Security of eGovernment Systems

Case Study Report

Science and Technology
Options Assessment

Security of eGovernment Systems

Case Study Report

IP/A/STOA/FWC/2008-096/LOT4/C1/SC10

July 2013

PE 513.510

The STOA project 'Security of eGovernment Systems' was carried out by The Danish Board of Technology (DBT) with the Rathenau Institute (RI) and the Institute for Technology Assessment and Systems Analysis (ITAS), as members of the European Technology Assessment Group (ETAG).

AUTHORS

Anders Jacobi , Project Leader, DBT
Mikkel Lund Jensen, DBT
Linda Kool, Rathenau Institute
Geert Munnichs, Rathenau Institute
Arnd Weber, ITAS

STOA RESEARCH ADMINISTRATOR

Peter Ide-Kostic
Science and Technology Options Assessment (STOA)
Directorate G: Impact Assessment and European Added Value
DG Internal Policies
European Parliament
Rue Wiertz 60 - RMD 00J016
B-1047 Brussels
E-mail: peter.ide-kostic@ep.europa.eu

LINGUISTIC VERSION

Original: EN

ABOUT THE PUBLISHER

To contact STOA or to subscribe to its newsletter please write to: STOA@ep.europa.eu
This document is available on the Internet at: http://www.ep.europa.eu/stoa/

DISCLAIMER

The opinions expressed in this document are the sole responsibility of the authors and do not necessarily represent the official position of the European Parliament.

Manuscript completed in July 2013.

ISBN 978-92-823-4767-6
DOI 10.2861/34324
CAT BA-02-13-353-EN-C

Abstract

The STOA project focuses on challenges of eGovernment security in delivering public services across borders. By identifying key security barriers and enablers, the project seeks to point to promising avenues of policy development in the face of rapidly changing, disruptive ICTs and changing socioeconomic concerns in the EU.

In this Intermediary Report of the STOA project 'Security of eGovernment Systems' the results of the knowledge building phase 2 of the project are reported. In the knowledge building phase, consortium partners have conducted detailed case studies of the three application domains of eGovernment: eProcurement, eHealth and biometric passports. In the previous project phase, the ETAG consortium identified key security concerns for eGovernment in the following seven areas: network security, interoperability, identification, usability, privacy, access control and function creep. These cross-cutting and interrelated security challenges are examined in the context of the case studies. These security challenges are evaluated by the consortium to be the most relevant issues to study for providing the best input to the STOA panel in relation to future recommendations and policy options for establishing secure eGovernment systems and services. With this report synthesizing the result of the knowledge building phase of the STOA project Security of eGovernment Systems, the ETAG consortium emphasise the necessity to treat security and data protection as the most pressing organizational and technical challenges, but at the same time approach these issues proportionally given that there is a trade-off between increased security and usage and harnessing of the transformative potential of eGovernment to improve citizen access to and participation in the crafting of public governance. The way forward is to build in security, data and privacy protection from the early start of any eGovernment initiative.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

eGovernment is at the forefront of current public sector reform policies across Europe and the rest of the world where the use of information and communication technologies (ICTs) to digitize transactions and deliver public services is seen as a major leverage of public sector innovation. However, providing public sector information and services online also poses profound challenges to security and citizens' trust in governments, including threats to identity, privacy and data systems. Thus, safeguarding data and systems is of pivotal importance since it can influence governments' and users' willingness to adopt the online services offered.

The STOA project 'Security of eGovernment Systems' aims to assist policymakers in discerning policy options for meeting future challenges in securing eGovernment systems. Supporting the mobility of citizens and businesses is a key ambition of European policy making and regulation. However, the delivery of cross-border eGovernment services entails new security issues that need to be handled in order to ensure the trust and confidence necessary for widespread use of eGovernment services in the EU 27. The STOA project focuses on challenges of eGovernment security in delivering public services across borders. By identifying key security barriers and enablers, the project seeks to point to promising avenues of policy development in the face of rapidly changing, disruptive ICTs and changing socioeconomic concerns in the EU.

In this second deliverable of the STOA project 'Security of eGovernment Systems' the results of the knowledge building phase 2 of the project are reported. In the knowledge building phase, consortium partners have conducted detailed case studies of the three application domains of eGovernment: eProcurement, eHealth and biometric passports. In the previous project phase, the ETAG consortium identified key security concerns for eGovernment in the following seven areas: network security, interoperability, identification, usability, privacy, access control and function creep. These cross-cutting and interrelated security challenges are examined in the context of the case studies. These security challenges are evaluated by the consortium to be the most relevant issues to study for providing the best input to the STOA panel in relation to future recommendations and policy options for establishing secure eGovernment systems and services. With this report synthesizing the result of the knowledge building phase of the STOA project Security of eGovernment Systems, the ETAG consortium emphasise the necessity to treat security and data protection as the most pressing organizational and technical challenges, but at the same time approach these issues proportionally given that there is a trade-off between increased security and usage and harnessing of the transformative potential of eGovernment to improve citizen access to and participation in the crafting of public governance. The way forward is to build in security, data and privacy protection from the early start of any eGovernment initiative.

In this report a number of conclusions are drawn in relation to the three specific application areas. These case specific conclusions are then analysed on an overall level to identify the most prominent security challenges for EU level eGovernment services and systems. The challenges are described in the final chapter of the report and can be summarised as:

Purpose specification and level of interoperability

When deciding upon the establishment and design of an eGovernment system, the purpose of the system, its necessity and the proportionality regarding the data to be collected should be considered thoroughly.

Too high political ambitions and too little awareness of complexities

Defining the precise purpose of an eGovernment system requires sufficient awareness among policy makers of the technical possibilities and impossibilities of the system, organisational consequences and possible legislative conflicts.

Safeguarding security and privacy

In order to meet a high(er) level of security, more investments in security and privacy measures are needed, i.e. with regard to verification and authentication procedures, training government officials, or protection against malware attacks.

Does one size fit all?

Another question raised by the case study findings is whether different eGovernment systems require different choices regarding the level of interoperability and harmonization.

Interferences between requirements

The cases show that different requirements, such as security, interoperability, privacy and usability may be at odds with each other and need to be balanced in designing and implementing an eGovernment system.

Full digitalisation?

Full digitalisation may not always be the optimal solution: as mentioned above, the case studies illustrate that policy makers often lack sufficient awareness regarding technical (im)possibilities of eGovernment systems, resulting in too high policy ambitions.

Standardization

All cases show a lack of technical and legal harmonization to enable interoperability between Member States.

These challenges and possible solutions will be debated thoroughly at a conference to be planned in the third phase of the project. The scope of the conference is described at the end of the report. It will build on a life-cycle approach to eGovernment systems, which has been debated at an expert workshop as part of the work with the case studies. The life-cycle approach is also described in detail in the last chapter of the report. It consists of four phases: Decision phase, Design phase, Operational phase and Decommissioning phase, and at the conference the challenges will be analysed within the framework of this approach.

Overall the case studies show a number of complex and difficult challenges regarding security of eGovernment services. It will be the further ambition of the project to develop relevant policy options for dealing with these challenges.

1 INTRODUCTION

eGovernment is at the forefront of current public sector reform policies across Europe and the rest of the world where the use of information and communication technologies (ICTs) to deliver public services in the public sector is seen as a major leverage of public sector innovation. eGovernment is usually presented as using ICTs to 1) provide easy access to government information and services to citizens, businesses and government agencies; 2) increase the quality of services, by increased speed and efficiency; and 3) enable citizens to vote electronically. The global financial and economic crisis has heightened the urgency of governments to harness possible benefits of ICTs to achieve efficiency and effectiveness in public sector government (Ubaldi, 2011) and eGovernment is accordingly a top priority for governments and a major focus of investments. According to the ongoing benchmarking reports of Gapgemini, online availability of the 20 most common eGovernment services in Europe increased from 20 % in 2001 to 82% in 2010 (Capgemini et al., 2010).

eGovernment is also a powerful guiding vision for the transformation of public governance. The latest UN eGovernment survey (United Nations, 2012) clearly states the need to re-think government in terms of eGovernance – "placing greater emphasis on institutional linkages between and among the tiered government structures in a bid to create synergy for inclusive sustainable development" (ibid., p. 9). The potential transformational role of eGovernment has been acknowledged and championed by a range of global organizations who offer support to governments in moving to a transformational government approach: The OECD heralds a 'paradigm shift' as "Governments are shifting towards this broader view rather than focusing on the tools themselves. They are shifting from a government-centric paradigm to a citizen-centric paradigm…." (OECD 2009). The World Economic Forum (2011) elaborates on future government architectures stressing the importance of open networked government highlighting the transformational potential of eGovernment, but also the sensitivities of cyber security. In the EU, the current eGovernment Action Plan 2011-2015 (European Commission 2010) acknowledges the need "to move towards a more open model of design, production and delivery of online services, taking advantage of the possibility offered by collaboration between citizens, entrepreneurs and civil society" and to support "the transition from current eGovernment to a new generation of open, flexible and collaborative seamless eGovernment services at local, regional, national and European levels that will empower citizens and businesses".

The point of departure in the 'Security of eGovernment' project is the EU level inclination to the development and roll-out of EU cross-border public services. The intention to deliver public services across the 27 Member States is strongly emphasized in the eGovernment Action Plan 2011-2015 (European Commission 2010) where the reinforcement of mobility in the single digital market supports Action 84 of the Digital Agenda (European Commission 2010b) also calling on cross-border eGovernment services. However, the delivery of cross-border services entails new security issues that need to be handled in order to ensure the trust and confidence necessary for widespread use of eGovernment services in the EU 27. The need to enhance security, privacy and trust in order to increase confidence in eGovernment services is globally recognized, and the European Commission's eGovernment Action Plan necessitates Member state commitment to the enhancement of security of eGovernment solutions at a local, regional, national and federal level in support of the third pillar on trust and security of the Digital Agenda for Europe (European Commission 2010b).

The project 'Security of eGovernment Systems' aims at assisting policymakers in discerning policy options for meeting future challenges in securing eGovernment systems. The project focuses on challenges of eGovernment security in delivering public services across borders. By identifying key security barriers and enablers, the project seeks to point to promising avenues of policy development in the face of rapidly changing, disruptive ICTs and changing socio-economic concerns in the EU. In seeking to understand and expose the complexities of security requirements of eGovernment systems

and develop policy options for meeting them the project consortium has conducted a set of case studies in three application areas of cross-border eGovernment: eProcurement, eHealth records and biometric passports. The aim of the case studies is to analyse identified threats and challenges related to security of eGovernment and draw out conclusions leading to the identification of policy options for securing the delivery of secure eGovernment services.

This report is the second deliverable of the project 'Security of eGovernment Systems'. The report marks the end of the second phase of the project, the aim of which has been to build knowledge on the challenges of securing eGovernment services in procurement, health and border control. Based on the previous project report Elaborated Scope Description with special attention to identifying relevant case studies for phase 2 of the project, the bulk of the work in phase two has concerned examination of security challenges of cross-border eGovernment systems in the three domains of procurement, border control and health.

In the previous project phase, the ETAG consortium identified the most pressing security challenges facing the roll-out and operation of eGovernment systems. They include network security, interoperability, identification, usability, privacy, access control and function creep. These cross-cutting security challenges have been examined in the context of the three case studies, each exemplifying different aspects of the security issue at hand. The selection of the 7 security issues was based on desk research (benchmarking reports, interviews and informal talks with security experts, industry stakeholders and MEPs interested in the development of eGovernment systems). These security challenges are evaluated by the consortium to be the most relevant issues to study for providing the best input to the STOA panel in relation to future recommendations and policy options for establishing secure eGovernment systems and services.

The 7 security issues identified during phase I (ref. Report table 2, page 13) are:

- Network Security – also covering lack of internet availability, network attacks, systems architecture and network topology issues
- Interoperability – or the lack of interoperability due to semantics, lack of standards, different classification systems
- Identification – How to secure unique identification of participants
- Usability – The security issue coming from complexity of systems, skill levels of civil servants or other users (patients, citizens)
- Privacy – risk of revealing confidential information, identity theft, access to sensitive information, consent (opt in/opt out)
- Access control – Secure systems against intruders via access control mechanisms, possibly combined with identity management systems
- Function Creep – risk that confidential data could be used for other purposes than original, including intrusion on privacy, third party use of data

In each of the selected case studies, the specific importance and relevance of these 7 security issues has been addressed.

In the case selection we have tried to strike a balance between similarity and diversity. If cases are performed on very similar eGovernment applications, it is easier to compare them, while a diversity of

cases allows us to draw more general conclusions on other eGovernment application. For the goal of this project, we have opted for case studies resembling each other in complexity and scale of use, but differing in terms of user groups, societal sectors and technologies used. All case studies deal with eGovernment systems which are applied throughout the majority of EU Member States. This allows us to compare different member states and variations between national and European legislations. Also, the cases should have a certain level of complexity, in order to address the seven security issues we defined. The diversity among the cases involves variations in the provider-user relationship. One case should concern a Business to Government (B2G) relation, a second should involve a Government to Citizen (G2C) relation and a third could involve governments, citizens and businesses. Also, we need a measure of diversity in technologies in use: data storage (one large database, networks of databases or other devices), identification techniques (username-passwords, tokens, smartcards, biometrics, etc.). Finally, cases involve applications which differ in the goals for which they are used.

Work in the knowledge building phase 2 of the project has included extensive desk top research and interviews and informal talks with the project's expert group members, additional security and legal experts as well as national authorities from the country case studies and Members of the European Parliament. Desk top research has included policy documents, consultancy reports, and reports from international bodies. The report reflects the current state of the art of the project. Further discussions of project findings will be pursued with the expert group set up in the project's first phase and refined during the planned workshop with MEPs in project phase 3, of which the aim is to debate the security challenges of eGovernment systems and the feasible policy options for meeting them. In the previous project phase, an expert group was set up. Their role in the future phases of the project will be to refine the conference scope and subsequently discuss the outcome of the conference and give suggestions for future policy options for actions on securing the delivery of eGovernment services.

The main part of this report consists of three chapters dealing with eProcurement (chapter 2), eHealth records (chapter 3) and biometric passports (chapter 4). In chapter 5 the conclusions of the three cases are used to identify the most pressing issues as a basis for developing policy options and the scope of the upcoming conference is described.

The consortium would like to thank the people who helped write this report: Christian Henrich, Forschungszentrum Informatik, Karlsruhe, Germany, Soeren Duus Oestergaard and Kristian Duus Oestergaard, Duus Communication, Denmark and Max Snijder, European Biometrics Group.

