: Enjoyment of the rights and freedoms recognized for Belgians should be ensured without discrimination. To this end, laws and decrees guarantee notably the rights and freedoms of ideological and philosophical minorities.

In general the principle of equality and non-discrimination prescribes that equal situations should be treated equally and unequal situations should be treated unequally, if that would be necessary to enable everyone to enjoy his/her rights and freedoms without discrimination. [38] This principle however does not exclude certain categories of people to be treated distinctly, but only if the criterion for the distinction is objective and reasonable. This has to be judged from the viewpoint of the goal and consequences of the proposed treatment. The principle of equality is violated, if the distinct treatment is not reasonably proportional to the goal. [39] The Court of Arbitration says that the principle is also violated when certain categories of people, who are in a substantial unequal situation vis--vis the contested measure, are treated equally, unless there is a reasonable justification for it. [40] The prohibition to discriminate implies prohibition to unreasonably limit the rights and freedoms of a category of persons than those rights and freedoms of other categories. The principle of equality implies an obligation to take certain positive actions to ensure an equal treatment. [41]

When developing applications for the e-ID card, this principle will have to be taken into account. Every citizen should have equal access to the facilities enabling all the applications of the e-ID card. It is clear that not every citizen is familiarized with using an e-ID card. People in a difficult social position may not become more isolated, when the e-ID is used for many applications. Thats why the card has to be user friendly. In a case of 16 June 2004 the Court of Arbitration made it clear that it has no problem that the government makes more and more use of Information technology, but it has to take positive actions to ensure equal treatment. [42]

[38] Cybervote, Report on electronic democracy projects, legal issues of internet voting and users (i.e., voters and authorities representatives) requirements analysis, `http://www.eucybervote.org/KUL-WP2-D4V2-v1.0.pdf`

[39] Court of Arbitration nr. 37/97, 8 July 1997, *Belgian State Gazette* 16 July 1997

[40] Court of Arbitration nr. 1/94, 13 January 1994, *Belgian State Gazette*, 1 February 1994

[41] Cybervote, Report on electronic democracy projects, legal issues of internet voting and users (i.e., voters and authorities representatives) requirements analysis, `http://www.eucybervote.org/KUL-WP2-D4V2-v1.0.pdf`

[42] Court of Arbitration nr. 106/2004, 16 June 2004, *Belgian State Gazette* 2 July 2004

The government has to be aware that there is a digital gap . Also in other applications than e-government it will be necessary to respect the principle of non-discrimination. Although the principle of non-discrimination incorporated in the Belgian Constitution does not apply between individuals, the anti-discrimination Act of 25 February 2003 protects everyone against discriminating behavior from other individuals. [43]

4.5 Electronic Signature Requirements

4.5.1 Definitions

Electronic Signature means data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication.

An **Advanced Electronic Signature** means an electronic signature which meets the following requirements:

- it is uniquely linked to the signatory;
- it is capable of identifying the signatory;
- it is created using means that the signatory can maintain under his sole control; and
- it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable.

In this report, the electronic signatures considered with respect to the e-ID are advanced electronic signatures.

4.5.2 Reference to use cases

Electronic signatures are used in the use cases presented in Chapter 3. In the case of E-Health services, the doctor electronically signs the prescriptions issued to patients. When the public administration issues a document to a citizen (e.g., a passport), this is electronically signed by the public authority. The long-term storage of documents in trusted archives often relies on electronic signatures in order to protect the integrity of the document. Finally, e-business and electronic commerce operations require electronic signatures in order to build the necessary trust to carry on financial transactions.

[43] H. DEKEYSER, noot onder Arbitragehof 16 juni 2004, Computerrecht, 2004, 294

4.5.3 Technical issues

The security properties that can be achieved through the use of electronic signatures (such as integrity protection, non-repudiation, authentication, etc.) are discussed in Sect. 4.2.

Electronic signatures based on public key cryptography fulfill the requirements to qualify as advanced electronic signatures. The e-ID uses for producing electronic signatures one of the most popular electronic signature algorithms, RSA [RSA78]. RSA relies on the hard problem of factorizing large numbers.

4.5.4 Legal issues

The digital signature technology provided by the e-ID serves two distinct purposes. One key-pair is used as an authentication tool, to ensure that only authorized persons gain access to certain information or services. The second key-pair is intended as a tool for the creation of signatures in the legal sense of the word.

Both uses of the e-ID stand to be scrutinized from an evidence law point of view. This is fairly obvious where the e-ID is used to sign contracts, administrative forms and other legal documents. But even when the e-ID is merely used for authentication, log files may in certain situations be produced as evidence in court proceedings.

The evidentiary value of digital signatures is relatively uncomplicated in the short term, but raises a number of difficult issues when considered from a long-term perspective. A great number of documents must be preserved for decades, some even indefinitely.

The general rule of evidence law is that all evidence is admissible in court, however the judge is free to assign it the legal value he sees fit. Thus, the party presenting the evidence must convince the judge of its reliability. Somehow, the judge must be persuaded to trust the authenticity and the accuracy of the evidence placed before him.

There are numerous exceptions to this rule, most notably in the domain of civil law. In these cases a so-called regulated evidence regime applies, only evidence that conforms to legally defined criteria is admissible in court. Usually, the law also defines what minimal legal value should be accorded to such evidence. The model regulated evidence regime is the one applicable to civil contracts. For contracts with a value over 375 EUR either a notarial deed or a private written document signed by all the parties is required. Notarial deeds cannot as of yet be created in electronic form and will not be considered any further. The law further differentiates between an original and a copy of the private agreement, only the former is admissible in court in principle. The distinction between 'original' and 'copy' is particularly ill-suited to the digital environment. Firstly, it is difficult to identify an 'original', since a digital document has various modes of existence. One mode is the bitstream, which is not human-readable, the other is its representation on a screen, which is ephemeral. Secondly, a digital original is not necessarily more reliable than a copy, especially if the latter is entrusted to a TAS while the former is not. Finally, the notion of 'original' appears not to be technologically neutral, since it is closely tied to the specific digital signature technology used upon creation. The law is written upon the flawed assumption that a digital signature will suffice to preserve the integrity of the signed document indefinitely. In light of these issues, the precise role of the originality requirement must be examined to fully understand current legal policy on digital evidence.

Though ensuring compliance of e-ID applications with applicable law is of great importance, it is of equal importance to analyze whether current law is appropriate to allow for the development of advanced applications for the e-ID. The solutions and strategies for reliable preservation developed within the ADAPID project will serve as crucial input for this analysis. Clearly, the legal framework must take into account the various technological and organizational aspects of preservation.

4.5.5 Deployment

The current e-ID contains two private keys to generate electronic signatures: one is used for authentication, while the other is used to electronically (and legally) sign documents.

The electronic signatures produced by the current e-ID meet the requirements of advanced electronic signatures.

4.6 Trusted Archiving Requirements

4.6.1 Long-term archiving: object and aim

Before going into the functions to be fulfilled by a digital archive, it must be clear what is the object of preservation. In archival science the term (archival) record is generally used to denote the archive's contents. A record is any document made or received and set aside in the course of a practical activity. A record is digital when it is capable of being processed by a computer. [44] A record is not the same as a digital object or computer file. One record may be represented by one digital object or by many digital objects. Conversely, many records may be represented by a single digital object.

[44] Authenticity Task Force Report in X. (ed.), *The Long-term Preservation of Authentic Electronic Records: Findings of the InterPARES project I*, InterPARES, 2001, p. 1

Archiving is often equated to storage, although the former has a broader objective than the latter. Storage is the practical activity of keeping data in an unchanged status for a period of time. The aim of archiving is to preserve records in an authentic way by managing them on an intellectual or conceptual level.

An authentic record is a record that is exactly what it purports to be. Authenticity depends on the integrity and the identity of the record. A records identity is based upon its origin and its context. [45] An example from the real world may serve to clarify this concept. Imagine a museum exhibit about money organized in fifty years, by which time paper money will surely have completely disappeared. The visitors of the exhibit may wonder whether all the objects on display are genuine or authentic. A first specimen appears to be a 100 bill, it possesses all the required formal characteristics, has not been tampered with and can be traced back to the National Bank of an EU member state. The first specimen is authentic money, based on its integrity, origin and context. A second specimen looks like a 100 bill, but upon close inspection it is shown to be a forgery, it cannot be traced back to a National Bank of an EU member state. The second specimen is not authentic money due to its origin. The specimen is an authentic example of a forgery and may be presented as such. The third specimen is a colorful set of bills with a nominal value of 1 up to 500. The only text on the bill is ”Monopoly (R)”. The third specimen is inauthentic if it is presented as legal currency, due to the context in which it was created and used. This does not change the fact that it is an authentic part of the game of Monopoly.

Integrity in this context does not necessarily refer to the integrity of the bitstream involved. Here, the integrity of the message conveyed by the digital record is considered.

Integrity means that the record is complete and unaltered. This does not mean that records may not experience any changes, but it does mean that records must be protected against tampering or corruption and that it's clearly defined which changes or annotations may occur after the creation or capture as record.

Thus, integrity does not mean that records must be identically the same as they were when created or received. The integrity of a record means that its function and finality has not been changed. Essential characteristics or components of a record may not be modified. Incidental characteristics or components on the other hand may be modified or may even be lost. This view is based on the premise that the original electronic records are doomed to disappear as a consequence of technological obsolescence and that changes and/or loss are therefore unavoidable. What we can preserve is the possibility of reconstruction, and preserve the records ’as close to the original

[45] Authenticity Task Force Report in X. (ed.), *The Long-term Preservation of Authentic Electronic Records: Findings of the InterPARES project I*, InterPARES, 2001, p. 1

as possible.' [46]

The same intellectual content can be represented by a variety of digital objects (Word document, Tiff, PDF, XML, etc.). All of these may represent the same record in an integral way. Making the leap from bit integrity to record integrity is not self-evident. Modifications in the bitstream may or may not entail a significant change in the contents of the record. If the money owed in a contract is changed from 100 to 1000 per item, the integrity of the contractual terms are clearly compromised. If one pixel in a photograph changes from one shade of gray to another, this is probably not at all relevant for the message conveyed. Ensuring the bit integrity of a file loses relevance when the document is no longer readable due to technological obsolescence. Noteworthy is also that bit integrity checking does not in itself actively protect integrity, it only signals if the integrity of the bitstream has been compromised. Most technologies don't indicate what changes have occurred.