2 CASE STUDY: EPROCUREMENT

Authors: Christian Henrich, Maik Herfurth, Forschungszentrum Informatik, Karlsruhe, Germany & Arnd Weber, Karlsruhe Institute of Technology

2.1 Introduction to eProcurement

This chapter describes the current state of public eProcurement in the European Union (EU) and worldwide and discusses possible security issues.

Procurement is the acquisition of goods or services, and public eProcurement refers to the use of electronic procedures by public institutions for conducting purchases on the Internet. Important examples of electronic procurement transactions are the publication of notifications and the submission of bids.

The value of public procurement spending in the EU amounts to around 19% of the GDP (European Commission 2011g). In some countries, such as Portugal, electronic procurement is mandatory. The EU's 2004 directive (2004/17/EC) aimed at supporting electronic procurement. The directive made it mandatory that tenders above certain thresholds are published Europe-wide. This is largely done electronically today. However, the Commission estimates that in the EU as a whole only about 5% of all public procurements above thresholds are done electronically. Transborder eProcurement is rarely seen. In 2009, more than 250,000 entities performed about 150,000 transactions above thresholds (European Commission 2011g), which means that the average contracting authority conducts only about one transaction per year. Of course, there is hope that once more procurements above thresholds are done electronically, the same electronic means will also be used for lower value purchases.

Public procurement is a field in which bid rigging and corruption can be seen (Thai 2009, OECD 2007). Furthermore, for many types of public procurement various paper documents need to be transmitted. Hence, electronic procurement is hoped to have the following effects:

- More competition as more competitors participate. If electronic procurement can be done easily from other countries, the number of competitors should increase and thus the costs of purchases decrease. Meyer (2011) reports savings of 2-3%.

- Lower transaction costs. Meyer reports about 0.3-0.4%.

As the value of public procurement in the EU is about 2 trillion €, a 3% savings would amount to 50 billion €. Achieving such savings is one of the objectives mentioned, for example, in the European eGovernment Action Plan 2011-2015 (European Commission 2010e).

Yet there are security risks when procuring on the Internet. For example, the content of bids is sensitive, and competitors might try to eavesdrop on prices or hack into systems in order to gain access to details of competing bids. There are also viruses, spam messages, etc. on the Internet that might hinder the proper functioning of eProcurement systems, just as any other IT-system on the Internet. Furthermore, as a traditional bid is signed by a representative of the bidder, some equivalent of a signature is needed so that buyers can rely on the seriousness of a bid. Documents may even be needed at court, so legally binding documents may be required. As long as no provably secure computers exist, tools for "digitally signing" documents might be hacked, as well. "Signers" could claim at court that a certain document was not signed by them; also, hackers might demonstrate that "digital signatures" are not valid if they succeeded in faking one. So eProcurement faces various security vulnerabilities. Yet these vulnerabilities may only be seen in practice once eProcurement is being widely used.

This chapter is focused on the potential security problems in eProcurement. First, an overview of procurement phases and of security solutions and techniques is provided. Security problems are discussed, including potential problems when using security tools. Short country studies both from within and outside of Europe as well as European initiatives are presented, including a new draft procurement directive from December, 2011 (European Commission 2011d) and the draft signature regulation (European Commission 2012f).

This chapter is essentially based on desk research. In principle, ETAG aims at reviewing existing assessments. However, we succeeded in identifying only one TA study that addresses procurement (Riehm et al. 2002). We have therefore reviewed many studies prepared by example consultancies and economists. It is, of course, possible that more relevant facts are mentioned in these and other studies than presented here. This chapter represents our best effort based on the large amount of literature reviewed, as listed in the references section. Some topics are mentioned because they were issues discussed at conferences or because they came up in explorative interviews. This is not the final project report; the findings are to be validated and refined during the next project phases. In particular, views of bidding and buying parties should be taken into account.

In Section 2.2, a short overview over the eProcurement process is provided. Section 2.3 presents security techniques that are employed in or useful for eProcurement processes. Existing obstacles to eProcurement are discussed in Section 2.4. In Section 2.5 an overview of how to secure computers connected to the Internet is presented. Several studies on the current status of eProcurement in different countries, including the EU, are presented in Sections 2.6 and 2.7. In Section 2.8, recent activities at the EU level are discussed, including the draft procurement directive. Thereafter, conclusions and options for action are presented in Section 2.9. The chapter concludes with a summary. An appendix lists events visited and experts talked to.

2.2 Overview of Procurement Phases

In this section the different pre- and post-award eProcurement phases are briefly described, following the structure given by the Siemens/time.lex study written by Graux and Meyvis in 2010 (2010a). The eProcurement process is generally divided into two phases, tendering (also called the pre-award phase) and purchasing (also called the post-award phase), separated by the award itself. Public eProcurement includes multiple stages, which are presented in the remainder of this section. Not regarded in detail in this study are the special provisions of EU directives for eAuctions, eCatalogues, Framework Agreements (with a restricted number of bidders), and Dynamic Purchasing Systems (which remain open to any bidder).

2.2.1 Pre-Award Phases

Before the award there is one potential buyer, often called "contracting authority", and several (competing) suppliers.

- "*eNotification* can be summarily defined as the electronic publication of tendering opportunities, including via procurement notices. As a unilateral process (involving only communication from the contracting authority to the tenderer, but not the other way around) it is relatively simple to implement compared to other phases." (Siemens/time.lex 2010a, p. 73)

- eAccess is the process of accessing tender documents and "refers to the ability to obtain (copies of) any tender documents and specifications that describe the scope and requirements of a specific procurement opportunity. In eProcurement, such information will of course be made available in an electronic format, typically by publishing the relevant information on one or

more website(s) or by sending it via e-mail as an automated response to a request from an economic operator. […] eAccess is […] a unilateral process […]." (Siemens/time.lex 2010a, p. 74)

"*eSubmission* – the electronic submission of tenders – is a more complex phase than those summarised above, due to its bilateral nature: rather than information merely being delivered to the economic operators (as in the earlier two phases), the economic operators will now need to be able to respond." (Siemens/time.lex 2010a, p. 75) "The authenticity and integrity of the offers will … need to be ensured, which notably poses interoperability challenges." (Siemens/time.lex 2010a, p. 75) A special role is played by the need to provide *eCertificates* or *eAttestations,* which demonstrate compliance with certain formal requirements and pose their own interoperability problems.

The phases of eNotification, eAccess and eSubmission are sometimes subsumed under the notion *eTendering*. *eEvaluation* and *eAwarding* refer to the partial or entire automation of the assessment of bids after the submission (eEvaluation) and the formalisation and communication of the outcome to the tenderers (eAwarding).

2.2.2 Post-Award Phases

eProcurement can be limited to pre-award phases, but the consistent integration of electronic means can significantly improve efficiencies by enabling Straight Through Processing (STP) by conducting the complete transaction (from eOrdering to ePayment) without any manual intervention.

- "*eOrdering* is the automatic placement of orders online, including particularly through the use of eCatalogues […]. This phase is optional, and will not take place in procurement contracts in which the contract conclusion already defines the exact supplies or services to be delivered under the procurement. eOrdering will only occur in cases where the concluded procurement contract has established a framework […] within which supplies or services can be ordered." (Siemens/time.lex 2010a, p. 77)

- "*eInvoicing* is the automated process of issuing, sending, receiving and processing of invoice and billing data by electronic means. […] [T]he invoice is not only generated but also delivered in an electronic format, without a transformation to a paper form being required. […] eInvoicing is a transversal process, since it plays a crucial role in any eBusiness process, rather than being specific to eProcurements. It has also been addressed as such: eInvoicing regulation and standardisation work at the European and international level is not specific to a public procurement context." (Siemens/time.lex 2010a, p. 78)

- "The exact methods of communication must be agreed between partners, and may be as simple as a one to one transfer of a data file sent via e-mail or FTP, or a fully integrated end to end process that may include the use of third party networks that track the files from point of entry to receipt...." (Siemens/time.lex 2010a, p. 186)

This chapter puts an emphasis on submission, as it is crucial for increased competition and as there are requirements regarding authentication and integrity. *ePayment* may be done as commonly.

2.3 Special Security Techniques for eProcurement

This section provides an overview over current security techniques that can be useful for eProcurement systems. For instance, encryption can be used to encrypt prices of bids, at least until the bid opening. Digital signatures can be used to replace the handwritten signature, e.g. on the bid. The EU signature

directive differentiates between various types of "electronic" signatures, which are described below. Other means include the authentication of a sender and the use of tamper resistant modules.

2.3.1 Encryption

Encryption schemes are used to encrypt digital documents to ensure confidentiality. An encryption scheme consists of an encryption algorithm and a decryption algorithm. The encryption algorithm requires a digital file and a key as input and outputs a cipher text of the digital file. The decryption algorithm takes a cipher text and a key as input and outputs the original file if the key used for decryption corresponds to the one used for encryption.

There are two classes of encryption systems, symmetric encryption and asymmetric encryption, which are described below.

A secure encryption scheme ensures that nobody is able to gain any information about the encrypted file from the corresponding cipher text unless they know the key used for decryption.

Symmetric encryption schemes use the same key for encryption and decryption. Modern schemes are very fast and efficient.

One big problem of symmetric encryption schemes is key management. Whether symmetric encryption is used for secure message transmission or for secure storage, the decryption key must be available for decryption. In the first case this means that sender and recipient must exchange a common key. This problem, called the key exchange problem, is often solved by using asymmetric key cryptography (see below). In the second case, the user must ensure that the key is stored safely and securely to be available to decrypt the data upon retrieval.

Asymmetric encryption schemes were invented in 1974 (Merkle 1974) and helped to solve one of the biggest problems of symmetric cryptography, namely key exchange. It has also made it possible for new techniques to be developed, such as digital signatures.

In an asymmetric encryption scheme, instead of one key used for both encryption and decryption there is a key pair of which one key is used for encrypting and the other one used for decrypting. The encryption key is often called the *public key* as publishing it does not compromise the security of the cipher text. The decryption key is supposed to be known only to the recipient and is also called the *private key* or *secret key*.

To encrypt a digital document an encryption algorithm takes the document and the encryption key as input and outputs a cipher text. The decryption algorithm takes the cipher text and the decryption key as input and outputs the original document. The encryption key is normally made public, so everybody is able to encrypt a message to the owner of the corresponding decryption key.

Note that encrypted information might be decrypted after a long time if the underlying algorithms get broken or if computing power increases sufficiently, perhaps after decades.

2.3.2 Digital Signatures

Digital signature schemes allow users to sign digital documents. It is used to achieve "non-repudiation". Non-repudiation means that the producer of a document cannot repudiate it because there is evidence that the document is genuine and can be attributed to the producer.

Digital signatures were first conceived in 1970 for use with high value purchases such as custom-made cars, to replace a handwritten signature on paper (Weber 2002). In this section only digital signature

schemes based on asymmetric encryption schemes are discussed. A digital signature scheme consists of two algorithms and operates with a key pair, very similar to asymmetric encryption schemes.

2.3.3 Public Key Infrastructure

The most important function of a certificate is to provide an unambiguous connection between an identity and a public key. For this, X.509 certificates use a hierarchical system of certification authorities (CAs). Each certificate is signed by a CA that assures that the public key indeed belongs to the identity specified by the certificate. To do this, the CA digitally signs the certificate. To ensure that the public key of the CA is indeed authentic the user has to verify it, e.g. by obtaining a certificate signed by a trusted CA. These CAs are often structured hierarchically so that there is a so-called root CA, which is supposed to be taken as the origin of trust. This root CA signs the certificates of other CAs after is has verified the public keys. The advantage for the user is that the user only has to trust one certificate of the root CA (called a root certificate) to build up a chain of trust to any certificate issued by any CA that is part of this system.

While in theory there is only a single root CA, the keys of which need to be verified, in reality there are several equal root CAs, meaning that the system is not a strict hierarchy. Modern operating systems often have the root certificates of several root CAs preinstalled.

A public key infrastructure (PKI) binds a public or a verification key to a user identity. A PKI consists of a set of parties as well as a set of policies and procedures and corresponding hardware and software to create and manage the required infrastructure using public key cryptography.

A full-fledged PKI requires each participant to possess a pair of a public key and a secret key. The public keys and their certificates used for SSL and TLS encryption are part of a PKI that does not encompass the user. This allows users to verify the authenticity of websites and use secure connections without being part of the PKI themselves. In contrast to this the PKI used for authentication by users of an eProcurement system requires each user to register in a PKI.

To become a part of a PKI each user has to obtain a certified public key. For signatures and authentication, to obtain a certificate from a CA that binds the public key with the identity, the user has to demonstrate his or her identity to the CA. The exact means to do this vary. The challenge is to find a balance between security (difficulty of obtaining a certificate for a false identity) and cost. The details are to be governed by the set of policies that are part of the PKI.

2.3.4 Implementing Digital Signatures Securely

In order to protect against abuse, secret signing keys can be stored in a tamper-resistant module, often called smartcard, or in a larger Hardware Security Module (HSM).

Unlike counterfeit handwritten signatures, counterfeit digital signatures are technically perfect (Langenbach, Ulrich 2002). So if a signature solution gets hacked, the situation becomes very difficult for the signer as well as for any party relying on it (called the relying party). Also, with imperfect solutions, signers who want to deny liability can simply claim to have become a victim of malware. Hacks might occur for various reasons. One is that hackers might wish to demonstrate that a system is insecure. As early as 2001, computer scientists from Bonn University designed a Trojan horse to forge a signature created using a smartcard (Spalka et al. 2001). So the challenge is to create a signing environment which reliably achieves “what you see is what you sign”, even in the presence of malware.

For further protection, a smartcard reader can be used to protect the PIN a user enters. As normal PCs might become subject to malware, a secure display could be used, e.g. for a contract to be signed. Trojan

horses as used in attacks on banking read the user's screen, send its content home, and send modified content to the user's screen (Bleyer 2011). This indicates the level of sophistication achieved by criminals. One possibility is to display the hash value of a document on a card reader, i.e. the user could compare the one created by the PC with and the one on the reader. In the future, secure compartmentalisation could be used for displaying documents correctly (see, e.g. General Dynamics 2011, Weber/Weber 2012; more on this in Section 2.5.). Also better platforms could be used, e.g. Sina (Secunet 2012). At a recent Commission event, Rannenberg reminded the audience of the issue of missing secure signing environments (Rannenberg 2011). As Schwemmer put it at a conference in 2011, players may consider implementing such means only if a severe problem has emerged, such as "signature deaths" (Schwemmer 2011).

Smartcard readers certified for use with digital signatures exist already, though usually without secure visualization. It has happened that such a reader certificate needed to be revoked (Bundesnetzagentur 2010), so a relying party might wish to store information on whether a reader was used which was certified at the time of signing.