Record identity is at the heart of archiving. [47] The design of applications must take into consideration the appropriate way to record the identity of the digital records it produces (if any), more specifically the originating entity or entities and reliable identification of the work process from which the record stems. While the e-ID may suffice to identify the originator of a record it does not serve to identify other contextual information on its own. Generally, such contextual information is recorded in meta-data. The identity of the record need not be universally understandable, it suffices when the intended user group is able to evaluate the authenticity of the records correctly. As time goes by, the intended user group may change, requiring more contextual information to be added. For instance, governmental records may be more or less self-explanatory while they are still in current use by the administration that created them. When reorganizations occur, a description of the original situation may need to be appended to these records in order to clarify their status and meaning. Historians consulting the same records in the public archives may need even more descriptive information for these records to make sense. Any archival service, whether internal or external must be flexible enough to meet these demands.

Providing means to overcome technological obsolescence is an essential function to be provided by any digital archive. [48] Obsolescence may strike

[46] See Boudrez, Filip, Digital signatures and electronic records, Expertisecentrum DAVID vzw, Antwerpen, 2005, `www.edavid.be`

[47] GARETT, JOHN AND WATERS, DONALD (ed.), Preserving Digital Information Report of the Task Force on Archiving of Digital Information, Commission on Preservation and Access and RLG, 1996, p. 23

[48] GARETT, JOHN AND WATERS, DONALD (ed.), Preserving Digital Information Report of the Task Force on Archiving of Digital Information, Commission on Preservation and Access and RLG, 1996, p. 8

any element of the operational environment required to ensure continued access to digital records.

4.6.2 Data Storage

4.6.2.1 Definition

The user must be able to store data on the TAS. Data that is written to the TAS must be protected immediately. This means that any subsequent hardware or software failure must never result in losing the freshly written data.

4.6.2.2 Technical Aspects

The throughput performance of writing data to an archival system is critical. Streaming performance (Megabytes per second) is typically most important for large objects. On the other hand, the number of objects per second is the most important throughput metric for small objects.

Latency is also important for writing data. If one has a single-process or single-threaded application writing to a TAS with high latency, then the total throughput and the system responsiveness will suffer.

Care must be taken to ensure that the system performance doesn't degrade, as more objects or Gigabytes are stored on the archive. It is a common phenomenon that filesystem or database performance drops dramatically once the internal index pages no longer fit in main memory, or once the disk is completely full. The archive must be designed such that filesystems are automatically de-fragmented when necessary, and such that locality is ensured in all the indices (e.g., write to the same directory, or to the same volume on a disk, or write sequential filenames, etc.).

Data integrity is also key. We need to protect both the integrity of the network communication, and the integrity of the persisted bits and bytes. An end to end integrity check is powerful. The client can use this as a way to ensure that the TAS didn't alter the data.

Storing data on the archive is only possible if there is enough free capacity. The system should monitor the used capacity and possibly quotas per user or per user group must be established. A charge-back system, where the user pays for the real capacity he uses, instead of paying for capacity upfront, might be deployed.

Strict access control might be required.

4.6.3 Data Retrieval

4.6.3.1 Definition

The user must be able to retrieve data from the TAS. Ideally a ubiquitous access model is built into the TAS. Multiple client devices speaking multiple access protocols can connect to the TAS. The higher the level of accessibility, the higher the value of the TAS.

4.6.3.2 Technical Aspects

The throughput performance of retrieving data from an archival system is critical. Streaming performance (Megabytes per second) is typically most important for large objects. On the other hand, the number of objects per second is the most important throughput metric for small objects.

Latency is very important for retrieving data, even more than for storing data. An archive exhibits human real-time retrieval latency if it provides sub-second response. This level of responsiveness and interactivity is required for certain mission critical applications (e.g., consulting financial information of a company before reacting on a market change and placing an order).

For other users, batched retrieval or asynchronous retrieval with callbacks might be a better access pattern.

Again, care must be taken that the system performance doesn't degrade as the system gets bigger or fuller. A large system without hierarchical indexing can result in data retrieval throughput bottlenecks (objects per second). On the other hand a large system with hierarchical indexing can result in larger latency.

During the data retrieval phase, data integrity checks of the network transport are mandatory. Ideally, end-to-end integrity checks might as well be implemented. For example, the client could keep a precalculated integrity check (a CRC or a cryptographic hash) to be verified when the data stream is retrieved.

Finally strict access control on the data retrieval is required. Both functional access control as bandwidth usage quota might be implemented.

4.6.4 Disaster Recovery

4.6.4.1 Definition

Disaster recovery is the ability of a system to survive large-scale disasters. Examples are earthquakes, fires, terrorism, demolition of an entire system and other havoc. Metrics are the percentage of data restored after the disaster (ideally 100%), and the downtime of the global system.

4.6.4.2 Technical Aspects

The first way to implement disaster recovery is through Backup and Restore. This way, the system can be restored to a previously known valid state. All new data or data modified after the last backup time, is lost. Also, restoring the data can take multiple hours to days. Of course the backup information carriers (e.g., tapes) should be stored on a physically different location from the primary site. If data is encrypted, one should make sure that the decryption keys are not destroyed.

The next way to implement disaster recovery is through asynchronous replication. Essentially there are two systems concurrently up and running, geographically apart from each other. The systems replicate data to each other, with some delay. This way the information lost after a disaster is kept to a minimum (not zero). The downtime is zero, since the replica site can immediately take over.

The best but most expensive way to implement disaster recovery is through synchronous replication. Here the data is updated on both replica sites, before it is acknowledged to the client. This might add extra latency to the client request, but it gives the maximal level of recoverability: no data lost, no downtime. For example, during the 9/11 attacks, many EMC systems were completely destroyed. However, this did not result in perceivable downtime for the customers, since replica sites took over the functionality immediately.

4.6.5 Data Retention

4.6.5.1 Definition

Data retention is the capability of the TAS to enforce retention policies, which forbids users and system administrators to delete data that is under retention.

4.6.5.2 Deployment

Examples are fixed retention periods based on legislation or regulatory requirements. For example, emails have to be retained for 7 years, accounting statements for 10 years.

Another example is Event-Based retention. This policy can for example enforce that data is retained for X years after a certain event is triggered. Triggering the event happens at an undefined point in the future. For example, medical images have to be retained up to 10 years after the patient's decease.

A third type of retention is the litigation hold. For example, if certain data is the subject of a legal procedure, the judge might decide to put data under litigation hold. A privileged user has to perform this operation. Data under litigation hold cannot be deleted, regardless of its retention period.

Finally, when data comes out of retention, the data expires and is ready to be deleted in order to free capacity, or get rid of the data.

4.6.6 Compliant deployment of Trusted Archival Service

4.6.6.1 Definition

An archival system and its deployment procedures are considered compliant if they have the ability to comply with legal and regulatory standards with regard to data retention.

Examples of such regulations are Sarbanes Oxley, Basel II, etc.

4.6.6.2 Deployment

Roles of the administrators and the users, procedures around physical access to the trusted archive, communication and security of the network are all part of this. The system by itself cannot provide full compliance unless the correct procedures are enforced by the various stakeholders.

This is very related to computer and network security in general.

4.6.7 Data Removal and Data Expiration

4.6.7.1 Definition

Data removal is getting rid of data.

Data expiration is the process where data comes out of its retention period; e.g., a company has stored an email for 7 years. After the data has expired, the system should get remove this data as quickly as possible.

4.6.7.2 Technical Aspects

Data removal has two major goals.

The first goal is to reclaim the capacity taken by data that is no longer needed. This allows to suppress the storage cost. Not all systems are capable to reclaim capacity; e.g., optical non-rewritable media cannot reclaim capacity.

The second goal is to physically get rid of the data and make sure that the data is impossible to recover. This is required for certain compliance regulations. This is called shredding. The paper analog is putting a sheet of paper in the shredder. Optical media might be destroyed in a similar way. Hard disks can be magnetically shredded. The proposal by Gutmann in `http://www.cs.auckland.ac.nz/~pgut001/pubs/secure_del.html` is way too expensive to deploy in a real life system. We should find a cheaper way; e.g., crypto-shredding (encrypt all data, and shred only the key). The level of shredding depends on the level of compliance required.

4.6.8 Trusted Archive Security Requirements

This section contains details specifically for TAS. Please refer to Sect. 4.2 for a full description of the security requirements.

4.6.8.1 Confidentiality

The TAS needs to ensure that a cleaning lady stealing a disk does not result in a confidentiality breach. Therefore, data needs to be encrypted on the disk. Example `http://www.seagate.com/cda/newsinfo/newsroom/releases/article/0,,2732,00.html` full disk encryption by SeaGate.

The management of the decryption keys is a huge challenge, especially at the scale of millions of users and billions of documents.

Finally, escrow services might be required.

4.6.8.2 Integrity

The TAS system must ensure data integrity for its entire lifetime.

- Ensure that unauthorized data is not removed/added to TAS
- Ensure that existing data is not modified.
- How can a user 10 years from now be certain that the retrieved data (stored today) is integer? Usage of hash functions might help (e.g., CAS), but how can we roll forward and upgrade to better hash functions as old ones get broken (e.g., MD5). Can we build forward integrity through "upgradeable" hash functions?

4.6.8.3 Authorization

The TAS system must grant access to documents only to clients who are authorized to retrieve the data. Also, the TAS system must forbid non-authorized users to store data.

The challenge is mainly to build a scalable authorization system. A per-object ACL (access control list) won't do the job if there are billions of objects, and millions of users.

Also, keeping authorization policies synchronized between replication sites is not trivial.

4.6.9 Longevity / Durability

4.6.9.1 Physical Longevity / Durability

Definition. **Physical Longevity** or **Physical Durability** is the ability of a physical information carrier to maintain its data and keep it available at an acceptable service level. All media suffer from degradation (paper, CD, DVD, disk, tape, microfilm) and have to be replaced at regular intervals.

Technical Aspects. The first challenge is to physically store the documents for many decades, yet keep them accessible in a user friendly way. Paper or parchment is surprisingly good at maintaining its data for many centuries. However, it is expensive and space-hungry to store, and it is not user friendly since it doesn't allow searching, remote consultation, or copying in a cheap way. Each consultation can degrade the state of the document.

Optical and Tape technologies are not up to the job either. Optical media survives not much more than 5 years. CDs and DVDs have to be rewritten very frequently in order to avoid losing data. Tape media require tape aerobics to keep the tape physically fit to be used, and to realign the magnetization once in a while. Tape has to be rewritten every few years.

Finally, both optical and tape media cannot be used in mission critical situations, since the latency to retrieve information is simply too big (minutes).

Online disk-based or solid-state memory based devices have the potential to solve the availability issue. However the disks or memory boards themselves are also vulnerable to ageing, and need to be replaced every so often. An active archive with permanent self-inspecting and self-healing seems required to solve the physical ageing of information carriers. Data needs to be proactively migrated away from the old hardware to newer hardware.

Regardless of the choice of medium, the TAS solution must introduce redundancy in its storage, such that errors at the physical layer can be solved by fetching a non-corrupt copy of the data somewhere else.

4.6.9.2 Technological Longevity / Durability

Definition. **Technological Longevity** or **Technological Durability** is the ability to keep the information available for the user of the archive, in light of technological evolutions, new formats of data, new physical data carriers, etc.

Technical Aspects. The main user interface of paper or parchment is the visual interpretation of the ink on the document. Looking at a sheet of paper, reading text or interpreting pictures is obviously a very instinctive and natural way for humans to retrieve previously stored information. Probably it is one of the oldest, next to speech.

When going digital, things change a lot. Will we be able to visualize the JPG or PNG format a few decades from now? What about a WordPerfect document. What about the PDF standard. What about active content interpretation (PDF and PostScript have this feature). What about HTML with broken links. How can we make sure that what is signed is really what is meant to be signed. Virtualization techniques (VMWare, Xen, etc.) might be the solution here.

Even if we have the WordPerfect software CD available, the question remains whether there will still be an operating system and hardware which can make this software 'happen'. Virtualization engines might help, but again they might not care about staying backwards compatible for multiple decades. Open standards for file formats are the best protection for the buyer.

The protocols for retrieving the information might be proprietary as well. Again open standards are the best protection for the buyer. For example, the POSIX filesystem API is an open standard which makes applications independent of the filesystem implementation. CIFS or NFS are a networked version of this. XAM (Extensible Access Method) is an open standard which is focused on location independent fixed content.

Apart from the formatting and visualization technology, and from the access protocols, there is also the technology used to build the archive. Over time, modern information carriers such as photography, film, microfilm, LP record, cassette, hard disk, diskette, mini-disk, tape, CD (+-RW), DVD (+-RW, dual, blue), storage arrays have appeared. However, the technology life cycle of these modern media is very short. Typically no more than a few years, at most a few decades. It is very expensive to find hardware which can deal with old carrier formats.

In general, technology obsolescence is a real risk that is taken into account by whoever purchases equipment. Especially for equipment serving the persistency layer (i.e., equipment managing long-term state) this choice is made very carefully.

Migration of data from one technology to another must be possible. Modern technologies such as content addressing can be used to avoid breaking the information linkage between various documents. For example, URLs or filesystem pathnames typically don't survive more than 10 years. The E: share becomes the G: share, etc. Content addressing solves this problem.

4.6.9.3 Business Longevity / Durability

Definition. **Business Longevity** or **Business Durability** is the ability of the TAS service to satisfy the service level in light of changing business environments. Business longevity is influenced both by a dependency on the vendor of the TAS archive solution, and by the availability of enough people with the necessary skills to operate and service the archive once it has become old technology.

Deployment. One cannot expect a vendor of hardware or software to stay in business ad infinitum. Nor can one expect that there will forever be technological consultants available which can help servicing old hardware, old software or old protocols.

Vendors will almost always sell a storage device containing pieces of proprietary technology. This ties the buyer to the vendor for the entire lifecycle of the data. That becomes a real problem if one wants to store the data for multiple decades since businesses typically don't plan much longer than 5 to 10 years.

Apart from purchasing new hardware or sparing broken parts, one needs support from to vendor or from the community to keep the box running. Note that this is less of an issue if there is enough critical mass. For example, today one can still find COBOL experts to service 40 year old banking systems. However, the common case is that technology becomes obsolete in less than one or two decades.

Purchasing from a big vendor which has been in business for a long time and has good prospects, is also a way for the buyer to protect himself.

Finally, not betting on the latest new technology is a good way to avoid getting obsolete technology. However, this makes the buyer lag behind on technological progress and possibly makes his business less competitive.

Open standards need to go hand in hand with migration tools which migrate data off one device to another, possibly from a different vendor.

4.6.9.4 Trust Longevity / Durability

Definition. **Trust Longevity** or **Trust Durability** is the property of the TAS solution to ensure long-term integrity and authenticity of digitally signed documents. The TAS is responsible for ensuring that documents that were digitally signed decades ago, cannot be tampered with and are guaranteed not to be fakes.

Technical Aspects. There are many challenges in storing digitally signed documents and preserving the authenticity of the document and the signature.

It does not make sense to validate a digital signature a long time after the signature has been placed. This is true for a variety of reasons. First of all, the certificates used to sign a document might expire, or might be revoked before their expiration time. Second, the hash function used and the encryption algorithm might be considered too weak some day. Finally, the trust chain might be broken at some point in time with an intermediate party in the chain considered unreliable.

We will pursue a solution along the following lines. We envision the Trusted Archival Service as an archive which screens the documents which are stored on the archive. The digital signature and the validation chain is verified briefly after the document is stored. For this the CRL is pushed from the instance issuing authentication tokens (e.g., e-ID cards), or an online OCSP service is consulted. Possibly, the TAS has to store which CRL was valid at which point in time, in order to complete the trust chain.

Once a document has made it into the TAS, it is considered as having a valid signature. Now the TAS signs all internal documents to provide the next step in the trust chain. The TAS can export its self-signed data to other systems. This allows for migration between different TAS systems, which can be used to expand the trust chain.

Every once in a while, the TAS system can re-sign (notarizes) all its data with the newest signature algorithms and keys. For this it is important that the TAS stores the data and the signature together in one system.

The TAS must be connected to a Trusted Clock Service in order to have an indisputable knowledge of the current time.

It has to be investigated how all this steps can be built into a real system with real deployment. The role of the company building and/or servicing the TAS must be clear and confined. That company should not have the possibility to alter data. The role of the company (or government) deploying the TAS must be clear and confined. The role of system administrators, information administrators, etc. must be well-defined. The problem of deploying a TAS is related to the problem of deploying PKI. Fortunately, the government has already taken care of the certificate issuance role and the providing of the trust chain for the individual citizens.

When encryption comes into play, the key management is very challenging, especially in light of the longevity requirements. Who will back up the decryption keys and how can they be used?

Finally, the TAS might have the opportunity to create 'authentic copies' of documents. Using principles borrowed from the Digital Rights world, the TAS can issue a document, sign it, make it valid for a specific amount of time, and allow or disallow certain activities such as printing, viewing on a PC, viewing on television, viewing on phone, copying, etc. The legal aspects of such an operation are to be explored.

4.6.9.5 Trusted Clock

Definition. A **Trusted Clock** is a clock which is accurate, secure and auditable.

Deployment. Business transactions, security controls, digital signatures, and system performance can only be trusted if they have time that is accurate, secure and auditable. When time stamps apply these three attributes to documents, transactions, or any other digital entities, they provide the following advantages over traditional computer clock based time stamps:

- Assurance that the time came from an official source
- Assurance that time has not been manipulated
- An evidentiary trail for auditing or non-repudiation

A Trusted Clock needs to be part of the TAS solution. Apart from synchronization between several geographically disjoint parts of the TAS, the trusted clock plays an essential role in ensuring long-term authenticity and integrity of digitally signed documents.

4.7 Enforcement and Accountability Requirements

4.7.1 Policies

This section describes the need for policies. Every system should have policies to be able to hold a person accountable. The next sections describe some extra requirements in order to make enforcement possible and to help making applications privacy-friendly.

4.7.1.1 Policy management

Description A very important aspect in enforcement and accountability is the use of policies. An entity can only be held accountable if there is some way to specify what he is allowed to do within a system. Therefore policies have to be defined.

Each policy should clearly define which actions are forbidden and what the consequences of misuse are. Policies should also contain rules to state what is allowed by law, where applicable. Different aspects should be taken in to account to achieve usable policies.

Next to stating which actions are allowed, it should also be possible to define the functionality of the services. That way a service provider has to deliver the promised functionality. If he fails to do this, he can be held accountable.

Levels of policies There are different levels of organizations who can define policies, so there are also different levels of policies. There should be for example *international policies*, defined by international organizations. These international policies can include international laws and regulations.

Second, governmental organizations can define *governmental policies.* Third, every particular system can have his own *internal system policy.*

The different levels can complement each other. Higher levels will have general rules which can be specified at lower levels. There may however be some constraints on lower-level policies. For example, when a government defines a policy which states that personal information cannot be sent to other countries, an internal policy has to follow this rule.

Different types of control measures Not every misuse should be punished the same way. Sometimes it will be sufficient to revoke some credentials of a user or have him pay a fine without revealing his identity. It should be desirable that users are only identified when no other measure is sufficient. Policies should clearly state what happens if abuse is detected.

User awareness It is important that users are aware of the policies which apply to a certain application. A service provider may want to have evidence that a certain person had seen the policy before using the service. In case of disputes the service provider can prove the user knew what was going to happen with his data. The evidence can for example be created by signing the policy.

Reference to use cases Policies are needed in almost every application. Users always should be informed about what happens with their information.

For example, trusted archival services can use policies. If every aspect (data retention, used shredding methods, ...) of the service is clearly defined in a policy, users will be ensured their data is handled correctly. If not, the archival service can be held accountable.

Technical aspects Two common privacy languages are P3P and EPAL. The platform for Privacy Preferences (P3P) [wwwb] standard provides an XML-based policy specification language to declare what kind of data is collected by a service and how this data will be used. P3P is intended for privacy promises to customers. It is able to express and match policies at the human user level.

The Enterprise Privacy Authorization Language (EPAL) [wwwa] is a formal language for writing enterprise privacy policies. It allows to govern data handling practices across IT applications and systems. It allows a fine-grained definition of privacy policies, including positive and negative rights, obligations, conditions, etc.

There must be a solution which finds *contradictions between policies* and checks whether a policy complies to every other relevant policy of an higher level.

Users should *be aware of policies* and this should be provable. This can for example be done by digitally signing the policy.

Policies should not be statically used. By using *policy negotiation mechanisms* it is possible to define in an interactive way the data to be released in order to get a certain level of services.

Legal aspects The content of the policy must conform with applicable legal regulations. Care must be taken to check that whenever data is processed in different countries, the policies are conform to the rules of all those countries.