As progress in mathematics or computing may mean that a digital signature can be counterfeited after a decade, for example, they may have to be re-signed to maintain the evidential value of digital signatures. A third party digitally signed time stamp should suffice to maintain the evidential value.

Another topic is that the relying party needs information as to whether the signature was valid at the point in time that the signature was made (chain model), not at the point in time it is verified (shell model). The reason is that the key may have been declared lost in the meanwhile or that the CA may have disappeared from the market (cf. Annex IV of the signature directive).

There are also the issues of the readability of document formats and the availability of software if one wants to verify digital signatures over a long period.

Verification components may need to verify the types of signatures and components used, which requires communicating these in the first place (Quiring-Kock 2009). A relying party may wish to store all the information mentioned above, for each signature, for later use in a dispute. Communicating this information, storing and updating it retains the evidential value, but contributes to the costs of digital signatures. On the other hand, without sufficient measures in place, there is a risk that signatures might not be usable in a dispute.

2.3.5 Electronic Signatures

Two different terms exist describing a signature for a digital document. The term *digital signature* describes a signature generated by a cryptographic algorithm as outlined before. The term *electronic signature* is broader. It also includes biometric signatures or digitally captured signatures, which in the easiest case is a scanned copy of a handwritten signature. This is not necessarily compliant with the EU Directive 1999/93/EC, however. The European Commission's definition of signature is: "It can be as simple as signing an e-mail message with a person's name or using a PIN-code. To be a signature the authentication must relate to data and not be used as a method or technology only for entity authentication." (European Commission 2006)

The strict legal requirements, especially the requirement that an electronic signature is specific to a certain document, means that in practice only digital signatures are used. In accordance with the literature and to avoid confusion the term electronic signature is used from now on often. In technical terms, digital signatures are meant.

Directive 1999/93/EC defines the following types of signatures:

1. "'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

2. 'advanced electronic signature' means an electronic signature which meets the following requirements:

   a) it is uniquely linked to the signatory;

   b) it is capable of identifying the signatory;

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

   d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable;" (article 2)

3. [Qualified signature:] "advanced electronic signatures which are based on a qualified certificate and which are created by a secure-signature-creation device" (SSCD, article 5)

The wording "means that the signatory can maintain under his sole control" might be interpreted in a way that the whole signing apparatus should be user-controlled. If a user had a practically unhackable device displaying what is being signed, and some secure approval procedure on it, like an entry of a passphrase, this would be the case. In practice, that clause has been interpreted to denote a smartcard, for example.

Sometimes the notion *qualified signature* is used for an advanced signature created with a SSCD. The major difference is that with a qualified signature, the signing key is always protected by an SSCD, while with an "unqualified" one it might be on the hard disk, though typically in the form of an encrypted file. However, if the encrypted key is copied with criminal intent, the criminal can use brute force to try to decrypt the file for accessing they key. Also, the key for advanced signatures will be in the clear in the computer's processor, where it might also be eavesdropped. Hence, tamper-resistant smartcards make faking one's signature more difficult. However, they make it necessary to first purchase and install a card and a card reader.

There are also *advanced signatures based on qualified certificates*, meaning that the signature is "only" advanced, but that the certification authority is accredited in a member state.

2.3.6 Commitments

The cryptographic algorithm of a *commitment* is a possible solution to the confidentiality problem of eProcurement.

A commitment scheme is a protocol in which the sender commits to a value v by sending a commitment c to the recipient. The recipient is unable to gain any information about v from c, but when the sender opens the commitment (by sending additional information) the recipient is able to verify that the value v has already been fixed when the commitment c was sent.

One example of a cryptographic commitment scheme is the *universally hiding discrete logarithm commitment* (UHDLC, Chaum et al. 1987), sometimes also called *Pedersen commitments* (Pedersen 1992).

A possible application for eProcurement is the following. Instead of sending the bid itself, the bidders submit a commitment to the bid. When the bidding process is closed, all participating bidders open their commitments and reveal their bids. As the bids are only revealed when confidentiality is no longer required, at no point sensitive data is stored outside the bidders' computers. This is obviously not true for bids with confidential content. But even in this case the use of commitments for the tendering process provides additional security as information about the content of the bid is only sent out by the bidder after the bidding phase has ended.

2.3.7 Authentication Methods

Instead of using a digital signature, participation in an eProcurement system can also be based on a password authentication system, as is common in Internet eCommerce. Log-in would be with a PIN or, ideally, with a somewhat longer passphrase. A more sophisticated approach would be to use a PKI-based authentication system. While in a normal password-based system obviously both parties know the password ("shared key"), one can use a PKI for encrypting a secret such that the verifying party, e.g. a server operator, can verify that the party trying to connect is in possession of the related secret key. This provides greater security. However, keys and certificates have to be managed in a suitable registration procedure, which makes PKI-based authentication more costly and more difficult to use across borders.

"In practical terms, username/password based systems pose no interoperability challenges other than the completion of the registration process (which may be complicated due to language barriers or the need to provide information which is only available at the national level). PKI systems on the other hand are currently [as of 2010] almost universally unable to accept foreign solutions, meaning that foreign economic operators will be unable to use eSubmission unless they can obtain a PKI solution issued in the country in which they wish to submit an offer. Thus, in practical terms, the choice of a PKI based authentication system has serious negative impacts on cross border interoperability." (Siemens/time.lex 2010a, p. 76)

According to Siemens-time.lex (2010a), "a small number of countries (with Ireland being the main example) have implemented systems based on simple username/password authentication. While such systems are inherently considered less secure than PKI based systems, the disadvantage of lesser security of username/password based systems appears to be largely theoretical in practice, since no incidents related to this approach have occurred since their introduction." (Siemens/time.lex 2010a, p. 31)

This means that the most simple log-in procedure, at least until 2010, did not cause any major problems and seems usable just as elsewhere in Internet eCommerce.

2.3.8 Tamper-Resistant Modules

As mentioned, secret cryptographic keys may need to be stored in tamper-resistant tokens (smartcards).

Another application of tamper resistance could be the following. For example, in military procurement one could use a Hardware Security Module (HSM) to conduct computations invisible to the operator. The system could be designed such that only the parties involved can see the documents in the clear, which would not only help against eavesdropping by insiders, but also against hacks into the system around the HSM.

An HSM could also be used for the protection of bids until the opening.

2.4 Security Issues of eProcurement

There are several obstacles to the widespread deployment of eProcurement, in particular for transborder eProcurement. There are language problems, problems with foreign eAttestations, and of course often a lack of geographical proximity. Last but not least, there are interoperability problems of digital signatures and PKI-based authentication (European Commission 2011g). In this section, we focus on security-related obstacles.

Thai (2009) and the OECD (2007) have shown that public procurement is a sector which often sees bid rigging and corruption. This means that at least information about the price of a bid is sensitive. Frequently, and in particular in military procurement, the contents of tender docs and bids are sensitive. This means that it must be anticipated that criminals might try to learn about bids by hacking into procurement systems. Furthermore, it must be anticipated that procurement systems on the Internet will be attacked just like any other system for criminal, political or other reasons. In this section an overview is provided of current threats and attacks. Similar attacks could be used to attack procurement systems.

2.4.1 DoS and DDoS (Attacking Availability)

A comparatively simple and therefore common form of attack on web services is the so-called *denial of service attack (DoS)*. This attack targets systems or subsystems with the goal of disrupting their functionality in part or completely. If a DoS attack is executed from several systems in parallel, it is called a *distributed denial of service attack (DDoS)*. Often the source is a *Botnet*, a network of "robots", i.e. hacked computers, which send out large numbers of messages. DoS attacks are considered prominent threats for systems connected to the Internet (BSI 2012).

A DoS attack affects the availability of a system and may in the worst case lead to a total failure of the complete system or a subsystem. In the simplest case this can be used to sabotage the eProcurement process without any benefit to the adversary. If the adversary is a member of the eProcurement system, he may use this to prevent other members from participating, at least temporarily. If this is used to effectively exclude competitors from business, the adversary may gain financial advantage.

It is easy to perform Botnet attacks, performing denial of service attacks or sending spam mails. Somebody could even make a large attack simply by mistake (Hange 2011). The reason is that one can buy toolkits to design attacks. Massive spam attacks with DoS-effect have been seen (cf. the attacks on Estonia in 2007).

It is hard to completely protect a system against DoS attacks (especially against DDoS attacks, the form most common nowadays). There are, however, several widely-used measures to alleviate the consequences of such an attack, which typically lasts only several hours (with at least one exception, the attack on Bayer in 2011; Hange 2011). The main reason why DoS attacks may impair the availability of eProcurement systems but are not practical for manipulating eProcurement processes is that they are almost impossible to conceal. Long-lasting DDoS attacks are rare since they are costly for the attacker and relatively easy to compensate for by allocating additional resources to the attacked infrastructure. The true threat of DoS attacks is preventing access to the server during a critical time (e.g. immediately before a tendering deadline) by running a DoS attack that the provider is unable to respond to due to either time or cost constraints.

There are several standard measures against such attacks, e.g. using filter mechanisms and redundant infrastructure. An attack before an important deadline may be averted by extending the deadline accordingly or by using a time-stamping service and uploading later.

2.4.2 Identity Theft (Gathering Credentials)

An eProcurement system using credentials entered by a human user is vulnerable to the attack of an adversary that convinces a user to enter the credentials into a fake website instead of into the real one, thereby gaining access to these credentials. This kind of attack is called *phishing*, a word created out of "password" and "fishing".

An adversary who knows the credentials of another user of an eProcurement system is able to impersonate this user until the theft is noticed and resolved. The adversary may learn sensitive information about the owner of the credentials (e.g. by obtaining documents containing information about their business) or participate in the eProcurement process with the intention of harming the original owner (e.g. by making wrong offers, cancelling existing contracts or undercutting prices).

Phishing sites are specifically tailored to the target audience and imitate single websites. The likelihood of an attack depends on the use of the eProcurement system (the more users it has and the bigger the volume of transactions is, the more likely is an attack) and the value of the information that can be obtained through phishing. Successful eProcurement systems with large transaction volumes are most certainly threatened, so countermeasures are advisable.

Like attacks based on social engineering, these attacks target human users. There are two major approaches to protecting systems against these attacks. The first is to educate employees having access to credentials, making them aware of clear security signs and procedures to make detection of fake websites more likely, thereby minimizing the probability that credentials are successfully "phished". The second approach is to make the information entered by humans less valuable by adding information used only once (to prevent repeated abuse with stolen credentials) or even responses depending on challenges given by the server (*challenge response authentication*). Countermeasures against these kinds of attacks are similar to security mechanisms used by online banking systems.

2.4.3 Malware (Attacking the Client)

There are several types of attacks aimed at the personal computer of the user of an eProcurement system. They attempt to gain access to the computer by installing a program on it, normally without the knowledge of the user. The general term for these programs is *malware*. There are several other notions to describe the different kinds of malware such as computer virus, Trojan horse, worm, spyware or rootkits. While these names denote different types of malware, the distinctions are not always clear as they refer to infection strategy as well as to behaviour. They all have in common that they are potentially harmful for the user of the infected PC (see Simons 2011 for an overview of how to hack into existing computers).

Depending on the exact program, the consequences of an infection can be quite severe. A malware program may interfere with the functionality of the PC, leading to slower performance or loss of data. More sophisticated programs are able to stay undetected and use the PC for their own means, turning it into a part of a botnet. But there are also several malware programs that do not attempt to control the computer but instead collect information entered by the user (including user credentials like passwords). One example for such malware is the Trojan horse Trojan-GameThief.Win32.WOW.el that specifically targets users of the popular massive-multiplayer online role-playing game "World of Warcraft", stealing their login data to steal and sell their accounts. It is to be expected that widespread use of eProcurement will face a similar threat if there is a way to turn sensitive information gained this way into money.

While the threats of malware will likely increase with the increased use of eProcurement, this is already a dangerous attack on businesses, mostly for industrial espionage. There are two major approaches to infect a target system. *Drive-by exploits* use a malicious website and a weakness in the user's web browser

to infect the system. *Targeted malware infiltration* targets a specific group of users and convinces them to initiate or allow the installation of the malware. Strategies to protect against these attacks depend on the attack vectors and are discussed in the subsequent sections.

2.4.4 Drive-by Exploits

Drive-by exploits attack a user who is visiting a malicious website with a vulnerable browser. Certain weaknesses allow the server to inject and execute code in the browser and therefore on the client system without the interaction and knowledge of the user.

The consequences of such an attack depend on the code that is executed, but in most cases it is possible to make the client system install arbitrary malware.

The best protection against such attacks is the use of up-to-date software (especially browser) and operating system. A better but more complicated solution is the separation of the system used for browsing the Internet and the productive system. There are solutions using virtual machines as well as the trivial solution of using separate computers. If virtualisation is used, a procurement compartment could be reserved for digitally signed procurement code only. The communication between compartments (or isolated systems) is a challenge.

Drive-by exploits are a very prominent source for infections of computer systems and therefore also pose a threat for systems involved in the eProcurement process.

2.4.5 Targeted Malware Infiltration by E-Mail or Social Engineering

A second common way of distributing malware is targeted malware infiltration by e-mail or social engineering. The aim of the attack is to convince the victim to install the malware himself. For this the attackers contacts the victim directly, for example using e-mail, and persuades them to install the malware, which is disguised as a desirable piece of information, for example a software update.

As the user installs the malware, it receives all the privileges and rights the user possesses. The user is more likely to tolerate strange behaviour like requests to enter sensitive information, since he trusts the software. This makes this attack the most specific and most elaborate but also the most dangerous attack as the attacker may gain not only complete control of the user's computer but also the user's cooperation.

There are two important ways to protect against these attacks. The first and most important is the correct education of users about social engineering (as this is an attack vector that is generally used to gain access to and knowledge of secured systems) and the establishment of clear and unambiguous security policies for users. This has to encompass the use of social networks, but also traditional communication channels such as telephone or e-mail. The second way is to grant a user no more rights on their system than are required to do their work. Installing and updating software should be done by a system administrator with security expertise. This also helps against other attacks.

Targeted malware infiltration is relatively expensive and time-consuming for the attacker in relation to the number of targets, but with the increased importance and prevalence of eProcurement a corresponding increase of number of these attacks is to be expected.

2.4.6 Hacking of Webservers (Attacking the Service Provider)

A significant number of web servers are vulnerable to attacks. Instead of attacking the user's PC, an attacker may therefore choose to directly attack the server providing an eProcurement service. Most of these weaknesses are due to out-dated software running on the server.

Depending on the details and the specific success of an attack, the consequences may be severe. An attacker may gain complete control over the server. This means that the attacker is able to do everything the owner of the server can do. In less successful attacks the attacker may only gain access to sensitive information stored on the server or change the behaviour of the server.

Protecting servers completely against attacks from the outside is hard since they have to be accessible over the Internet, giving the attacker access as well. The most important countermeasures include keeping the software up to date and reducing the accessibility as much as possible without interfering with the functionality.

Central servers containing information about eProcurement procedures probably are a profitable target for attacks and require special protection. The assessment of how much protection is necessary depends on the content and exact nature of a server and is out of scope of this work. Still, as currently no provably secure systems exist and formal verification of software is a topic of ongoing research, it is impossible to entirely eliminate vulnerabilities and zero-day exploits that address confidential procurement data or prevent the attacked system from running properly.

2.4.7 Multi-step Attacks (Attacking the Infrastructure)

Multistep attacks are elaborate attacks in which, first, parts of a central infrastructure are compromised and then in a second step the actual target is attacked. Examples are attacks on the certification infrastructure to gain the ability to distribute fabricated certificates that are recognized as valid by the target system or to compromise servers distributing software updates in order to modify software updates for the target system to contain malware (attack on Diginotar in 2011). It appears that Diginotar, a CA used by the Dutch government, did not take immediate action, nor publish the attacks in time, see Prince (2011). Similarly, there have been reports about a hack into the Verisign systems (Reuters 2012).

These attacks are very elaborate but promise huge rewards as the identity of anybody could be faked. A successful attack on the certificate infrastructure may effectively abolish secure communication, making the authenticity of the sender or recipient of a message as well as its secrecy uncertain. Compromising update servers and infecting software updates with malware provides the attacker with control over the affected system.

Protecting against these attacks is very hard for users as they have to trust that the infrastructure itself is protected. Enhanced control of CAs could help.

These attacks become more relevant for eProcurement systems when a centralized infrastructure is used since such a target is very rewarding for an attacker.

Possibly trust models other than certification could be used, but this cannot be investigated here. As long as CAs need to be used, it might be necessary to control them more intensively than was done with Diginotar. Taking into account the report about Verisign, it might even make sense to have government-run CAs for government purposes. Not that it would be guaranteed that these will work error-free, but they could be set up in a way that they have fewer incentives to hide attacks.

2.5 Securing Computers

2.5.1 Paths for Securing Computers

As mentioned above, certain attacks are difficult to protect against. Operators use penetration tests to protect against main attacks (cf. OWASP 2012). However the situation may get worse. The Stuxnet attack

(Falliere et al. 2011, Langner 2011) has demonstrated that an attack is possible even if the target is well-protected. Stuxnet attacked a very specific target using zero-day exploits (weaknesses that are exploited before they are known and patched) and establishing its own infrastructure to update itself. It also managed to bridge the so-called air gap between PCs connected to the Internet and computers that for security reasons were not connected to the Internet using USB devices. While this scenario is not typical, it demonstrates the difficulty to protect against an ambitious and capable adversary.

In general, cybercrime and cyberwar are becoming professionalized and industrialized (Advanced Persistent Threats, APT). Major attacks, such as on company data, are performed using social engineering (Waidner 2011). For instance, Trojan horses can be put into specific systems by crafting a personalized email, using information from social media, with a fake sender address and an attachment containing a Trojan horse (Hange 2011; see Open Hypervisor [2011] reviewing a recent attack on the company RSA). Manufacturers of Trojan horse toolkits even guarantee that virus scanners won't notice them for 10 days (Bleyer 2011); see e.g. Bleeding Life from Damagelab (http://damagelab.org/lofiversion/index.php?t=20426). eProcurement is on weak ground if there are players out there who know vulnerabilities for months, if not more, and work on exploiting them (see Dalton 2009 for information about weaknesses which can neither be published, nor be dealt with).

How to secure computing systems? A list of options has been provided in Weber/Weber (2012):

- "Future updates of Microsoft Windows might address this problem. However, completely securing Windows 'isn't going to work', as Paul England of Microsoft put it [England 2008], due to the complexity and desired extensibility of the system. Also, attacks often exploit weaknesses of applications.

- Other operating systems, such as the Apple Macintosh system or Linux, are similar to Windows and therefore would probably also be attacked in a similar manner as soon as the user base is large enough for criminals to consider attacks worthwhile.

- Yet another approach would be to totally redesign computers from scratch. However, in practice such a system would not be very useful as existing user applications and data could not be used on such a system.

Another approach would be to use physically separate machines, and only use them for certain security-critical actions. While this works for small devices such as smartcard readers with a display and may also work for certain applications such as military ones, these solutions are costly and inconvenient, just like rebooting a different operating system. Also, if the smart card reader can be hacked [Secorvo 2010] or if the vendor demands that the user only operate it in an environment free of malware, the risk is only marginally reduced.

Existing hypervisors have not been designed to provide bullet-proof isolation to laypersons." (Weber, Weber 2012)

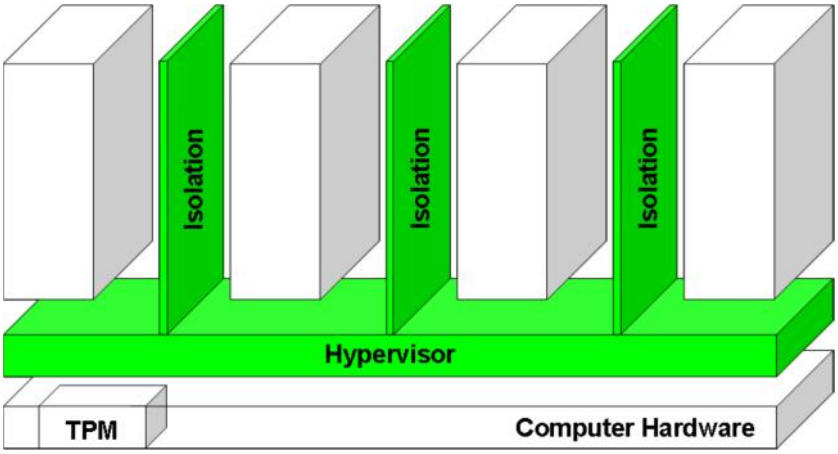


Figure 2.1: High level architecture of a secure hypervisor. Computer with a hypervisor (green), providing isolation to the operating system compartments (white). "TPM" refers to the "Trusted Platform Module" used to measure the correctness of the hypervisor system. The hardware needs to support similar "curtaining" (source: Weber, Weber 2012).

The following remedies have been discussed in the public. A large Internet security project could be worked out, a kind of a Manhattan project, addressing all kinds of computers including smart phones (Vishik of Intel, 2011). More concretely and already on-going, there are initiatives in the US to use virtualisation for a highly secure separation of tasks, each running in its own virtual machine (General Dynamics 2011), based on the Intel TXT architecture (Arbaugh et al. 1997, Grawrock 2006; similarly AMD VT). Even better from a security point of view, open source virtualisation could be used to make sure that no functionality can be hidden (Pfitzmann et al. 2001). Virtualisation could make crafted attacks more difficult, as companies could ensure that only trusted information is used in a company or procurement compartment, while private mails etc. would have to be read outside. Virtualisation could thus be used to enforce code-signing, which would work to reduce the spread of malware including botnets (see Figure 2.1).

Some researchers claim to be able to produce verifiably secure systems (Heiser et al. 2010). Related research towards creating practically unhackable virtualisation has been supported by the EU (see Kuhlmann, Weber 2009). Often, the implementation of security measures has a "commons" nature, as their effect is enjoyed by all. However, the costs of developing protective means are born by a few, and if they do not see a business case, they will not design them. Society would, however, benefit if somebody undertook the effort (Waidner 2011). Some government push could therefore help. In 2012, the following list of desired actions for migrating towards secure computers was published (Weber, Weber 2012):

1. "Privately financed marginal improvements.

2. A large government-funded project, starting with a proper, threats-based specification of hardware and software and followed by subsequent implementation. This would take the commons-nature of the problem into account, i.e. the distribution of costs across many users.

3. Governments create incentives via regulations or procurement. Requirements might push this approach, similar to the incentives provided by PCI-DSS (Payment Card Industry Data Security Standard), the Sarbanes-Oxley Act on auditing requirements, requirements for Trusted Computing, or military requirements.

4. Global discussion of this path will create demand. Think of the changes in the car industry, which was challenged by events such as publication of a book titled 'unsafe at any speed' [Nader 1965]. Also imagine big customers demanding updates towards the goal. Newsletters and our website http://open-hypervisor.org/ can also be regarded as steps towards the creation of demand."

The European Parliament could consider creating incentives to procure such more secure computing systems.

2.6 Current State of Play in Europe

2.6.1 General

In the EU, electronic procurement is governed by two directives. Directive 2004/17/EC addresses certain utilities, such as water, while Directive 2004/18/EC addresses public supply contracts and public service contracts in general. They contain rules on the electronic publication of procurement notices and the submission of bids. eNotifications have been made mandatory only above certain thresholds, which currently are between € 130,000 and € 5 million, depending on the type of work to be conducted (for an overview, see European Commission, 2012a, and Official Journal, 2012).

In 2009, more than 250,000 entities performed about 150,000 transactions above the thresholds (European Commission 2011g), which means that the average contracting authority conducts only about one transaction per year, if any at all. This is of relevance when analysing the transaction costs of traditional paper systems vs. electronic systems (set-up, costs for PKI solutions, fees for sites if used, etc.). In general, no more than 5% of submissions above thresholds are conducted electronically, as mentioned before.

Electronic publication of tenders and access to tender documents seems to have reached eProcurement nearly universal availability in 2010, with the exception of Greece, where no advanced infrastructure could be identified (Siemens/time.lex 2010a, p. 73). The Siemens/time-lex study evaluated the state of development in the different European countries. They found "that data collection is still in its infancy in most Member States" (Siemens/time.lex 2010a, p. 25).

2.6.2 eSubmission

It seems various procedures are used for conducting eProcurement submissions with regard to achieving non-repudiation.

1. Simple PDF-files are sent via email, e.g. by the World Bank and the European Commission (Rosenkötter et al. 2011, p. 74).

2. Various electronic files are transmitted on some channel and a paper document referring to these files is signed with a handwritten signature. This procedure is used for example by some German cities (cover sheet ("Mantelbogen"), ibid.).

3. Some websites use simple, password-based authentication, e.g. the Irish eTenders site (ibid.). "The only really cross border accessible systems are the ones that kept things very simple (username/password based systems), and contrary to concerns, no notable security incidents have been observed." (Siemens/time.lex 2010a, p. 324)

4. Others use local software for signing bids, which are subsequently sent to the contracting authority, or uploaded to a server, for instance in Estonia (Rosenkötter et al., p. 74).

5. An eProcurement website is used in which a digital signature module is used (ibid., p. 75. As the authors of the Siemens time.lex study (2010a) observed in 2010, "Countries which rely on eSignatures for electronic authentication have (with few exceptions) failed to resolve the cross border accessibility challenge."

6. It appears that some sites use a PKI system for authentication only. These "are currently almost universally unable to accept foreign solutions, meaning that foreign economic operators will be unable to use eSubmission unless they can obtain a PKI solution issued in the country in which they wish to submit an offer" (Siemens/time.lex 2010a, p. 24).

This means that simple systems, e.g. those based on passwords, have so far been appropriate, while digital signatures in general have not been available for cross border procurement.

The Siemens/time.lex study (2010a) investigated the situation in 30 EU member states and the EFTA countries Norway, Iceland and Liechtenstein. They identified use of central purchasing body platforms as well as of privately run websites (p. 134). Such central providers are quite able to manage eProcurement, as they would do it often. They can also manage the formal processes well on behalf of individual contracting authorities and provide the results conveniently.

However, it appears that there are hundreds more contracting authorities using their own solutions (Siemens/time.lex 2010a, p. 134, referring to Capgemini et al. 2009). It was not possible to identify how many contracting authorities use local procedures, and how many use central servers. Cattaneo reported in 2012 that there are 331 eProcurement platforms running in Europe, of which 154 offer eSubmission. National platforms are operated in 19 of the member states (Cattaneo 2012).

eSubmission is available in 93% of the member states, even if it is hard to measure whether eSubmission is used in practice (Siemens/time.lex 2010a, p. 175). eSubmission is already mandatory for some procurements in only a few countries (Austria, Portugal and Sweden) (Siemens/time.lex 2010a, p. 175).

eSubmission systems also need to take into account that the confidentiality of the bid needs to be ascertained up to the submission deadline and ultimately up to the opening of the bids.

2.6.3 Low Level of Use of eProcurement

eEvaluation and eAwarding functions are available in a majority of the member states (17 out of 27, according to [Siemens/time.lex 2010a, p. 77]). All in all, significant obstacles do not appear to have been encountered during these phases. A review of the use of eCertificates and of post-award phases is not made here, as these do not pose special security problems to be regarded in this study (see Siemens/time.lex 2010a, p. 24, 79f, 87, 258).

The Siemens/time.lex study found that the Directives 2004/17/EC and 2004/18/EC had been implemented by only 11 of the 27 member states by 2010 (ibid., p. 20).

As mentioned, it is believed that no more than 5% of the submissions above the threshold are made electronically. Given the lack of proper statistics, it seems that actual figures for all eProcurement transactions might be higher if we take into account the simple transmission of PDF files or the use of paper for the binding contract itself.

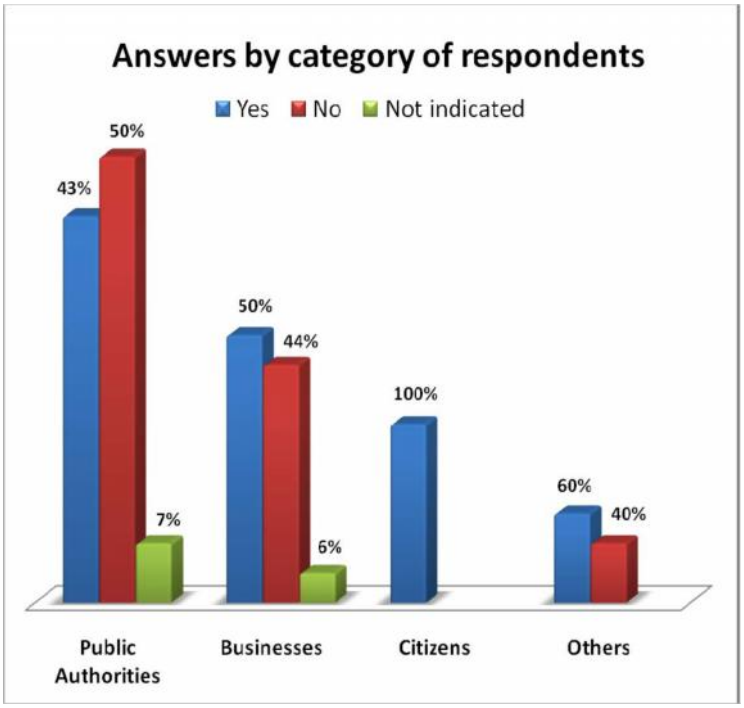


Figure 2.2: Answers to the question "Should EU law impose e-Procurement?" (from: Summary of responses to the Green Paper on expanding the use of e-procurement in the EU, European Commission, 2010f).