The policy itself is evidence in the case of a dispute, therefore it must be ascertainable which policy was applicable at a certain point in time. Policy documents will need to be archived in a reliable way.

Deployment Data systems can be very complex. Policies must be enforced in every process. This, however, is a non trivial task.

It is not easy to hold an organization accountable for disclosing some information. Therefore, there is also need for trust management.

4.7.2 Enforcement

It is not possible to hold users or service providers accountable by only using some policies. Different aspects are needed to do this. From a legal point of view accountability has no meaning unless the party in question can be forced to assume liability for his actions. The aim of enforcement is thus to ensure that accountability is translated into liability where appropriate. This section gives more information on some properties which are required to make enforcement possible.

4.7.2.1 User identifiability

Description Persons should be able to act anonymously in a system. However when they abuse the system some way, they should be identifiable. To ensure the privacy of the users, only (a collaborating set of) trusted third parties can identify people. As stated in the first section, policies should describe the conditions under which a user may be identified.

Reference to use cases In every system where persons can be held accountable, it is needed to be able to identify them. For example, the possibility to identify a person is being used in the e-health use cases. A doctor remains anonymous to the system when submitting some health records. In case the doctor made some mistakes, the system must be able to identify the doctor.

Technical aspects Anonymous credentials (see anonymity requirements) have deanonymization properties. With the help of third parties it is possible to find out the identity of an anonymous user. Of course the deanonymizing process has to be handled carefully. How can a third party be sure some deanonymization conditions are met?

Somewhere in the system the user should have used his e-ID card to obtain some credentials. Showing the credential however should not point directly to the user's identity.

Legal aspects Identification of users must comply with data protection regulations. The legitimacy of any request to identify a user must be examined before proceeding to do so.

Deployment Trusted parties are needed which deal with the deanonymization of anonymous credentials and pseudonymous certificates. It is difficult to know which parties can be trusted to perform deanonymizations only when certain conditions are met. Untrusted organizations should not be allowed to do this.

4.7.2.2 Action linkability

Description To ensure anonymous operations, different actions of a user should not be linkable. In some cases however, it may be useful to link some of the actions. This way, it can be possible for example to find out information about how the abuse was performed.

Reference to use cases This requirement can for instance be used in the e-health use cases. Patients will go to the pharmacist to buy medicines. The use of some medicines, however, can lead to addictive behavior. If the government can link the actions of a patient, it is possible to detect abuse in order to take countermeasures.

Technical aspects Anonymous actions can easily be linked by using pseudonyms for every transaction.

Also, anonymous credentials (see anonymity requirements) have deanonymization properties. With the help of a trusted third party, actions can be linked. The trusted third party will only do this in case of abuse. That way anonymity is ensured. Note that deanonymization does not always reveal the identity of the user. When using *local deanonymization*, only a pseudonym of the user is revealed. In case of *global deanonymization*, his identity is revealed. By using local deanonymization, it is possible to take action against abuse, while maintaining privacy.

Legal aspects Where action data concerns identified or identifiable natural persons, compliance with data protection regulation is necessary.

4.7.2.3 Evidence

Description In case a dispute arises, the parties involved will need reliable evidence in order to enforce their rights. Every protocol must be engineered securely to ensure that every party can gather enough evidence. Only the necessary evidence should be kept to limit the amount of disk space required.

Policies must clearly state how long evidence must be saved. When some party cannot deliver certain evidence his chances to win a dispute are very small.

Reference to use cases The financial use case "contract negotiations over the public web" shows the need for evidence in financial transactions. When money is involved, people will want evidence which ensures not risking any losses. The e-health use cases, too, need this requirement. When a patient wants to accuse his doctor, there must be evidence that the doctor made some severe mistakes.

Technical aspects There are different aspects with respect to evidence. It would be a nice feature to be able to automatically find which evidence is strictly required for a certain application or protocol. Furthermore, it is necessary to store evidence on the right place. Of course adversaries may not be able to change evidence. Aspects like available disk space and the security of a system can influence the choice of where to store evidence. It should be possible to use escrow services to store evidence.

Legal aspects In certain contexts evidence must conform to certain formalities, for instance contain certain clauses or specific information. The applicable formalities are subject to change, therefore applications should be able to adapt to such legal modifications.

Evidence can only be assigned legal value if it is sufficiently reliable. The accuracy and authenticity of evidence are important qualities in this respect.

4.7.2.4 Data under litigation

Description In case a dispute arises about access to or ownership of data, the data under litigation may be sequestered. Likewise, data may be seized in the course of a criminal investigation. No party is allowed to delete the data during the litigation. The TAS has to enforce this, since the TAS needs to protect the interests of the patient, relatives, hospital, insurance company etc.

Reference to use cases Data litigation is especially used by trusted archival services. It is also very important for every use case where evidence is important such as the financial and the e-health use cases. If data can be put under litigation securely, organizations will be more willing to use the system.

Technical aspects It must be ensured that no data is deleted. Of course also the integrity of the data is very important. Both aspects are necessary in order to protect the interests of every party involved.

If data is stored on certain systems of an organization, the organization must still be able to use the rest of the system.

Legal aspects When so ordered by the court, the application provider must be able to sequester data under litigation himself or be able to transfer the data to service provider who can do this in his place. The application provider must be able to respond adequately to writs of seizures issued by enforcement agents.

Deployment In order to establish trust in the TAS system, probably only the government can own and deploy the TAS.

4.7.2.5 Non-repudiation

Description Non-repudiation is the concept of ensuring that an action cannot later be denied by one of the entities involved. Persons or organizations can only be held accountable when the non-repudiation property holds. When there is no proof, users will deny having done certain acts and it will be impossible to hold them accountable. The different aspects of non-repudiation are described in Sect. 4.2.

4.7.3 Other requirements

Next requirements help applications to be more usable and privacy-friendly.

4.7.3.1 Minimal monitoring

Description Although it should be possible to identify persons who abuse the system, it should not be possible to systematically monitor normal users. The system must maintain the anonymity as much as possible, while maintaining the possibility to hold users accountable for their actions.

Reference to use cases This requirement should hold in every system where anonymity is important. It mostly applies to inquiries and the e-health use cases. For example, when a patient goes to the pharmacy in order to obtain medicines, he may not want the government to monitor the medicines he buys. However, when the government suspects abuse, it must be possible to monitor the patient's behavior.

Technical aspects Every process of an application should reveal as little identifiable information as possible. An identity management system can monitor the release of information. Furthermore identifiable information should only be saved by a service provider when needed.

By making it time consuming or difficult to monitor the actions of users, monitoring can be minimized. This can for example be done by using several parties which have to collaborate to be able to link some actions.

Legal aspects Monitoring the activities of natural persons is subject to data protection regulation.

4.7.3.2 Ensuring correct transactions

Description When agreeing on privacy policies, every party commits himself to act according this policy. Service providers can only perform actions on data if this is allowed by the policy. Especially when providing identifiable information, users should be ensured transactions are performed the way they should. This way it is possible to have more trust in an application. Furthermore, when an organization has put much effort in techniques to handle information correctly, it is more difficult to be held accountable in case of mistakes.

There are two ways to ensure the correctness of transactions. A service can go through a procedure to get accredited. When actions of an accredited service are not performed correctly the accreditation organization can be held accountable. A more technical solution is the use of policy enforcement mechanisms.

Reference to use cases This requirement, again, can be used by a lot of applications.

Commercial applications (TAS) can use some accreditation procedure to gain trust of users. E-government and e-health applications, too, need accreditation techniques. When creating services used by an entire population, it is important that everyone can have trust in this service.

An example where policy enforcement mechanisms can be used to achieve more trust in the correct functionality of transactions is archival services. Users may want to provide information only if they are sure that the data will be removed after two months. If they know that certain policy enforcement mechanisms are used to treat the information correctly, they will be more willing to provide the information.

Technical aspects A accreditation proof signed by a trusted party can be used to ensure a user that the services of a provider are correct. Of course users must be sure that accreditation organizations are reliable parties. This, again, is a matter of trust.

There are no technologies which can make certain that policies are enforced in every situation. It is impossible to prevent every kind of abuse. Incorrect handling can however be reduced by technologies such as sticky policies or digital rights management (DRM).

Sticky policies are introduced in [KSW02]. When submitting information, the user consents to the applicable policy. The policy sticks with the information and remains enforced when the information is transferred to other systems.

DRM [KC04] is also a technology which can be used. Service providers get certain rights on user data. This way they can for example have the right to use certain data for two weeks.

Legal aspects In certain cases applications may be submitted to audits and/or accreditation by law, for instance as part of a public procurement procedure.

Deployment In practice, enforcement of privacy policies is very difficult. No technical solution can prevent disclosure of information. It is also very difficult to hold someone accountable for the release of information.

In complex, distributed applications it is very difficult to prove the correct usage of data. Accreditation organizations will not take full responsibility in case of errors.

4.8 Trust Requirements

4.8.1 Definition

A system or party is trusted when an expectation rests on it to behave in a determined way or achieve a determined result, and where the relying system or party acts on this assumption.

More generally, trust is a quality of a relationship between two or more entities, in which an entity assumes that another entity in the relationship will behave in a fashion agreed beforehand, and in which the first entity is willing to act on this assumption.

Whether or not to trust depends on a natural persons decision. It is possible, but not necessary, that several entities trust each other mutually in a certain context. Trust decisions of legal persons depend on the decisions made by the legal persons responsible natural persons. Trust may be limited to one or more specific functions, and may depend on the fulfilment of one or more requirements.

4.8.2 Reference to Use Cases

Trust is needed in every application. Service providers (and the services they are offering) need to be trustworthy in order to become successful.

If one entrusts certain documents to a trusted archival service provider with the view of archiving them, the service provider must act the way he is expected to act. This means that a lot of requirements need to be fulfilled. Only authorized persons should have access to the archived data and the integrity and the authenticity of the documents that are archived, has to be guaranteed.

In e-health applications it should be guaranteed that only authorized persons have access to the electronic health records. It is very important that the health records cannot be abused by anyone. Otherwise people wont trust these applications.

Taking into account the importance of e-government applications, it is necessary that persons trust these applications. This is only possible if the e-government services work in an appropriate way.

4.8.3 Technical issues

The goal of trust distribution schemes is to distribute the trust among several trusted entities, so that the trust on each single trustee is lower. In a secret sharing scheme we have a group of participants that all get a “share” of the secret we wish to distribute among these participants. The goal of the scheme is to give each participant a piece of the secret. The different pieces (or shares) are constructed in such a way that some subsets of the participants can reconstruct the secret and others cannot gain any information about it.

The most common secret sharing schemes are t out of n threshold schemes. In this case any subset of at least $t+1$ participants can combine their shares to obtain the secret while a coalition of t or less than t players have no information about it.

In Verifiable Secret Sharing Scheme (VSS) a dealer distributes a secret value among the players, where the dealer and/or some of the players may be cheating [CGMA85, BOGW88]. VSS guarantees:

- Privacy - if the dealer is honest then the curious players learn nothing about the secret;

- Correctness - after the secret is shared there exists a unique value that can be reconstructed by the players, and this value is equal to the shared secret, when the dealer is honest;

- Robustness - the shared secret can be reconstructed even if the corrupt players hand in incorrect shares.

In many situations, such as cryptographic master keys, data files, legal documents, etc., a secret value needs to be stored for a long time. In these situations an adversary may attack the locations one by one and eventually get the secret or destroy it. To prevent such an attack, proactive secret sharing schemes have been proposed. Proactive security refers to security and availability in the presence of a mobile adversary. The life time of the system is divided into time periods which are determined by the global clock. At the beginning of each time period the servers engage in an interactive update protocol. The update protocol will not reveal the value of the secret. At the end of the period the servers hold new shares of the same secret.

Secure multi-party computation (MPC) can be defined as follows: n players compute an agreed function of their inputs in a "secure" way, where "secure" means guaranteeing the correctness of the output as well as the privacy of the players' inputs, even when some players cheat. A key tool for secure MPC, is the verifiable secret sharing (VSS).

A threshold cryptosystem is a system with n participants where an honest majority can successfully decrypt a message or issue a signature, but where the security and functionality properties of the system are retained even as the adversary corrupts up to some threshold t players [DF89]. The threshold setting generalizes a cryptosystem in the sense that the operation (signing, decryption) is performed by a group of servers instead of just one. This setting is non-trivial because some minority of the servers may be malicious. Threshold cryptography yields implementation of one trusted party, under the assumption that the majority of some servers can be trusted. There are numerous solutions (schemes) proposed for threshold cryptosystems, such as:

- Group Signatures

- Group Encryption

- Group Key-Generation

4.8.4 Legal issues

Trust is necessary to build complex systems. Otherwise every individual would have to be completely self-sufficient, which is a contradictory with a networked information society.

There is no need to trust a system or party if it can only show a determined kind of behavior or produce a determined result by force of nature.

The law may intervene to decrease the need to trust. This is one justification for issuing regulations for the accreditation, operation and audit of trusted third parties. Accreditation and audit may also be organized privately, for instance by trade organizations. Technology may also be used to decrease the need to trust. Essentially, a TTP service decreases the need to trust the network as is.

The law may increase the willingness to trust, by providing protection in case things go wrong. A similar effect can be achieved through underwriting private insurance policies that cover performance of the trusted system or party.

Which level of trust will be successful in the market will depend on a cost-benefit analysis. Regular e-mail presents very few characteristics to make it a trustworthy means of communication, still it is enormously successful because it is cheap and convenient.

From the definition of trust given here, it follows that a clear picture of the expected behavior or result to be obtained is a crucial requirement. A complementary requirement is the a posteriori evaluation of the actual behavior or result in comparison with what was expected.

4.8.4.1 Expected behavior or result

Either the expected behavior or the expected result must be clearly specified in a policy. This policy may be specified by the trusted system or party itself, by the person or system intending to make use of it or by a third party.

The specification of the expected behavior or result does not necessarily depend on past experiences with the trusted system or party. 1 It is possible to place trust in a system one has not dealt with before.

A system of accreditation and audit may be useful to determine whether the trusted system's policies are sound. Possibly, legislation might even impose a priori accreditation before allowing operation to commence.

Where different trusted systems or parties build on each other, it must be clear what is expected of each of them. Also, there should be no contradictions or gaps, which would make the whole system untrustworthy.

4.8.4.2 Actual behavior or result

Once the trust relationship has (started to) run its course, issues of accountability and enforcement may rise. From a legal point of view a distinction must be made between contractual relationships and non-contractual relationships.

Generally both types of relationships will be present. Frequently, the service of a trusted system or party is used by someone who wants to convince third parties of the trustworthiness of the object of the service. The relationship between the subscriber to the service and the trusted system or party is contractual in nature, while the relationship between the third parties and the trusted system or party is of a non-contractual kind. Also, one trusted system may build on other trusted systems or be part of a distributed system, transparently to the end users. A subscriber may have a concluded a contract with the first trusted system, but not with the others. In the case of the e-ID there is no contractual relationship between the users of the system and the provider.

Accreditation and audit may be equally important to verify actual behavior or results of the trusted system or party, specifically when the evidence procured by the trusted system or party is used in a dispute with another party.

Two main situations may occur: the trusted system's or party's actual behavior or results conform with the expectations or they don't conform with it.

4.8.4.3 Conforming with expectations

The trusted party may have an interest to be able to prove that his behavior was indeed compliant, especially when evidence procured by it is used to convince third parties of its reliability. One important question is to know where the burden of proof lies.

4.8.4.4 Deviating from expectations

The trusting party or a third party may have an interest to be able to prove that the of the behavior or the result of the trusted party was not compliant. Again the question who carries the burden of proof is of great importance.

4.8.4.5 Variation over time

External factors may cause a system or party that was previously trusted to become untrusted. One issue is what the responsibility of any of the actors involved is to monitor such external factors and disclose them to the other interested parties. This is relevant in particular for the determination of accountability and enforcement.

To prevent the loss of trustworthiness, trusted systems may be adapted over time. The modification over time of the applicable policy must be recorded reliably, thus allowing all parties involved to know what they can expect at any specific point in time.

In some situations, modifications to the trusted system or party may be unacceptable to certain users. This fact may need to be reflected in appropriate contractual agreements or even in regulatory measures.

4.8.5 Deployment

In the current version of the eID does not provide tools to support distribution of trust. Implementation of trust distribution with the e-ID would require that the e-ID keeps the (shares of the) secrets. In addition, dynamic properties of card will be necessary - the e-ID holders should be able to store secrets (shares) on their cards.

4.9 Physical Requirements for e-ID Cards

4.9.1 Introduction

In this section we describe the evolutions in e-ID card technology. On the one hand, we describe the current path of smart card technologies, on the other hand, we describe all possible technologies that can be used to implement the card. We briefly indicate the advantages and disadvantages of each of those technologies, and show to which extent each of them qualify for the e-ID application.

The candidate technologies that we are considering are namely:

- RFIDs (Radio Frequency Identifiers)
- 2D-barcodes
- Smart-Cards
- Mag-Stripe cards

Before we start analyzing each of these technologies, we first mention the criteria on which we base our evaluation and, eventually, our decision to keep or dismiss any of those technologies. There is a variety of evaluation criteria available, but for the purpose of this report our main criteria will be based on the following questions:

- Physical Security/Privacy: how secure is the data stored on the card? Are there mechanisms for tamper-resistance? Are there solid mechanisms to authenticate and authorize readers to access the data? Are there ways to prevent a non-authorized reading of the data both directly from the card and during the transfer of data from the card to an authorized reader?
- Storage Space (and possibly Processing Power): Given the list of data items required by the law to be stored on the card, how much space/memory do we need to provide on the card?

4.9.2 General Comments

Before we make an overview in detail of the possible technologies for the e-ID application, we make some general comments on the subject. e-ID cards evolve more and more in the following three directions.

4.9.2.1 SIM cards are increasingly used as universal proof of identity

Due to communication advantages, most people dispose of at least on SIM card, or at least it should be very easy to get hold of one of them. Therefore, it is a very logical evolution that this SIM card, which can be seen as a smart card, and which is, in a lot of cases, a real PKI-enabled smart card, can be used as a proof of identity. We sum up some recent, and very successful, examples of the use of the SIM card as an identity proof:

- Finnish e-ID card. Finland has recently introduced the new identity card. This card can be a SIM card. In this case the user decides where to buy the SIM card, and the government furnishes the e-ID certificate that is loaded on the SIM card.

- GMAIL service from Google Inc. Here a GSM number is used as the only way for new admittance for the service. This implies that the Google company values the identity proof that is already associated with a normal SIM card, mostly because of telecom regulations in most countries.

- Other internet services. GSM is also used as a means of payment for different internet services. The SIM card number is used to identify the user that pays. An example is a day ticket for a newspaper website. Also in this case the natural identity proof of a mobile telephone number is valued.

In general, governments have two ways to legalise/streamline this evolution:

- They can choose to offer an extra certificate. This certificate can then be stored on a SIM card of the provider of choice.

- The government can make laws that tightly couple a person with the SIM card. An example of this can be the registration obligation when buying a prepaid SIM card.

Furthermore there are also some disadvantages to this approach.

- People are usually not aware that this kind of 'identification' has serious privacy issues. For example, tracking of persons is possible if the mobile phone is turned on.

- The telecom companies will have more power, because they provide the 'bearers' for the identity information. This disadvantage will however diminish if the market is more open competitive.

4.9.2.2 Biometric data is increasingly included in identity documents

This is mostly, but not only, due to the restrictions imposed by the USA on passports, which require biometric data to be inside in order to enter the country. An identity document with biometric data could potentially be used as a passport document. There is some dispute about biometrical data, but the general feeling is that it is an improvement if it is used for extra verification only. Some advantages are that it makes the authentication harder to pass; and it introduces the third safety level (something you have, something you know and now also something you are). Among the disadvantages we find: The only way of stealing an identity is stealing by means of stealing the real physical characteristics. (for example your finger). This introduces a physical risk to the person who is granted the access. Another disadvantage is that biometric data has with the current state of technology a very high error rate and is therefore only an improvement as an extra verification. Biometric authentication will because of this limited technological evolution, in general also present a lot of false denials.

4.9.2.3 Contactless cards are increasingly chosen

Contactless cards are cards that can be read by holding them within centimeters of a reader. These cards have clear advantages of duration and usage issues. An extra safety can be build in, like in the passport for the US, where the machine readable optical strip has to be scanned first before the contactless feature is usable. There are however security concerns about the resistance of this technologies towards attacks.

4.9.3 Card format and comparative technology description

In general, the card format is based on the ISO/IEC 7816 standard. This means that the card format and physical characteristics correspond to Bank Card ID1 type or the standard bank card in nowadays wallets. We can distinguish between two major categories: contact smart cards and contactless smart cards.