In a response to a Commission Green Paper, about 50% of the participants expressed that they are against mandatory electronic procurement (European Commission 2011g p. 53; Ferger 2011). Similarly, at the Commission-organised conference "Electronic Procurement – Challenges and Opportunities", 39% of registered participants stated that they do not consider using eProcurement, as Alain Deckers said (Deckers 2012). One reason mentioned is the high complexity. The European Commission (2010f) has summarised this kind of feedback as follows: "Complexity in this instance covers two main aspects: complexity of the technical environment and complexity of legislation/processes. Technical reasons cover technical sophistication, low user-friendliness of systems and the existence of too many technical solutions....Some replies highlight that there are too many eProcurement solutions within one single country, or region and that companies have to adapt to each one of them….Generally there is 'no exchange of current invitations to tender between the individual procurement platforms, and at best (this) is only possible through commercial service providers'. As a result, some contracting authorities need to use several platforms to receive enough tenders….The legislation/processes are generally perceived as overly complex, sometimes requiring dedicated resources..." (ibid., p. 10) Some expressed the view "that certain existing challenges should be addressed first, such as: interoperability, security of sensitive data, standardised eligibility criteria and certificates, decreasing the number of eProcurement solutions and the complexity of systems." (ibid., p. 16); see Figure 2.2. From interviews we have learned arguments such as: A personal trust relationship to a supplier is needed; paper is easier to handle than digital signatures, as it is easy to handle several signatures, even in copies.

2.7 Short Country Studies

2.7.1 General

Three countries have been selected. The first one is South Korea. It was selected because, according to the United Nations and the OECD, it is a good case (National Information Security Agency 2010). As early as

2007, most public procurement was done electronically. Also, digital signatures are used. The second country is Portugal. It was selected because eProcurement has been mandatory there since 2009 (Ricou 2010), and an ID card is used for signing submissions. The third country is Germany, as it is the largest EU country and has no mandatory eProcurement.

Table 2.1: Significance of public eProcurement, country comparison

Country	Share of eProc/total gov. procurement	No. of electronic transactions	Volume of electronic transactions	Non-repudiation
Germany	2010: ~4% (Vergabeblog 2011) [x]	unknown	unknown	Until 2008: qualified Since: also advanced (Siemens/time.lex 2010a, p.134, 307)
Portugal	2009: 100% [xx] (Rosenkötter 2011, EC 2010d)	30,000 (Ricou 2010)	2010: € bn 5.8 (Ricou 2010)	Qualified signatures (Siemens/time.lex 2010a, p. 3, 75)
South Korea	2007: 92% (Ovum 2009) 2008: ~60% (Kang-il Seo 2009)	2005: 20 mio (Soontiens et al. 2007)	2008: $ bn 63 (Kang-il Seo 2009) 2011: $ bn 50 (UN 2011)	Advanced sig. (European Comm. 2010d)

[x] It was not possible to determine whether, for example, purchases from electronic catalogues or offers such as PDFs with scanned handwritten signatures are taken into account in this figure.

[xx] Even below EU thresholds.

There are differences in the information presented on these three countries in terms of the aspects covered and the figures presented. This is due to the lack of better material identified so far. Still, large discrepancies are visible.

2.7.2 South Korea

The "Korea Online E-procurement System, or KONEPS, won the United Nations Public Service Award (PSA), and was selected by OECD as one of the best cases for improving transparency, and won the 'Global IT Excellence Award' from World Congress on Information Technology (WCIT) in 2006." (National Information Security Agency 2010, p. 24) In 2009, B2G e-commerce volume accounted for South Korean Won (KRW) 59,456 billion (about € 40 bn, ibid. p. 42). Of this amount, the volume of purchasing goods and services was KRW 31,024 billion and the construction contract volume was KRW 28,432 billion. Outside Koneps, there are "20 public enterprises that operate independent e-Procurement systems" (Kang 2012).

South Korea established interoperability among accredited CAs in 2001. For banking and stock trading, the use of certificates has been mandatory since 2005. Users have been provided a secure environment (HSM) since 2006. "All electronic signing operations are performed within the BIO HSM […]" (apparently a hardware security module with a fingerprint reader, cf. Moon 2010, p.18; it was not possible to verify whether signatures are exactly equivalent to advanced signatures in Europe). The Ministry of Information and Communication (MIC) arranges laws and decrees. The MIC is responsible for the management of CAs. The Korean Information Security Agency represents the electronic signature authentication management centre and issues certificates for accredited CAs (Baer 2011).

KONEPS integrates the entire procurement work. Transactions are secured through encryption and digital signatures.

South Korea has undertaken some steps to prevent attacks. In 2009, the Korean government decided to step up the prevention and response system to DDoS (Distributed Denial of Service) attacks, after experiencing a DDoS attack on July 7, 2009. In particular, it was decided to establish an emergency rescue service system for small-sized public offices and SMEs. Moreover, 'response scenarios for risk situations' will be developed to strengthen the national capacity to respond to cyber risks, and public-private drills will be put to practice (National Information Security Agency 2010).

2.7.3 Portugal

Portugal made eProcurement mandatory since 2009 for all public bodies, including municipalities, regional authorities and public companies. A National System of Public Procurement (NSPP) was created and made mandatory for all public institutions (around 1800 entities). The system is currently managed by a new entity, Entidade de Serviços Partilhados da Administração Pública (ESPAP).

In Portugal legislation was produced to pre-qualify the privately owned electronic platforms for the use in public procurement. Each electronic platform must pass a security audit each year to assure:

- Authentication of all users by using digital certificates.
- Digitally signed and encrypted submissions.
- Time-stamping of bids, notifications, decisions, etc. (Luis Vidigal, pers. communication).

The main signature solutions offered in Portugal are a national eID card as well as privately issues smart cards ("generic crypto token" according to the table on page 25 in Graux et al. 2009, another study authored by Siemens/time.lex). The former, called the Citizen's Card (Cartão de Cidadão), offers eSignatures. The Portuguese eProcurement Program (PNCE) was built around the following components:

- "eProcurement Pilot Projects
- eTendering Platform
- eAuction platforms and catalogues e-requisition
- Contract terms download tool
- Studies: 'Background for the adoption of dynamic negotiation in public acquisition procedures'; 'Management and sourcing in public procurement'
- National eProcurement Portal [was www.Compras.gov.pt, now Vortal https://www.vortal.biz/]
- Human Resources & Training
- National Registry of Suppliers
- Electronic Aggregation Tool
- Central Electronic Catalogue Management Tool
- eInvoicing" (Adrião 2006, p. 2)

Portugal has established a citizen's portal and an enterprise portal. The Citizen Card, the Portuguese electronic identity card (eID), is a smart card providing "visual identity authentication with increased security and electronic identity authentication using biometrics (photo and finger print) and electronic signatures" (European Commission 2009c; Portuguese Citizen Card 2008).

The Portuguese government has set up a State Electronic Certification System (SCEE), which is an infrastructure for public key management (European Commission 2012b).

The European Commission observed: "e-Procurement provisions are based on three major innovations:

- full adoption of e-Procurement for any open, restricted or negotiated procedure in awarding a public contract, avoiding traditional paperwork and increasing speed, transparency and competitiveness;

- increase of accessibility through electronic publication by an official portal ('base.gov.pt') of all notices and contract announcements;

- full specification of the multicriteria model to be adopted by the jury in selecting the most economically advantageous proposal and its presentation in the procedure documents to be known by any tenderer so that equity and equal treatment will be fully respected." (European Commission 2012b)

There are cases, however, in which the awarding procedure is finalised by a negotiation of details, finalised with the signature of paper contract that holds all the details (interview).

2.7.4 Germany

At the beginning of this century, the German parliament requested a study on eCommerce, which was conducted by the Office of Technology Assessment at the German Bundestag (TAB, related to KIT; see Riehm et al. 2002). The study contains sections on private and public eProcurement. The authors state that public eProcurement is sought by public institutions in order to reduce costs, improve transparency and reduce corruption. The authors observe that public eProcurement was in an early state. In Germany, bids for public procurement that were submitted digitally must be signed with a digital signature. The authors concluded that the discussions about procurement should be intensified and more tests conducted. The study refers to a subcontracted study performed by the consultancy company KPMG (2002). The subcontractor analysed private and public eProcurement. KPMG reports that electronic procurement as conducted by German manufacturers is profitable. About 10 years later, it appears eProcurement is still rarely used, as shown above in Table 2.1.

Germany has some main central purchasing bodies: the Federal Office of Defence Technology and Procurement, the Federal Office for Information Management and Information Technology of the Bundeswehr and the Procurement Agency of the Federal Ministry of the Interior. Germany relies on specific smart cards for its main signature solutions (Graux et al. 2009). Signatures based on national eID cards are provided by the ePA (elektronischer Personalausweis).

Germany has been implementing the EU Directives for eSignatures. Suppliers of eSignatures support the industrial signature interoperability specification Common PKI (formerly Industrial Signature Interoperability and Mailtrust Specification (ISIS-MTT)). The Common PKI Specification (T7 & TeleTrust 2009) describes a profile for standards for electronic signatures, encryption and public key infrastructures. It is officially recommended by the German Government and supported by leading German product developers. International companies including Microsoft and Entrust have obtained the so-called Common PKI compliance label, certifying conformity with the Common PKI specification.

The Common PKI specification considers most business-relevant electronic signatures up to qualified electronic signatures based on the German Signature Act SigG (Bundesrepublik Deutschland 2001a). The German Signature Act defines the general framework for so-called qualified electronic signatures that can be used in legal actions. It was first passed in 1997 and was modified in 2001 to meet the

requirements of Directive 1999/93/EC. The signature law and the ordinance on its technical realization (Signaturverordnung, SigV, Bundesrepublik Deutschland 2001b) put fairly strong security requirements on the entire public key infrastructure providing the means for the signatures, i.e. on signature devices, signature software as well as CA services (T7 & TeleTrust 2009).

The new eProcurement website (http://www.xvergabe.org) claims that the current eProcurement situation is problematic:

1. "Many solution providers
2. Different technologies
3. Incompatible bid-clients (browser- or software based)
4. No standard for the exchange of notices

Result: For bidders the access to electronic tendering is far away from the optimum." (XVergabe 2011, p.4) Currently, there is a variety of client code in place to achieve non-repudation and confidentiality, up to the bid opening. The goal of the new eProcurement website is to change this situation by making the use of a small number of clients possible.

2.7.5 Comparison of Country Studies

It is peculiar to note that the two countries which offer most functionality for the signature function of their eID also possess the more advanced eProcurement system. Germany has only recently introduced an electronic ID card and seems to have deficits in the area of eProcurement. Of course it would be rash to conclude that there is a cause-effect-relationship. However, it can be concluded that a central government push is very useful to create a frequently used system. For Europe, this means that legislation directly applicable in all member states should be discussed. It would mean that any services such as registration or PKI service, should be available for any bidder or contracting authority, perhaps with a user interface in the national languages and in English.

From interviews, indications have been obtained that some central procurement systems have a physically separate backup system, while others do not. Such a system might be costly because its parts must be physically separate while connected, but in a way that the spread of malware is hindered. Still, this is an important issue with regard to the availability of data, but also to increasing transaction costs.

Regarding transaction costs, it was not possible to identify what the costs of digital signatures are in these three countries. Other researchers have also found it difficult to identify changes in process costs (Croom, Brandon-Jones 2009, p. 456).

A coversheet used in Germany and called a Mantelbogen, a paper document to be signed, was mentioned. From interviews, it became apparent that paper contracts are also used in Portugal to finalise eProcurement transactions. This brings up the question as to how often electronic procurement is accompanied by paper documents. NATO is systematically using a system of electronic procurement in which the final contract is made on paper: "print out a paper version of the contract to be signed by hand" (Smit 2011). Given the above-mentioned estimate of costs of a paper document of about €15, using that procedure just for the case of a short or even long-run warranty and dispute clarification cannot yet be judged to be inefficient, according to the information identified. Again, no indication was found that it is not practical for the parties to exchange the bulk of documents electronically.

2.8 EU Regulation and Initiative

2.8.1 Regulation

The following European Parliament and Commission regulatory documents have been identified as being of relevance for this report:

- Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community Framework for Electronic Signatures.
- Directive 2004/17/EC … of 31 March 2004 coordinating the procurement procedures of entities operating in the water, energy, transport and postal services sectors.
- Directive 2004/18/EC … of 31 March 2004 on the coordination of procedures for the award of public works contracts, public supply contracts and public service contracts.
- Directive 2009/81/EC … of 13 July 2009 on the coordination of procedures for the award of certain works contracts, supply contracts and service contracts by contracting authorities or entities in the fields of defence and security, and amending Directives 2004/17/EC and 2004/18/EC.
- Decision 2003/511/EC of 14 July 2003 on the publication of reference numbers of generally recognised standards for electronic signature products in accordance with Directive 1999/93/EC of the European Parliament and of the Council.
- Decision 2011/130/EU of 25 February 2011 establishing minimum requirements for the cross border processing of documents signed electronically by competent authorities under Directive 2006/123/EC of the European Parliament and of the Council on services in the internal market.
- Decision 2009/767/EC setting out measures facilitating the use of procedures by electronic means through the 'points of single contact' under Directive 2006/123/EC 2009(d).

Furthermore, the following Commission documents are of particular relevance:

- Green Paper on expanding the use of e-Procurement, COM(2010) 0571, October 2010
- Proposal for a Directive on public procurement, replacing Directive 2004/18. Brussels, 20.12.2011, COM(2011) 896 final, from hereon named "Draft Directive 896".
- Proposal for a Directive on procurement by entities operating in the water, energy, transport and postal services sectors. COM(2011)895 final. Brussels, 20.12.2011.
- Proposal for a Directive on the award of concession contracts. COM(2011)897 final. Brussels, 20.12.2011
-
- Communication: A strategy for e-procurement. COM(2012) 179 final, 20.4.2012. Communication (2012d)

The Draft Directive COM(2011)896 addresses classical public procurement and will be summarised, with regard to security, below, in Section 2.8.2. Not taken into account here are COM(2011)895 and

COM(2011)897, which address the utilities sector, and whose concessions are substantially similar, according to the European Commission (2012d).