4.9.3.1 Contact Smart Cards

The card has to be inserted into an electrical reader and the circuits of the card and that of the reader have to be in physical (electrical contact) The described connections are the following: RST,GND,CLK,Vpp,Vcc,I/O.

4.9.3.2 Contactless Smart Cards

The card can be accessed when it is in close proximity to a reader. There is no electrical contact between the circuits of the card and the circuits of the reader. The card is accessed using short range electro-magnetic waves. These cards are build according to the ISO 14443 standard.

4.9.3.3 Optical/magnetic data storage

We want to note that for secure data storage, also optional equivalents can be considered. For example, 2D barcodes can store a lot of information (up to 5k) on a 2D barcode. Also, optical rewritable memory on the outside of the chip is an option. Next to the aspect that a 2D barcode is easy to produce, it can also be seen as an extra security check to ensure the data inside is correct.

4.9.3.4 2D-barcode

2D barcodes, just as their predecessors the uni-dimensional barcodes, are visible, printed codes that use a machine-readable alphabet. There is significant difference between uni-dimensional and 2D barcodes. Uni-dimensional codes usually represent only a serial number that should be used in connection with a database to retrieve relevant data. Whereas, 2D-barcodes carry themselves the data rather than just a database key. Barcodes can be read only from a close range using laser beams. Barcodes contain redundancy mechanisms to correctly restore the encoded information when damage occur in the print.

There is a variety of advantages and limitations to the barcode technology. The advantages are mainly 1) the low cost, and 2) the better security because of close range reading. The disadvantages are 1) the size limitation, that is, 2D barcodes require geometric space to store the data. As a result, for portable documents, such as ID cards, that are subject to a size constraint, 2D barcode technology may not be suitable unless we limit the data to be stored. For an accurate decision on the suitability of this technology, one has to compare the size of the actual data to be stored, to the maximal size of data the card is capable of carrying given a certain geometry. 2) The second disadvantage is the durability of the print. It happens often that cards get worn off after some time because of improper use or storage. One way to improve durability by using appropriate plastic coating for instance.

4.9.3.5 Magnetic Stripe Technology

Magnetic stripe cards are cards with a small stripe on their back (e.g., credit cards, airline tickets, etc.). The stripe is made up of tiny magnetic particles in a resin. These particles behave as small magnets with north and south poles. It is possible to change the polarity of the magnetic particles by exposing them to a magnetic field. A blank card is initialized by aligning all its particles in the same (horizontal north-south) direction. The result is a series of alternating north-south poles along the horizontal (longer) dimension of the card. If we flip the polarity of one the magnetic particles, we end up with a local north-north or a south-south. By convention a north-north is interpreted as a passage from bit 0 to 1 and a south-south is interpreted as the opposite. To encode a string of binary data, one only needs to flip the polarities of the magnetic particles at the right locations. To read the encoded data, one has to detect the changes in polarities and convert them into binary bits.

There are three main concerns with magnetic stripe cards:

- The easy reading of the data on the card: Anyone with a magnetic stripe reader that has access to the card can read its content. For that reason, sensitive information are never encoded directly on mag-stripe cards. Instead, only ID numbers are stored on the card that serve during authentication.

- Limited storage space: It is possible to store only textual data on magnetic stripe cards. This technology will not qualify if biometric data for instance is required.

- The easiness to duplicate/counterfeit the card: The inherent easiness to read, manufacture, and encode a magnetic stripe card, makes it also easy for fraudsters to duplicate cards and produce counterfeit ones. There are few technologies (e.g., Watermark Magnetics) available, however, that link individual properties (e.g., thickness, density, etc.) of the magnetic stripe, the card, and the data on it together, making any counterfeiting of the card very difficult.

4.9.3.6 RFID technology smart card

RFIDs (also know as RFID tags) are small devises that can be attached both to objects and living beings in the purpose of identifying them. RFID tags are equipped with antennas to receive and respond to radio-frequency queries from RFID readers. RFID tags can be queried from a distance and without a line of sight. We distinguish two main families of RFID tags:

- Passive tags, they carry no internal source of power, and function on current induced by the electro-magnetic field generated by the RFID reader at the time of query.

- Active tags, however, are equipped with their own internal power supply, and are therefore capable of more elaborate computations. Active tags could also be permanently sending signals to the outside world, the same way cell phones do to ensure a timely reception of calls.

Both, passive and active RFID tags, may contain a non-volatile memory to store data.

There are many advantages to RFIDs, the most important being 1) their relatively small size, 2) the possibility to remotely query them (and thus speed-up processes), and 3) their ability to autonomously send signals (for Active tags).

On the other hand, there are serious concerns with RFIDs, the most important of which is privacy related. RFIDs are, by design, an easy target for remote unauthorized querying, and as a result of that, when used on identification documents (e.g., e-ID, ePassport), RFIDs may jeopardize the privacy of the person who owns the ID document. There are ways to improve the security of RFIDs, but they are not 100% fool-proof and they come at an extra cost (computational and monetary).

One can find a more exact format specifications in the following documents:

- ISO/IEC 7816-1:1998 Integrated circuit(s) cards with contacts - 1. Physical characteristics
- ISO/IEC 7816-2:1999 Integrated circuit(s) cards with contacts - 2. Dimensions and location of the contacts

4.9.4 Electrical Requirements

The electrical requirements are described in detail in the following standards:

- Amd 1:2002 Electrical characteristics and class indication for integrated circuit(s) cards operating at 5V, 3V and 1.8V
- ISO/IEC 7816-10:1999 Integrated circuit(s) cards with contacts - 10. Electronic signals and answer to reset for synchronous cards
- ISO 14443 Integrated circuit(s) contactless cards standard

4.9.5 Memory Requirements

The memory requirements depend a lot on the architectural decision to include or not to include biometrical data on the card. Biometrical data requires more memory space than non biometrical data and PKI data.

Another possible requirement, which is not discussed here is the extensability. Extensablitity means the possibility to add extra data. This can be specific biometric data, but also data to allow the combination of different user cards, or different pseudonymous or anonymous credentials.

For the case of the non-biometrical card without extensions, we can compare best with the current Belgium e-ID card: ROM: 136kB EEPROM: 32kB RAM: 5kB.

For the case of a biometric card, additional storage space needs to be foreseen. Biometric systems either store the full biometric image, or a biometric template. Biometric templates are very small, and, according to Frost and Sullovan, range from 9 bytes for Hand geometry to 300-1200 bytes for a fingerprint scan to 512 bytes for iris recognition to 1500 bytes for voice verification. This means most smartcards have enough memory for storing the templates. If one wants to save the biometric image, extra memory is required. A possible solution here can come from flash chips.

4.9.6 Processing power

Also in the aspect of processing power, the decision to include biometrical data (and operations) can play a crucial role. The basic processing power decision will be to include a 16 bits processor or a 32 bits processor. In the case of biometrical data, handling of more data is required, and a 32 bits processor will be a definite advantage. An other processing power decision is the operating system that is on the card. If the card operations become more complex, also this operating system becomes more complex and more processing power is required. As a note can be seen that the complexity of the operating system does also affect other requirements, such as operation storage memory (ROM) and working memory (RAM).

4.9.7 Tamper Resistance Requirements

An important security measure for chips on contact or contactless cards is tamper-resistance. This implies the resistance against non-allowed data reading. For example, the private keys should remain absolutely secret and on the card only. We will discuss tamper-resistance, depending on the type of attack that will be carried out.

4.9.7.1 Tamper resistance against DPA (Differential Power Analysis) attacks

In these attacks, the power consumption of the chip is measured and coupled to the execution of cryptographic operations. This can lead to the detection of 'secrets', and eventually to the detection of a secret key.

Some technical countermeasures aim at reducing power leaks in the chip reduces the possibility of a successful DPA attack. Adding noise to the power consumption curve is also a good method to disguise the read power consumption of the chip. Randomizing the power consumption of the chip is an even better solution against this type of attack.

A solution on a different level is to introduce algorithms that remain safe, even if the chip leaks information (cryptographic countermeasures)

4.9.7.2 Tamper resistance against EMA (Electro-Magnetic Analysis) attacks

In this attack, the electro magnetic radiation from the chip is analyzed, and coupled to the execution of cryptographic operations at the same time. Out of this information, secrets can be deducted.

Electromagnetic countermeasures are aimed at generating random radiation to disguise the normal radiation. A simple solution is to add noise to the electro-magnetic radiation.

A basic counter-measure is to install an opaque passivation layer around the chip (shielding).

4.9.7.3 Tamper resistance against more exotic attacks

One example of such attacks is the 'frozen RAM scan' technique, where a scan of RAM that is very quickly frozen, and therefore retains some of its magnetic data, is performed. Countermeasures to this attack include RAM encryption (encryption of the RAM itself can be an effective measure); and location scattering of registers (when the registers are not physically in one place, it becomes very hard to deduct the information inside).

4.10 Quality of Service, Affordability and Usability Requirements

4.10.1 Performance

4.10.1.1 Definition

The performance of e-ID enabled applications is the speed perceived for the users of the application, or the speed perceived by the total application infrastructure.

4.10.1.2 Technical Aspects

First of all this involves latency; i.e., performance measured and perceived by an individual user. The number of round trips between terminal and card(s) is important. The number of interactions between client and server or archive must be minimized. The network latency must be minimized. The number of user interactions must be minimized. For example, we don't want to enter our PIN five times.

Secondly, throughput is important. This is performance measured from the server. How many transactions per second can be accepted or can be processed. A related number is the performance of a batched client; e.g., the bulk processing of e-ID cards.

4.10.2 Reliability and Availability

4.10.2.1 Definition

Reliability is an attribute of any system that consistently produces the same results, preferably meeting or exceeding its specifications. Specifically, with respect to a Trusted Archival Service, reliability is defined as the ability to ensure that data doesn't get lost. A typical metric for reliability is MTTDL (Mean Time Till Data Loss), typically expressed in millions of hours.

Availability is the degree to which a system suffers degradation or interruption in its service to the customer as a consequence of failures of one or more of its parts. Specifically, for a Trusted Archival Service, availability is the ability to keep the data accessible for the client at all times, at an acceptable performance level (throughput and latency). Apart from performance metrics, the MTTDU (Mean Time Till Data Unavailability) is used, typically expressed in millions of hours. A related metric is the MTTR (Mean Time Till Repair), which measures how fast the system can self-heal from a failure.

Availability is typically expressed in "number of nines" (e.g., 99.999%) availability indicates that the system suffers only 5.5 minutes downtime per year.

4.10.2.2 Technical Aspects

High availability is an essential part of the e-ID applications, and must be included in the design of the distributed infrastructure.

We need to investigate solutions to improve the MTTDL and MTTDU of the TAS. We will investigate techniques such as storage based on IDA (information dispersal algorithm).

4.10.3 Affordability

4.10.3.1 Definition

Affordability is the level at which the production and operational deployment of the e-ID card and its applications is cost effective for both the citizens, and the government.

4.10.3.2 Deployment

The e-ID applications should replace existing applications such as legal systems, traffic fines, medical prescriptions, proof of allergies, etc., with a more secure, more flexible and more cost effective solution.

Note that both the upfront investment cost must be taken into account (creating and distributing e-ID cards, creating an infrastructure, teaching the citizens how to use it, developing or purchasing the applications, etc.) as the operational recurring costs (running the applications on servers using electricity, floor space, cooling; software and hardware maintenance costs, etc.). This has to be compared to the current analog applications (e.g., paper archives which use a lot of floor space).

In an ideal environment, one can seamlessly scale up the required TAS storage capacity (in terms of Terabytes), and pay as you scale up.

4.10.4 Usability

4.10.4.1 Definition

The system usability is the effectiveness, efficiency, and satisfaction with which users can achieve tasks in a particular environment of a product. High usability means a system is: easy to learn and remember; efficient, visually pleasing and fun to use; and quick to recover from errors.

4.10.4.2 Deployment

Using an e-ID card should become trivial and intuitive. All layers of the population must be able to use the e-ID card without fear. It should not be difficult to deploy the e-ID card or its applications. The people should trust the e-ID card and its intuitive applications.

Usability at server side is less of an issue. We will assume the availability of technically skilled people.

4.10.5 Manageability

4.10.5.1 Definition

The system administrators must be able to manage and monitor the e-ID infrastructure and the TAS system. The challenge is to have few administrators with low technical knowledge being able to manage multiple petabytes of storage. Also, the monitoring must be smart and not throw too many false positive alerts.

4.10.5.2 Deployment

The system administrators must be able to manage and monitor the e-ID and TAS system. The challenge is to have few administrators with low technical knowledge being able to manage millions of e-ID cards and certificates, and multiple petabytes of storage. Also, the monitoring must be smart and not throw too many false positive alerts.

The vendor of the system have to service the system every once in a while. The cheapest serviceability model is full remote servicing of the system. However, that might not be possible in all circumstances (physical or legal reasons not to allow such interventions).

Another model is a grooming service model; i.e., the vendors comes and services the box every 6 months or so. Components fail, but the e-ID and TAS systems happily continue to run. Every 6 months broken parts are spared. This is a very cheap model as well.

The most expensive model is to call service every time something goes wrong. This is expensive both for the customer as for the vendor. The service call might be triggered automatically by SNMP, email or remote monitoring.

Transforming a system from FRU (Field Replaceable Units) to CRU (customer replaceable units) might drive down service costs tremendously. It means that a customer can replace broken parts himself without too much risk and complexity.

Ideally, servicing a box is a non-disruptive event. There must be limited system availability or performance loss during a service event such as hardware or software upgrade, or parts replacements.

4.10.6 Scalability

4.10.6.1 Definition

Scalability is a metric indicating how well a solution to some problem will work (both from a functional and a performance point of view) when the size of the problem increases by several orders of magnitude.

4.10.6.2 Technical Aspects

In every part of the architecture of the e-ID system and the TAS, we need to take into account scalability.

The size of the system, the number of e-ID cards and certificates, the number of e-ID readers, the amount of Terabytes raw capacity in the TAS, the number of individually managed objects, the number of concurrent clients, the total number of users, the granularity of access control, the size of an access control list per object, the speed at which the system can heal itself from a failure, the size of security policies, the geographic structure of the cluster, etc. These are all excellent examples of where scalability must be taken into account.

The TAS has to be able to store billions of individually managed objects. Think of ten million citizens which each store hundreds of digitally signed official documents. High Object count is an enormous challenge for archival systems.

The Certificate Revocation Service, the TAS and many other e-ID applications have to be able to let a large number of clients connect concurrently. It will not be uncommon to have thousands of clients concurrently connecting to the system.

4.11 Interoperability

4.11.1 Description

The mobility of people in Europe is increasing. Citizens will want to use their e-ID card to interact with service providers coming from different countries and operate from both home and abroad. In Belgium alone, issues of interoperability affect one million people, either because they work abroad or because they reside in Belgium but do not have the Belgian nationality. This reality makes interoperability an important requirement for the Belgian e-ID card.

4.11.2 Reference to use cases

Interoperability is needed in a lot of applications. It is important to notice that in Belgium there is an obligation to give an ID to all the persons legally established on the territory. This could mean that for e-government applications interoperability is less important. Persons that want to make use of these services, will often have a Belgian e-ID. For e-health applications this can be different. It is possible that a foreigner requests for medical help. It would be useful when these persons could make use of their e-ID card.

The e-ID card is currently used by lawyers for the electronic submission of conclusions in court cases. Sometimes foreign lawyers have to intervene in such a court case. They of course do not have a Belgian e-ID. To give these lawyers the possibility to submit their conclusions electronically, their e-ID cards should have to be accepted.

4.11.3 Technical aspects

In order to ensure interoperability, it is necessary that there is, to a certain extent, harmonization. For example, it is not necessary that all certificates contain the same information. However, minimum data content needs to be defined. [49] Service providers have to be able to trust eIDs that have been issued in other states. So it is necessary that in the other states suitable procedures for the issuance and management of the eIDs have been implemented. Only eIDs that fulfill these requirements must be able to make use of the different applications. Service providers also have to be able to verify whether any issued e-ID is indeed still valid at the time of attempted use. In addition, service providers must be able to notify an identity provider that an identity could be compromised. [50] As long as these requirements have not been fulfilled, the e-ID applications cannot be interoperable.

4.11.4 Legal aspects

It is unclear whether the current legal context contains barriers against interoperable use of e-ID cards, aside from any technical issues. The EU electronic signature directive does not regulate e-ID cards directly, but may have an impact as it regulates the activities of certification service providers.

Essential is that there is a common terminology. Before any sensible discussion can take place, it is necessary that there is a common definition of terms concerning e-ID. Agreement on terms like identity, authentication, entity, identification, has to be reached. Current definitions in Europe vary

[49] The e-signatures directive provides a working example in the requirements for qualified certificates contained in annex I

[50] Overview of identified difficulties in the creation of pan-European IDM systems, Modinis IDM, eGovernment Unit, DG Information Society, European Commission

widely, which makes it very difficult to achieve interoperability. A consensus on EU level is necessary.

With regard to all the legal requirements defined in this report, it must be noted that the various Member States may have different regulations in place, thus impacting the way the applications are to be designed. One notable example is the use of unique identifiers. The European Member states take greatly different approaches to the use of unique identifiers. Several legal frameworks forbid the obligatory assignment of unique identifiers to their citizens. Others, like Belgium, do issue a mandatory identifier to their citizens. Some countries issue different sectoral identifiers. For e-ID applications to be interoperable, they must be able to take into account such differences in policy.

4.11.5 Deployment issues

Obviously, the ADAPID project will in many instances be limited to incorporating the potential for interoperability in the design of e-ID applications. In order for this potential to become reality, agreements between the various providers of e-ID systems will no doubt be necessary. The difficulty generally does not lie in tying disparate technical systems together but in making effective information sharing possible.

Chapter 5

Conclusions

At the time of finalization of this report, approximately 2.5 million Belgian citizens possess a e-ID card. By 2009 the whole Belgian population should have an e-ID. What is more important, is that right now only 1% of the citizens use their e-ID online. The major reason for this is the lack of attractive applications making use of the e-ID. The aim of the ADAPID project is precisely to construct a framework for new and advanced e-ID applications.

The current version of the e-ID card is not designed to provide a high level of privacy protection. From this perspective, the e-ID in its current form is open to a number of criticisms.

Ensuring compliance of advanced e-ID applications with applicable law is of utmost importance. It is of course possible that, during the ADAPID project, it becomes clear that the current legal framework is not adequate to deal with the issues arising from the use of the e-ID card. In that case it will be vital that we give an indication of which changes are necessary. Requirements regarding privacy and data protection are of major importance. Making use of the e-ID should not reduce the personal privacy of the citizens. An electronic identity management system implies very strong privacy enforcing requirements in order to offer the necessary protection. Not only privacy is important, there are also other requirements. Services based on the e-ID should be sufficiently trusted, discrimination should be avoided and interoperability must be taken into account.

From a security point of view, the current Belgian e-ID contains two public key certificates for authentication and electronic signatures. The e-ID provides integrity protection and non-repudiation for signed documents. A session key is generated in order to encrypt information and preserve confidentiality. The current e-ID does not, however, provide public key encryption for confidentiality. This functionality may not be included as it raises serious issues in case of loss of the keys (as important information may not be retrieved if the e-ID used to decrypt it is lost or destroyed).

The public key certificates used for authentication and electronic signatures provide by default unique identifiers and leak personal data. The interactions with current e-ID cards are thus identifiable and provide full linkability of different actions, which contradicts the principle of data minimization. The privacy preserving properties of the current e-ID cards could be improved by enabling pseudonymous identity management mechanisms. Users would then be able to provide the minimal set of information that is required for securely carrying out the transactions. Using different identifiers when interacting with government or commercial organizations would reduce the potential of abuse of personal data.

An important aspect in enforcement and accountability is the use of policies. An entity can only be held accountable if there is some way to specify what he is allowed to do within a system. Users should be able to act anonymously in a system. It should not be possible to systematically monitor normal users. In case of abuse, however, it must be possible to identify them and link their actions. When a dispute arises, the parties involved need reliable evidence in order to enforce their rights.

We have compared the technologies that can be used for e-ID tokens. We have discussed RFID, 2D barcodes, smart cards and magnetic stripe cards, together with their advantages and disadvantages. The requirements for smart cards include processing, memory and security requirements. We have also discussed the impact of including biometric data on the cards.

We have recognized three main directions in which the identity card market is evolving: contactless readers, inclusion of biometric information and usage of legally backed SIM cards as a universal proof of identity.

The Trusted Archive or Trusted Archival Service distinguishes itself from a regular archive in a number of domains.