2.8.2 Activities Regarding Non-repudiation

Initiatives from Member States

The EU member states still develop national standards. In the first Internet boom, many states in the US as well as, for example, Germany developed national digital signature legislation, prior to the emergence of the electronic signature directive. One view is that this was not very helpful. A reason is that without legislation private companies could have developed solutions regarding the quality of the implementation and the liability for signatures, without falling risk of being non-compliant to a law. As Stewart Baker put it at the 1998 hearing of the signature directive: "laws create uncertainty" (similarly: Reimer, Lapp 2009).

Anyway, the Commission later tried to harmonise regulation with their directive, but this led to incompatibilities, as will be shown below. Member states continued to pursue national paths. From a neutral technology assessment perspective, it must be asked whether the European legislators really want cross border usability if they start making laws and implementations on a national basis. However, there are also efforts by the member states to make implementations compatible.

The Germany initiative *Common PKI specification* (formerly ISIS MTT) aims at creating interoperability between digital signature products (European Commission 2006). "The Common PKI (Public Key Infrastructure) specification describes a profile of standards for electronic signatures, encryption and public key infrastructures which is officially recommended by the German Government and supported by the leading German product developers and solution providers for e-Business and e-Government." (Rosenkötter et al. 2011, p. 35)

Austria was developing the Austrian Citizen Card as an electronic identity card. This concept allows also the integration of foreign signature cards, e.g. since February 2006 of Belgian, Estonian, Finnish and Italian ID cards.

The initiative *European Bridge-CA (EBCA; TeleTrust 2012)* aims at facilitating validations and other services. As Rosenkötter et al. put it: It is "operated by the German industry association TeleTrusT Deutschland e.V. [and] connects the PKI of each participating organisation... Existing certificates can be used beyond local 'identity islands', which allows business processes to span across different organisations. Subject to the conclusion of a single contract with EBCA, its members benefit [inter alia] from directory and validation services without having to set up agreements with each of the EBCA partners." (Rosenkötter et al. 2011, pp. 35)

2.8.3 EU Studies and Projects

In parallel, in a top down approach, the European Commission aims to solve interoperability problems by employing standardisation and legislation, which can make national efforts superfluous.

IDABC and CROBIES Studies

In 2009, a study on cross border interoperability of digital signatures was conducted within the framework of the IDABC programme (Interoperable Delivery of European e-Government Services to public Administrations, Businesses and Citizens; Graux et al. 2009). "At the European level, full interoperability means that an eGovernment application of a given Member State should accept any (valid) electronic signatures sent by any natural or legal person from any other Member State even if the

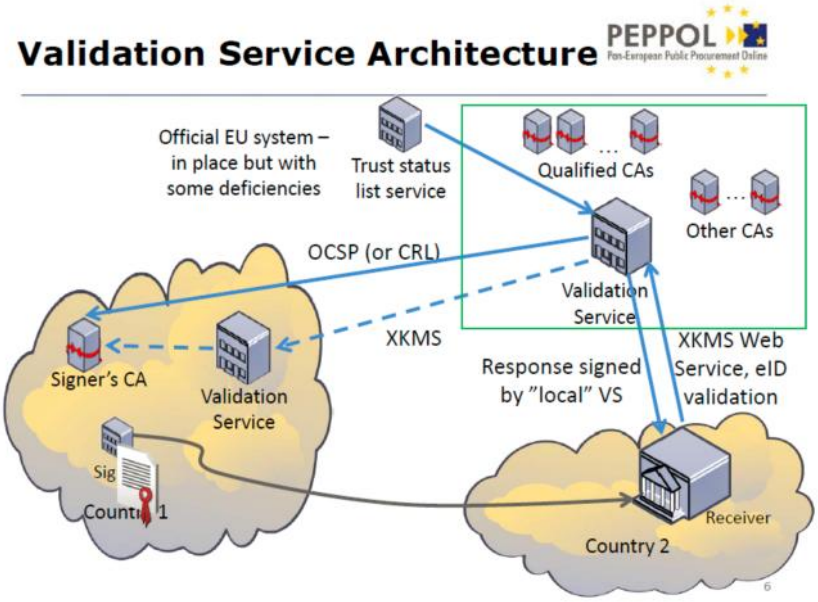
signature is created using credentials (certificates) issued by non-national Certification Service Providers (CSPs). Due to ... the technical differences between signature solutions and the difficulty of determining the trustworthiness of foreign signatures – full operability currently does not exist in Europe." (Graux et al. 2009, p. 145) The authors continue: "[M]any applications currently rely only on CSPs accredited by their own national accreditation authority. The application profiles show that they often claim to be open for cross border use on this basis, meaning that non-nationals are expected to first apply for credentials from one of the accredited CSPs. Where qualified certificates are concerned, this means that non-nationals must physically appear in the country where the application is deployed." (Graux et al. 2009, p. 146) The study identified various interoperability issues, such as that a "national perspective in choosing signature solutions" (ibid., p. 150) was taken, implementing concepts specific to a country. Technical incompatibility issues comprise formats, validation of signatures, certificates and attributes (e.g. authority to sign). It seems many of these issues could be addressed if the trans-border perspective were taken. For instance, a foreign entity could identify an individual.

The Commission has conducted various studies to analyse the situation and provide recommendations. Of note are a study on the standardisation aspects of eSignature (Sealed et al. 2007), another on electronic documents and electronic delivery (Siemens/time.lex 2009b) and the *CROBIES study* (Siemens-time.lex 2010b), which analyses the requirements and establishes a general strategy for cross border use of qualified eSignatures and advanced eSignatures based on qualified certificates. Particularly noteworthy is the *Study on a European Federated Validation Service,* which was launched to examine the existing issues of signature validation at the European level and to assess the legal, operational and technical feasibility of a European scale electronic signature verification functionality based on a federated model of national validation service providers (VSP; Siemens-time.lex 2010c). Its final report of March 2010 (Siemens-time.lex 2010d) concluded that it is virtually impossible to design comprehensive and durable validation solutions with a general EU level impact in the current environment characterised by a lack of legal regulations for VSP, by inappropriate standards and by a trust framework developed on an ad hoc basis. The study therefore proposed a comprehensive revision of the existing legal, technical and trust framework.

PEPPOL Project

Of relevance in our context is the *Pan-European Public Procurement OnLine (PEPPOL)* pilot project, which is a large-scale cross border eProcurement project. Its Working Package 1 aims at achieving European interoperability of electronic signatures. It addresses a specific cross border validation tool. One key element is to create national validation services which produce messages informing a foreign receiver whether a signature is valid, see Figure 2.3. PEPPOL pilot transactions do, however, not yet involve real purchases, according to project participants. However, it is anticipated that its results will be used in future activities. As becomes visible from the complexity of entities in Figure 2.3, the approach may lead to significant costs.

Figure 2.3, PEPPOL Validation Service Architecture. Source: PEPPOL.



IMCO Study

The IMCO study commissioned by the European Parliament, prepared by Rosenkötter et al. (2011), is summarised in this section. The authors identify some obstacles, such as unclear wordings of the Signature Directive [1999/93/EG], the unclear liabilities of CAs, the diversity of national systems, the lack of conformity assessments of SSCDs, the widely different means for identifying signers that depend on national systems, and finally the uncertain costs for archiving. All in all this leads to low use, incompatibilities and high costs (ibid., pp. 9, 25, 30).

To overcome the above-mentioned obstacles, Rosenkötter et al. provide ideas for two main strategies for eSignatures, a small-scale approach and a large-scale one, and discuss two main solutions for future eProcurement, one with signatures and one without signatures. Regarding solutions without digital signatures they see the options of:

- "Submission of an unsigned electronic file and simultaneously, via ordinary mail, a paper standard form – generated by the e-Procurement website itself and linked to the digital transmission – duly signed by the company's legal representative […].

- User-ID and password-based model, in which the user is signing [apparently this does not refer to digital signatures] an offer by uploading it to an e-Procurement website after simple online registration that did not use any PKI components […].

- Major Contracting Authorities such as the European Commission […] accept very simple solutions such as a PDF document sent via email."

They conclude: "These options seem not to pose any interoperability barriers, including cross-border." (Rosenkötter et al. 2011, p. 74) As noted above in Section 2.6 on "eSubmission", no notable security incidents have been observer with such approaches.

Regarding digital signatures, Rosenkötter et al. describe, inter alia, the use of a "signature module integrated into the website" (p. 74), referring to https://www.marchespublics.gouv.fr and https://www.e-Procurement.gov.cy/ceproc. No details about the website signature module have been provided. Also, it was not possible for us to verify, in the available literature, how signing keys are generated and used. This is mentioned here because it resembles the "provisional token" in the Draft Procurement Directive of December, 2011, discussed in Section 2.8.4.

Regarding a small-scale digital signature approach, they describe, as one option, a small-scale approach, namely to issue a nonbinding Commission document providing an interpretation of the current directive, plus a set of European norms, referenced via Commission decisions based on Art. 3.5 of the directive (Rosenkötter et al. 2011, p. 8).

Regarding a large-scale approach, they describe the option to comprehensively revise the Signature directive and to create a comprehensive and consistent framework, covering all types of electronic signatures, including Commission decisions mapping technical standards with legal requirements. "This approach which is mainly supported by the CROBIES and EFVS Studies further recommends creating a sound and stable Trust Framework through appropriate supervision and voluntary accreditation schemes, certification of products and applications and Trusted Lists for all types of certification (CSP) services." (ibid., p. 8)

2.8.4 EU Standardisation Activities

In 2009, the Commission submitted a four year Standardization Mandate M/460 to CEN and ETSI, which aims to enhance the current complex set of standards into a rationalised European electronic signature standardisation framework (European Commission 2009, Rosenkötter et al. 2011). "The main objective of the mandate is to rationalise the existing standardisation framework around the various types of TSP services, the electronic signature creation and verification, as well as the secure user devices." (Graux et al. 2010) The objective is to create a set of European Electronic Signature Standards (EESS).

In addition, the CEN Workshop on 'Business Interoperability Interfaces on public procurement in Europe' Phase 2 (WS/BII 2) was set up to provide a basic framework for technical interoperability in pan-European electronic transactions. This framework was expressed as a set of technical specifications that refer to the relevant activities and in particular are compatible with UN/CEFACT - in order to ensure global interoperability. The workshop is focused on facilitating implementation and on coordinating pilot implementations of the technical specifications. The requirements and final specifications are to be input into UN/CEFACT (European Commission 2010a, 2011b).

2.8.5 Proposal for a Signature Regulation

The European Commission has published a proposal for an eSignature regulation "on electronic identification and trusted services for electronic transactions in the internal market" (European Commission 2012f). It is meant to replace the signature directive (ibid, p. 18). Some clauses are of particular relevance for eProcurement:

- The proposal would allow for various ways to store a secret signing key. One way comes down to storing it in an encrypted manner on an ordinary storage medium (advanced signature), another would involve the use of a smart card or HSM (Annex II), and finally it seems there is also the option to store it outside the user's immediate sphere of control on some server (Annex II), e.g. to be accessed with a mobile phone (European Commission 2012g). The server operator

would even be allowed to store backups of the secret key (Annex II; usually the advice would be not to have a copy of a secret signing key, but to generate a new key pair if it gets lost).

- The regulation does not anticipate any improvement in qualified signature procedures (§ 20), such as readers with secure user input and output.

- Member states may opt to have their national ID cards used as signing devices, or not (European Commission 2012g).

- Qualified signatures are given legal value ("legal presumption"), while others are admissible at court, too, taking into account their "assurance level" (§ 34).

- The validity of a signature needs to be established at the time of signing (§ 25), which appears to solve the issue of Annex IV of the current directive, mentioned above in Section 2.3.

The variety of means implies various means to attack keys or signing environments and may introduce some uncertainty as to what the value of the means will be in a dispute. The regulation addresses, of course, more issues, in more detail.

2.8.6 Conclusions at EU Level

Cases of the cross border use of digital signatures are very rare, if they exist at all. Studies of such cases also seem to be non-existent. The costs of relevant security implementations, which only can be determined by practical use, are also unknown. It still has to be proven if the amount of effort being put into security implementation is worth the possible cost of any attacks. A paper signature reportedly costs only 12.5 Brit. Pounds, about €15 (Posch 2011, referring to British estimates). As mentioned, there are costs for software, cards and card readers (if used), time-stamping close to the moment the signature is made, re-signing for archival reasons, storage of the necessary information on the relying party side, learning, etc. – in an environment in which only few such transactions are performed per party per year (though this is hoped to change for transactions below thresholds).

Furthermore, the suitability of digital signatures in disputes and court cases is not reflected in the studies we reviewed. Interviews indicated that there have been some cases of digital signatures used at court, but no documents have been found about this, nor is it clear whether their evidential value was scrutinised. Simulation of different use cases for future scenarios would be a way to learn more about what is needed, possibly with participation of judges.

Another potential issue is the following. Assume digital signatures are to be used for dispute clarification. Currently, there is some emphasis put on authenticating submissions. This makes sense from the point of view of the contracting authority, which wants competition and a legally binding bid. Similar emphasis on authenticating the earlier tendering documents is not visible. It can be assumed that in a dispute, one will want to have all documents authenticated.

2.8.7 Other Activities

The European Commission has adopted a number of related initiatives, such as working papers (European Commission 2004), studies (European Commission 2011c), and action plans (European Commission 2008) and the Digital Agenda for Europe (European Commission 2010b). Regarding authentication, it is worth mentioning the STORK pilot project: *Secure idenTity acrOss boRders linKed.* It has the objective to enable cross -border recognition of eID systems and easy access to public services in 18 European countries to demonstrate solutions for the cross border use of eID. The role of the STORK

platform is to identify a user who is in a session with a service provider, and to send his data to this service. The aim of the STORK project is to establish a European eID interoperability platform that will allow citizens and businesses to establish new e-relations across borders, just by presenting their national eID with minimal disclosure of data (European Commission 2010a, 2011b).[1]

In our context, two more activities need to be briefly mentioned.

2.8.8 eCertificates

The information system *eCertis* helps to identify the different certificates and attestations in procurement procedures across the 27 member states. eCERTIS is a free, online information tool which provides details of the different certificates and attestations frequently requested in procurement procedures. It represents a response to the problems encountered by economic operators and contracting authorities when submitting and receiving evidence documents within a cross border procurement process (European Commission 2010a, 2011b).

2.8.9 Procurement Software

The eProcurement platform *ePRIOR* is a pilot eProcurement platform for public authorities and includes a cross border aspect. ePRIOR has to produce business requirements for eProcurement systems in a public procurement context and cross border environment. A pilot was set up to be used by the Directorate General Information Technology (DIGIT) and some of its suppliers (European Commission 2010a, 2011b). In addition to ePRIOR, there is an open source version called Open ePrior whose goal is to accelerate the implementation of eProcurement.

2.8.10 Proposal for a New Procurement Directive

As mentioned above, the Commission has published a number of proposals for new procurement directives, namely COM(2011)895, COM(2011)896 and COM(2011)897. COM(2011)896 addresses classical public procurement and will be taken into account here with regard to security. COM(2011)895 and COM(2011)897 address the utilities sector and concessions are substantially similar, according to the European Commission (2012d); it is not addressed here.

The Commission strategy becomes visible from a press release of April 20, 2012 (European Commission 2012e), see Box 2.1.

In this section, some key elements of "896" are presented, based on quotations, together with a simplified interpretation as to what they mean regarding security, and comments.

[1] Two more projects are SPOCS (Simple Procedures Online for Cross-border Services) and eTEN (http://www.epractice.eu/cases/eTENPROCURE).

Box 2.1: Sections from the European Commission Press Release of April 20, 2012

Delivering savings for Europe: moving to full eProcurement for all public purchases by 2016

… Increasing the use of eProcurement in Europe can generate significant savings for European taxpayers. Public entities that have already implemented eProcurement report savings of between 5% and 20% of their procurement expenditure… eProcurement can significantly simplify the life of companies, especially SMEs, by increasing the transparency of and access to tender opportunities and by reducing the costs of participating in a tender (reduced mail costs, less printing, etc.)….

In the context of the modernisation of the European Public procurement Directives, adopted in December 2011, the Commission has proposed to make eProcurement the rule rather than the exception, by making it the standard method of procurement in the EU by mid-2016….

Today's Communication ["179", 2012d] sets out a strategy to achieve this ambitious transition. It proposes a series of flanking measures meant to support all stakeholders, including SMEs, in completing the transition on time…. The Communication also announces that the European Commission itself will move towards full eProcurement by mid-2015 – a full year ahead of the deadline for Member States – and that the Commission will make its eProcurement solutions available to Member States.

Articles 19(7), 92(1), 35(4)

19(7): "Member States shall ensure that, at the latest 2 years after the date provided for in Article 92(1), all procurement procedures under this Directive are performed using electronic means of communication, in particular e-submission..." (except for unusual file formats)

92(1): Member states to comply by 30 June 2014.

35(4): "All procurement procedures conducted by a central purchasing body shall be performed using electronic means of communication".

Interpretation of key meaning

eSubmission above thresholds will become mandatory (from 2016 on if transposed quickly). Central purchasing bodies have to use electronic means.

Comment

Authorities are no longer allowed to request bids using paper and have to bear the costs of other means. As there currently are not enough trans-border interoperable solutions for achieving non-repudiation and confidentiality, the German industry has suggested that first such solutions should be developed and tested, before eProcurement can be made mandatory (BDI 2012).

Article 19(3)

"To ensure the interoperability of technical formats as well as of process and messaging standards, especially in a cross border context, the Commission shall be empowered to adopt delegated acts … to establish the mandatory use of specific technical standards, at least with regard to the use of e-submission, electronic catalogues and means for electronic authentication."

Interpretation of key meaning

The Commission can impose standards for formats and authentication of submissions.

Comment

Contracting authorities will lose control of what technologies they use, which is of relevance regarding the risks as well as regarding the costs of the procedure. Competition between different tools could be reduced. Given the Commission's activities regarding the regulation of digital signatures, it must be anticipated that a possible outcome is that digital signatures will be made mandatory.

The draft directive does not clearly argue in favour or against digital signatures. As became visible in the literature review above, some players find passwords or PDFs sufficient. According to the study by Siemens and time.lex (2010a), the economic viability of electronic procurement using digital signatures is unclear, not only because of the costs, but also because of the lack of data (ibid., p. 344). This means that an empirical clarification would make sense, e.g. of South Korea. Also, the legislator might decide that the Commission is not authorised to make signatures mandatory. This holds also with regard to means of encryption to be used.

A possible option is to make mandatory use of standards subject to parliament approval.

Article 19(5)

"The following rules shall apply to devices for the electronic transmission and receipt of tenders and for the electronic receipt of requests to participate…

b) devices, methods for authentication and electronic signatures shall comply with the requirements of Annex IV;

c) contracting authorities shall specify the level of security required…;

d) where advanced Electronic Signatures … are required, contracting authorities shall… accept signatures supported by a qualified electronic certificate referred to in the Trusted List provided for in the Commission Decision 2009/767/EC, created with or without a secure signature creation device, subject to compliance with the following conditions:

- they must establish the required advanced signature format on the basis of formats established in Commission Decision 2011/130/EU and put in place necessary measures to be able to process these formats technically;

- where a tender is signed with the support of a qualified certificate that is included in the Trusted list, they must not apply additional requirements that may hinder the use of those signatures by tenderers."

Interpretation of key meaning

If authorities request advanced signatures (a minimum required to replace a handwritten signature), they must accept signatures with qualified certificates as long as the certification authority is on the Trusted List. Methods of authentication need to comply with Annex IV (see below).

Comment

Authorities must accept advanced signatures even if they deem them to be not secure enough, e.g. regarding the signing environment used; no upgrade path is visible, unless perhaps indirectly, via editing the Trusted List. Annex IV (below) does not appear to specify methods of authentication. It

seems that clause (h) in Annex IV is an error in editing, as requirements for authentication are spelt out in Article 19 (Council of the European Union 2012).

Article 19(4)

"Contracting authorities may … require the use of tools which are not generally available, provided that they offer alternative means of access… They … ensure that tenderers established in other Member States than the contracting authority's may access the procurement procedure through the use of provisional tokens made available online at no extra cost."

Interpretation of key meaning

Member States have to provide a provisional token if they require tools which are not generally available.

Comment

It appears that it has not been defined what a provisional token is. Non-repudiation with digital signatures is usually achieved by binding a public key to a secret key in possession of the user, and to a secure identification procedure of the signer. It is difficult to imagine how non-repudiation can be achieved without secure storage of keys on the signer's part and without prior identification. If, however, the signer registered properly and is in possession of a secret key, certified via the public key, the characterisation as "provisional" would not be needed.

Article 84

"Member States shall appoint … [an] oversight body … Contracting authorities shall transmit to the national oversight body the full text of all concluded contracts" with a value above €1 mio (€10 mio. in case of works contracts).

Interpretation of key meaning

An oversight body has to obtain all contracts > €1 million/€10 million.

Comment

This poses a potential privacy issue. Contracting authorities can no longer keep valuable content of contracts confidential. Suppliers may dislike the fact that their IPR will be lodged with a central authority (see also BDI 2012).

Annex IV

"Devices for the electronic receipt of tenders, requests for participation and plans and projects in contests must at least guarantee, through technical means and appropriate procedures, that

(a) the exact time and date of the receipt of tenders, requests to participate and the submission of plans and projects can be determined precisely;

(b) it may be reasonably ensured that, before the time limits laid down, no-one can have access to data transmitted under these requirements;

(c) where that access prohibition is infringed, it may be reasonably ensured that the infringement is clearly detectable;

(d) only authorised persons may set or change the dates for opening data received;

(e) during the different stages of the procurement procedure or of the contest access to all data submitted, or to part thereof, must be possible only through simultaneous action by authorised persons…

(h) authentication of tenders must conform to the requirements set out in this Annex."

Interpretation of key meaning

Systems have to guarantee that nobody has access to data prior to opening, and that the exact time of receipt of tenders is recorded.

Authentication of tenders must conform to the requirements set out in this Annex.

Comment

The need to use a secure time stamp may have an impact on small authorities or on their operating costs, and may create incentives for them to rely on central systems. The need for an exact time might be reduced if the content of a submission has to be encrypted until the opening. Receipts might be given upon submission of a tender.

The requirements for authentication of tenders (clause h) are not visible in Annex IV, which seems to be an error in editing.

Additional comments

- The European Commission Communication (2012d) mentions that "openness of e-procurement systems to bidders from all jurisdictions, especially among WTO GPA members, must be ensured." No detailed plan has been identified, and given the problems of making digital signatures work across borders, this is a challenge, unless one uses password-based systems. The issue could be discussed at the planned project workshop.

- The Commission presented an impact assessment (2011g), which, however, does not so much assess the impact of each article and make an estimate of its costs and benefits, but rather is a justification of the strategy behind the draft.

- It might be useful to openly discuss the pros and cons of the various suggestions. The conference on electronic procurement of June 2012 certainly was a useful step (http://ec.europa.eu/internal_market/publicprocurement/e-procurement/conferences/index_en.htm). It would, however, be good to take the views of small and large bidders and contracting authorities into account at a larger scale. In particular, the views of public procurers who do not seem to want eProcurement should be taken into account; some 50 percent dislike making eProcurement mandatory, according to a survey conducted in the framework of the Green Paper (Ferger 2011).

In sum, the above comments and considerations provide a larger number of topics which, to be on the safe side, might justify additional analysis, be reviewed during the legislative process, and discussed at the planned project workshop.

2.9 Conclusions

Reviewing the findings of this chapter, the main conclusions can be grouped as follows.

2.9.1 General Conclusions

This chapter has provided a review of the security issues in public eProcurement mentioned in the literature. It has also provided a review of emerging EU procurement legislation. Based on this, a number of options for actions that the European Parliament could take are spelt out. These options should be evaluated at the planned project workshop and in additional research, taking in particular the views of the contracting parties into account.

The procurement landscape is very fragmented

Many eProcurement initiatives work at a national scale, sometimes even regional. There is scepticism towards the concept of mandatory eProcurement, even on the part of the contracting authority. Otherwise 50% of them would not reject the concept, according to a Commission survey. Obstacles can be assumed to be the advantages of in-person contacts, paper documents, and process control on the one hand, and the complexity of electronic processes on the other hand. Language problems could be among the most severe ones hindering cross border delivery. PEPPOL spent much effort on making cross-country systems interoperate. It might indeed be more economic if services were available across borders. Conclusions would be that (1) a procurement server should have an interface in several languages or at least one in English, (2) a PKI-based authentication or signature service, if one agrees to use one, should be available throughout the EU with local registration, e.g. via traditional mail, (3) encryption tools should be applicable across borders, and (4) the requirements for company certificates and statements should be identical in all countries.

Options:

- Investigate in greater detail the reasons for the reluctance of public procurers to have more electronic and more trans-border procurement.

- Have more direct, EU-wide regulation, e.g. regarding procurement and authentication, to enable cross border authentication, non-repudiation and encryption. Consider using security means used for procurement only, in order to make fast progress, independent of ID and signatures cards.

Central procurement systems increase vulnerabilities

Central procurement servers might become attractive targets of attacks. Outsiders or insiders could figure out prices ahead of the end of a bidding process and the content of procurement documents could leak, which would have a major impact on military procurement, for example. Also, the costs of central solutions might increase over time if a monopolistic situation emerges. For eProcurement, the use of central servers is increasing, as opposed to each contracting authority conducting their own, local tender. However, there are hundreds of servers in use, which reduces vulnerabilities, see Section 2.6 above. Attacks might address the server or the clients.

- While central procurement systems can currently be regarded as an option, there is a possibility that their use might become mandatory and that they might need to be used for purchases below the thresholds. An alternative would be to empower local contracting authorities to keep the whole process in their hands. Also, central systems might need physically separate backup

centres, with good isolation of any malware, while a local loss would lead to less damage. Also, more players would be harmed if a denial of service attack takes place on a central system. Local solutions would mean not to have such single points of failure. Options are:

- To support the development and deployment of suitable software for local use by authorities (see ePrior, mentioned above), in order to make eProcurement cheap and robust. However, bidders will wish to inform themselves about new bids easily, and will wish to prepare bids in a similar way, so the issue of interoperability standards with signatures and encryption emerges.

- To use encryption to make it impossible for everyone, even insiders, to read confidential information, such as prices, ahead of the bid opening.

- To hide confidential information after bid-opening, by using tamper-resistant storage and processing, such that only the buyer and the seller see the documents in the clear.

- In particular for local systems: If bids are encrypted by the sender for later decryption by the contracting authority, it could be considered that the contracting authority does not need to provide receipts with precise time. A bidder who does not receive a receipt in time could complain (automatically); one could have a certain delay between the end of the bidding time and the decryption of bids, to buffer small discrepancies in time.

- In particular for central systems: Measures may need to be taken such that robust, malware-protected backup systems are used.

Computers can be attacked

From a security point of view, computing is on thin ice. Commonly used hardware, software as well as cryptographic algorithms share the fact that their security properties are not proven. As algorithms do not appear to be an immediate problem (the only major issue is that decryption might be possible after perhaps a decade or more), hardware and software remain a problem. One important objective would be the reduction of attacks based on unpublished weaknesses. Another issue is the reduction of the effects of malware in general. Increased use of unhackable compartmentalization, without hidden functionality, could help reduce both. Compartmentalisation could be used to separate procurement systems from other systems (e.g. browsing the Internet, reading of untrusted USB-sticks) and provide a secure compartment for any kind of authentication. This leads to the following option:

- The European Union could encourage the emergence of better general purpose hard- and software by means such as making the use of renowned, possibly certified products with certain characteristics mandatory, e.g. when procuring IT-equipment.

Encrypting bids requires that decryption is only possible after opening

Encrytion is used to encrypt bids so that competitors or insiders with the buyer cannot read a bid ahead of the bidding deadline. Such processes require careful setup:

- It must be ascertained that insiders cannot decrypt bids, even when colluding. However, they may need to be able to decrypt bids at the opening. This poses procedural challenges.
- It might be safe that the bidders supply decryption keys once the bidding deadline is over. However, this requires some additional work on the bidders' side.
- In any case, encryption solutions should be available across borders.