First of all there is the aspect of privacy and security. The TAS system is an essential component in the overall architecture of e-ID enabled applications. The TAS system must avoid to become the weakest link in terms of security and privacy. Therefore, we believe that the security must be embedded in the archive itself and aspects such as confidentiality, authorization and integrity are an essential part of the architecture.

Secondly, the TAS system has very specific requirements towards scale and longevity. e-ID enabled applications will push the envelope into millions or billions of individually archived files with each their own access control and retention life cycle. Also, data will need to be physically stored for multiple decades, and will need to be readable at some time in the future. Long-term data integrity and readability (for humans and for tools) is a largely unsolved technical and organizational problem.

Finally, the TAS archive must be deployed in a simple and cost effective manner. The operational complexity should be kept at a minimum, in order to maximize deployment of the solution.

The e-health application domain is complex, as it is reflected in the myriad of use cases which can be derived from the scenario. The e-health domain poses complex requirements, especially if we want to protect the privacy of the different parties by normal use. Clearly, the current Belgian e-ID card does not satisfy to support all these requirements. The analysis is specific for the Belgian social security system, which can be considered as a case study of how to combine smartcards and privacy in the e-health domain.

The development of e-government services can significantly benefit from the e-ID infrastructure. We have presented two basic use cases for requesting and submitting information; many other services, such as tax declarations, can be implemented. The current e-ID technology based on public key certificates, imposes a unique identifier for the transactions between a citizen and all public services. This introduces privacy concerns, as all actions done with the e-ID can very easily be traced back to the e-ID holder.

e-ID cards can be most useful for financial applications as a first step towards general adaptation and dissemination of the card usage. Important prerequisites for a good usability of an e-ID token for financial transactions are legally valid signatures and legally valid identification, but also liability and anonymity.

In summary, services based on the e-ID should provide sufficient security guarantees to be trusted by the citizens. Moreover, the e-ID infrastructure should allow for interoperability between the different operation domains, while preventing un-necessary cross-domain linkages of information. In other words, a user should be able to use his single e-ID to perform health-care, government, and financial transactions without fearing any of the three transactions be linked to one another. Preventing the flow of cross-domain information is, in our opinion, an efficient way to technologically help reinforce civil values such as the right to anonymity and the right to non-discrimination. At the same time, for the sake of fairness and accountability, the e-ID infrastructure, when given the necessary legal permissions, must be capable of provably tracing down culprits in cases of fraud or cheating. One of our goals in the ADAPID project is to build an e-ID infrastructure that satisfies the above mentioned properties.

The outcome of this requirements study will be used for the definition of a framework, for the different basic research topics and for the applications to be developed. In a later phase of the project the initial requirements will be revised and it will be checked whether they have been implemented.

Bibliography

[BCOP04] D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano. Public key encryption with keyword search. In *Advances in Cryptology – EUROCRYPT 2004*, volume 3027 of *LNCS*, pages 506–522. Springer-Verlag, 2004.

[BOGW88] M. Ben-Or, S. Goldwasser, and A. Wigderson. Completeness theorems for non-cryptographic fault-tolerant distributed computation. In *ACM STOC*, pages 1–10, 1988.

[Bra99] Stefan Brands. *Rethinking Public Key Infrastructure and Digital Certificates – Building in Privacy.* PhD thesis, Eindhoven Institute of Technology, 1999.

[Bro02] Zach Brown. Cebolla: Pragmatic ip anonymity. In *Ottawa Linux Symposium*, 2002.

[CE87] David Chaum and Jan-Hendrik Evertse. A secure and privacy-protecting protocol for transmitting personal information between organizations. In *Advances in Cryptology, Proceedings of CRYPTO'86*, pages 118–167. Springer-Verlag, LNCS 263, 1987.

[CGKS95] Benny Chor, Oded Goldreich, Eyal Kushilevitz, and Madhu Sudan. Private information retrieval. In *IEEE Symposium on Foundations of Computer Science*, pages 41–50, 1995.

[CGMA85] B. Chor, S. Goldwasser, S. Micali, and B. Awerbuch. Verifiable secret sharing and achieving simultaneity in the presence of faults. In *IEEE 26th Annual Symp. on Foundations of Computer Science*, pages 383–395, 1985.

[CH02] Jan Camenisch and Els Van Herreweghen. Design and implementation of the idemix anonymous credential system. In *Proceedings of the 9th ACM conference on Computer and Communications Security*, pages 21–30. ACM Press, 2002.

[Cha88] David Chaum. The dining cryptographers problem: Unconditional sender and recipient untraceability. *Journal of Cryptology*, 1:65–75, 1988.

[Cha90] David Chaum. Showing credentials without identification: Transferring signatures between unconditionally unlinkable pseudonyms. In *Advances in Cryptology, Proceedings of AUSCRYPT'90*, pages 246–264. Springer-Verlag, LNCS 453, 1990.

[Che95] Liqun Chen. Access with pseudonyms. In *Cryptography: Policy and Algorithms*, pages 232–243. Springer-Verlag, LNCS 1029, 1995.

[CL01] Jan Camenisch and Anna Lysyanskaya. Efficient non-transferable anonymous multi-show credential system with optional anonymity revocation. In *Advances in Cryptology, Proceedings of EUROCRYPT'01*, pages 93–118. Springer-Verlag, LNCS 2045, 2001.

[Dai96] Wei Dai. Pipenet 1.1. Usenet post, `http://www.eskimo.com/~weidai/pipenet.txt`, 1996.

[DF89] Y. Desmedt and Y. Frankel. Threshold cryptosystems. In Gilles Brassard, editor, *Advances in Cryptology - Crypto '89*, pages 307–315, Berlin, 1989. Springer-Verlag. Lecture Notes in Computer Science Volume 435.

[DMS04] Roger Dingledine, Nick Mathewson, and Paul Syverson. Tor: The second-generation onion router. In *Proceedings of the 13th USENIX Security Symposium*, pages 303–320. USENIX, 2004.

[FM02] Michael Freedman and Robert Morris. Tarzan: A peer-to-peer anonymizing network layer. In *Proceedings of the 9th ACM Conference on Computer and Communications Security (CCS 2002)*, pages 193–206. ACM Press, 2002.

[FNP04] M. Freedman, K. Nissim, and B. Pinkas. Efficient Private Matching and Set Intersection. In *Advances in Cryptology – EuroCrypt'2004*, volume 3027 of *LNCS*, pages 1–19. Springer Verlag, 2004.

[GRPS03] Sharad Goel, Mark Robson, Milo Polte, and Emin Gun Sirer. Herbivore: A Scalable and Efficient Protocol for Anonymous Communication. Technical Report 2003-1890, Cornell University, 2003.

[JAP] JAP Anonymity & Privacy. `http://anon.inf.tu-dresden.de/`.

[KC04] William Ku and Chi-Hung Chi. Survey on the technological aspects of digital rights management. In *ISC*, pages 391–403, 2004.

[KM05] A. Kiayias and A. Mitrofanova. Testing Disjointness of Private Datasets. In *Financial Cryptography and Data Security*, volume 3570 of *LNCS*, pages 109–124. Springer Verlag, 2005.

[KS05] L. Kissner and D. Song. Privacy-Preserving Set Operations. In *Advances in Cryptology - CRYPTO 2005*, volume 3621 of *LNCS*, pages 241–257. Springer-Verlag, 2005.

[KSW02] G. Karjoth, M. Schunter, and M. Waidner. The platform for enterprise privacy practices - privacy enabled management of customer data, 2002.

[LRSW99] Anna Lysyanskaya, Ronald L. Rivest, Amit Sahai, and Stefan Wolf. Pseudonym Systems. In *Proceedings of the 6th Annual International Workshop on Selected Areas in Cryptography*, pages 184–199. Springer-Verlag, LNCS 1758, 1999.

[MvOV96] Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone. *Handbook of Applied Cryptography.* CRC Press, 1996.

[OS05] Rafail Ostrovsky and William Skeith. Private searching on streaming data. *Proceedings of Advances in Cryptology, (CRYPTO-2005)*, 2005.

[PH01] Andreas Pfitzmann and Marit Hansen. Anonymity, Unobservability and Pseudonymity – A Proposal for Terminology. In Hannes Federrath, editor, *Designing Privacy Enhancing Technologies*, Lecture Notes in Computer Science, LNCS 2009, pages 1–9. Springer-Verlag, 2001.

[PPW91] Andreas Pfitzmann, Birgit Pfitzmann, and Michael Waidner. ISDN-mixes: Untraceable communication with very small bandwidth overhead. In *Proceedings of the GI/ITG Conference on Communication in Distributed Systems*, pages 451–463, 1991.

[RP04] Marc Rennhard and Bernhard Plattner. Practical anonymity for the masses with morphmix. In *Proceedings of the Financial Cryptography Conference (FC 2004)*, pages 233–250. Springer-Verlag, LNCS 3110, 2004.

[RR98] Michael Reiter and Aviel Rubin. Crowds: Anonymity for Web Transactions. *ACM Transactions on Information and System Security (TISSEC)*, 1(1):66–92, 1998.

[RSA78] Ronald L. Rivest, Adi Shamir, and Leonard M. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM*, 21(2):120–126, 1978.

[RSG98] Michael Reed, Paul Syverson, and David Goldschlag. Anonymous Connections and Onion Routing. *IEEE Journal on Selected Areas in Communications*, 16(4):482–494, 1998.

[SBS02] Rob Sherwood, Bobby Bhattacharjee, and Aravind Srinivasan. P5: A protocol for scalable anonymous communication. In *Proceedings of the 2002 IEEE Symposium on Security and Privacy*, 2002.

[SWP00] Dawn Xiaodong Song, David Wagner, and Adrian Perrig. Practical techniques for searches on encrypted data. In *Proceedings of the 2000 IEEE Symposium on Security and Privacy*, pages 44–55. IEEE Computer Society, 2000.

[WP90] Michael Waidner and Birgit Pfitzmann. The dining cryptographers in the disco: unconditional sender and recipient untraceability with computationally secure servicability. In *Advances in Cryptology, Proceedings of EUROCRYPT'89*, page p. 690. Springer-Verlag, LNCS 434, 1990.

[wwwa] The enterprise privacy authorization language (epal 1.1). `http://www.zurich.ibm.com/security/enterprise-privacy/epal/`.

[wwwb] Platform for privacy preferences (p3p) project. `http://www.w3.org/P3P/`.