No evidence of the economic efficiency of signing procurement documents digitally was found

It has not been possible to find evidence of the costs of using digital signatures in procurement. Alternatives are to use password-based systems, PDF documents, or paper contracts. It appears that there are no doubts that, in general, the electronic exchange of documents is economic. However, for legally binding documents, such as bids or contracts, there seems to be no evidence that digital signatures are cheaper than paper. One reason is that it was not possible to find figures on the total costs of digital signatures. A second reason is that there is a possibility that with time-stamping, validation services, and resigning these might increase. Alternatives to using legally binding digital signatures would be to use password-based systems or weaker digital signatures, in particular in combination with producing a paper contract. Not using digital signatures could also ease bidding from non-EU countries. A different issue is how to design digital signatures such that they have enough evidential value to be used at court. Options are:

- To conduct additional studies on the total cost of using digital signatures, e.g. investigate South Korea, Portugal or other signature-using countries, and make projections of costs for procedures as with PEPPOL or the proposed signature regulation.
- To allow the contracting authorities to request whatever authentication they find useful. In particular if they sign paper contracts, weaker means of authentication would suffice. This might need to be considered regarding the approval of Draft Directive 896, which would empower the Commission to impose means.
- To create a world-wide repository of digital signatures used in disputes, and the steps used for creating evidence, to clarify their value in a systematic way.

Advanced signatures may get attacked

If advanced signatures are used, players might express additional requirements. Hacks might occur, either because criminals find usage attractive enough to develop tools, or because somebody demonstrates the weakness of systems, possibly regarding another kind of application, i.e. one that is not procurement-related. Usage might decrease if hacks of signing environments get publicized. Candidates for such requirements are messages concerning the validity of equipment and statements, as well as about more secure user input and output than currently available, with, e.g. means for comparing the documents on the PC and on the card readers, as described above. This might warrant explicit consideration in Draft Directive 896. It also applies to the draft signature regulation, § 20, also mentioned above.

The provisional token solution is unclear

This would require a change to the Draft Directive.

Certification authorities sometimes do not report successful attacks

Certification authorities are needed for key management in common public key-using systems (used for confidentiality or non-repudiation). It does not seem to be acceptable if they do not report systems hacks or do not take actions on such intrusions. Options:

- Closer auditing of privately run CAs.
- Comprehensive government control of CAs.
- Using other methods than CAs cannot be ruled out, but this is not a topic of this report.

Players may need to prepare for a long denial of service-attack

Contracting authorities and CPBs should be prepared for a denial of service attack, lasting as much as several days. Options:

- Prepare for means to fight denial of service attacks, in particular prepare for alternative ways of submission or for a prolongation of deadlines.

Annex IV of Draft Directive 896 is unclear with regard to authentication

Requirements for authentication, while announced under clause (h), are not spelt out here, so (h) can be deleted.

2.10 Summary

With some exceptions, eProcurement in Europe is conducted rarely. Making online submissions possible, allowing for trans-border procurement, and abolishing paper documents could reduce the costs of procurement. However, there are obstacles to eProcurement. First, there is the issue of a lack of interoperability that might arise if any special tools are used, such as PKI-based authentication, digital signatures, encryption, company eCertificates, or server-specific documents and clients. This hinders in particular cross border procurement. Second, there are a number of security threats, such as distributed denial of service attacks, which might hinder the proper termination of bidding procedures. Other malware could address systems processing confidential information such as the price or the contents of bids, whether these are on PCs or servers. Finally, hacks on the certification authorities have been seen which make it possible to use faked entities, so that an adversary can collect confidential information.

To improve the security of eProcurement systems, secure compartmentalisation could be used to separate procurement systems from others and, if in widespread use, to reduce the effect of malware in general. Secure computers would also allow having a secure environment for signing digitally.

In Europe, it is hard to determine whether eSubmission is used in practice, as there are cases with electronic submission and paper contracts, as well as use of PDFs. In general, eSubmissions seem to be rare; however, there are exceptions such as Portugal, which have made eSubmission mandatory. Cross border interoperability is hardly achieved. In one survey, 50% of public procurers expressed that they are against mandatory electronic procurement.

There are countries such as South Korea and Portugal that are using digital signatures and in which there is a high share of eProcurement. However, it was not possible to learn what the transactions costs of these signature-based procurements are. There are other countries such as Germany which use eProcurement far less. It has become obvious that a central government push can achieve a widespread adoption of eProcurement. For Europe, this would mean investigating how bidders and contracting authorities can freely register and participate from any country, using tools ubiquitously available. The use of certain tools for European eProcurement only might even be given consideration in order to achieve rapid progress in that field.

Regarding non-repudiation, on a European level various studies have been commissioned to clarify the problems afflicting the cross border use of digital signatures. Also, pilot projects have been conducted on issues such as a signature validation service. Furthermore, standardisation activities are supported, in particular a CEN-workshop, also aiming at compatibility with UN/CEFACT. However, it was not possible to clarify whether the benefits of digital signatures would justify their costs.

Several types of consequences are discussed. (1) Use unsigned files in combination with signatures on paper, which does not pose interoperability problems. (2) Use simple procedures, such as log-in via passwords. (3) Use well-standardised digital signatures.

Other important European activities are the production of procurement software (ePrior) and the establishment of the eCertis system of company certificates.

The new draft procurement directive would empower the Commission to establish mandatory use of technical means. It does not appear to be clear whether an upgrade path for digital signature environments would be hindered by this clause. The role of provisional online tokens would require some explanation ahead of any analysis. An in-depth public discussion with bidders and contracting authorities of the pros and cons of the various articles would be of help.

The conclusions drawn throughout this report can be summarised as follows:

1. The interest of European contracting authorities in conducting cross border, fully electronic procurements does not appear to be sufficiently proven in the studies identified, so the obstacles could be explored in more depth.

2. Country-specific regulations and requirements could be reduced.

3. Procurement systems run by local contracting authorities should not be discouraged by putting too much emphasis on central systems. Having a large number of local systems will provide more robustness against attacks from the Internet such as crafted attacks via Trojan horses on data such as prices, as well as against distributed denial of service attacks. However, bidders will wish to inform themselves about new bids and participate easily, so the issue of interoperability of any signing and encryption tool emerges.

4. Unhackable compartmentalisation of computers would help fight malware, and would provide a secure environment for any kind of authentication and encryption, including any client code. Therefore moves towards such compartmentalisation could be supported by the European governments.

5. Tools for authentication and encryption should be available at a European scale, not only in a single country, with suitable registration procedures, i.e. a European trust framework. Encryption must make sure that bids remain encrypted until the submission deadline, even if insiders collude.

6. The economic case for digital signatures needs to be clarified, e.g. by collecting data in countries with long experience (including costs for validation, time-stamping or re-signing), by interviewing experts and by performing projections. European legislation should remain open for various means of authentication until the case of digital signatures is better proven. Weak forms of authentication could be used if the parties intend to sign a paper contract anyway.

7. Certification authorities may need to be controlled more tightly, if not even government-run.

All of these issues could be discussed at the planned project workshop and be investigated in more detail. In such processes, emphasis should be put on taking the views of small and large bidders and contracting authorities into account, from European countries as well as from countries with long-lasting experience with eProcurement.

2.11 References

- Adrião, Renato: Best Practice Long Description: Portuguese Public e-Procurement Program. Tampere 2006. Available at http://www.4qconference.org/liitetiedostot/bp_long_descriptions/PortugalB_long.pdf

- Arbaugh, W., Farber, D., and Smith J. "A Secure and Reliable Bootstrap Architecture," Proceedings of the 1997 IEEE Symposium on Security and Privacy: 65-71.

- Austrian Citizen Card (website): www.buergerkarte.at/index_en.html

- Bae, K. Y.: PKI, Digital Signature and e-Government, 2011, available at http://unpan1.un.org/intradoc/groups/public/documents/ungc/unpan046553.pdf

- BDI: Stellungnahme des BDI zu den Vorschlägen der Kommission zur Neufassung der EU-Vergaberichtlinien. May 31, 2012.

- BSI: Register aktueller Cyber-Gefährdungen und –Angriffsformen, Analysen zu Cyber-Sicherheit, 2012, https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Gefaerdungslage/Register/cs_Register_node.html

- Bundesnetzagentur: Aktuelles und Hinweise. 27.4.2010. Access 20.1.2011. http://www.bundesnetzagentur.de/cln_1932/sid_549EABA42E20859F39864A802651F979/DE/Sachgebiete/QES/Aktuelles%20und%20Hinweise/Aktuelles_und_Hinweise_node.html.

- Bundesrepublik Deutschland: Law Governing Framework Conditions for Electronic Signatures and Amending Other Regulations (Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften), Bundesgesetzblatt Nr. 22, 2001, S.876, non-official version available at http://www.bundesnetzagentur.de/media/archive/3612.pdf (2001a)
- Bundesrepublik Deutschland: Ordinance on Digital Signatures (Verordnung zur digitalen Signatur – SigV), 2001, non-official version available at http://www.bundesnetzagentur.de/media/archive/3613.pdf (2001b)

- Capgemini, Rand Europe, IDC, Sogeti and DTI: Smarter, Faster Better e-Government. 8th Benchmark Measurement, November 2009. http://ec.europa.eu/information_society/eeurope/i2010/docs/benchmarking/egov_benchmark_2009.pdf

- Capgemini, IDC, Rand Europe, Sogeti and DTi: Digitizing Public Services in Europe: Putting ambition into action 9th Benchmark Measurement, December 2010, i2010.

- http://www.epractice.eu/files/Digitizing%20Public%20Services%20in%20Europe%20Putting%20ambition%20into%20action%20-%209th%20Benchmark%20Measurement%20-%20December%202010.pdf

- Cattaneo, Gabriella: The e-procurement landscape in the EU 2012. Presentation given at: Electronic Procurement – Challenges and Opportunities. 26 June 2012, Brussels.

- CEN Workshop on 'Business Interoperability Interfaces on public procurement in Europe' Phase 2 (WS/BII 2) http://www.cen.eu/CEN/Sectors/Sectors/ISSS/Activity/Pages/Ws_BII.aspx

- Chaum, D., Damgård, I. and van de Graaf, J.: Multiparty computations ensuring privacy of each party's input and correctness of the result. In Advances in Cryptology - CRYPTO '87, LNCS 293.

- Cimander, R.; Hansen, M.; Kubicek, H.: Electronic Signatures as Obstacle for Cross-Border E—Procurement in Europe, 2009. http://www.epractice.eu/en/library/292080

- Council of the European Union. Note. 21 February 2012. Interinstitutional File 2011/0438 (COD). http://www.parlament.gv.at/PAKT/EU/XXIV/EU/07/33/EU_73332/imfname_10019377.pdf

- Croom, Simon; Brandon-Jones, Alistair: Key Issues in E-Procurement: Procurement Implementation and Operation in the Public Sector. In: Thai 2009, 446-458

- Cypriot e-Procurement platform (website): https://www.e-Procurement.gov.cy/ceproc

- Dalton, C. "A Hypervisor Against Ferrying Away Data," Interview by Furger, F. and Weber, A. OpenTC Newsletter, April 2009. http://www.itas.fzk.de/deu/lit/2009/webe09b.htm.

- Deckers, Alain: Comment made at: Electronic Procurement – Challenges and Opportunities. 26 June 2012, Brussels.

- DIGIDOC (website): http://digidoc.sk.ee/entry_splash.html

- Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community Framework for Electronic Signatures. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31999L0093:en:HTML
- Directive 2004/17/EC of the European Parliament and of the Council of 31 March 2004 coordinating the procurement procedures of entities operating in the water, energy, transport and postal services sectors, available at: http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004L0017:en:NOT

- Directive 2004/18/EC of the European Parliament and of the Council of 31 March 2004 on the coordination of procedures for the award of public works contracts, public supply contracts and public service contracts, available at: http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004L0018:en:NOT

- Directive 2009/81/EC of the European Parliament and of the Council of 13 July 2009 on the coordination of procedures for the award of certain works contracts, supply contracts and service contracts by contracting authorities or entities in the fields of defence and security, and amending Directives 2004/17/EC and 2004/18/EC, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:216:0076:0136:en:PDF

- eCertis (website): http://ec.europa.eu/markt/ecertis/login.do

- EESSI (website): http://ec.europa.eu/employment_social/social-security-directory/welcome.seam?langId=en

- England, P. "Practical Techniques for Operating System Attestation". Presentation given at: Trusted Computing - Challenges and Applications, First International Conference on Trusted Computing and Trust in Information Technologies, Trust 2008, Villach, Austria, March 11-12, 2008.

- ePRIOR (website): www.epractice.eu/cases/ePRIOR

- eTen (website): www.eten-procure.com

- eTendering and e-Procurement platform | Vortal, https://www.vortal.biz/

- European Commission: Decision 2003/511/EC of 14 July 2003 on the publication of reference numbers of generally recognised standards for electronic signature products in accordance with Directive 1999/93/EC of the European Parliament and of the Council, Available at: http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2003:175:0045:0046:EN:PDF

- European Commission: Commission staff working paper – Legal barriers in e-business: The results of an open consultation of enterprises, SEC (2004) 498, 26/04/2004. Available at: http://ec.europa.eu/enterprise/sectors/ict/files/legal_barriers_sec_2004_498_en.pdf

- European Commission: Report on the operation of Directive 1999/93/EC on a Community framework for electronic signatures, report from the Commission to the European Parliament and the Council, COM (2006) 120 final, 15/03/2006, Available at: http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0120:FIN:EN:PDF

- European Commission: Business Life Cycle. 2007 http://www.epractice.eu/files/documents/cases/1720-1181344346.pdf

- European Commission: Action Plan on e-signatures and e-identification to facilitate the provision of cross-border public services in the Single Market, Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions, 28/11/2008, COM(2008) 798 final, Available at: http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2008:0798:FIN:EN:PDF

- European Commission: eGovernment in Portugal, September 2009, Version 12.0, eupractice.eu. http://www.epractice.eu/files/eGovernment%20in%20PT-Sept%2012.0_.pdf (2009a)

- European Commission: Standardisation mandate to the European Standardisation Organisations CEN, CENELEC AND ETSI in the field of information and communication technologies applied to electronic signatures, M/460 EN, 22/12/2009, Available at: http://www.etsi.org/WebSite/document/aboutETSI/EC_Mandates/m460.pdf (2009b)

- European Commission: New Pombal Municipality portal integrates eAuthentication via the Citizen Card. 2009. http://www.epractice.eu/en/news/293175 (2009c)

- European Commission: COMMISSION DECISION of 16 October 2009 setting out measures facilitating the use of procedures by electronic means through the 'points of single contact' under Directive 2006/123/EC of the European Parliament and of the Council on services in the internal market. Corrected version available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:299:0018:0054:EN:PDF. (2009d)

- European Commission: The e-Procurement Map Third Edition, A map of activities having an impact on the development of European interoperable e-Procurement solutions, June 2010. http://www.epractice.eu/en/library/322148 (2010a)

- European Commission: Information Society, 2010, A Digital Agenda for Europe, Available at: http://ec.europa.eu/information_society/digital-agenda/index_en.htm (2010b)

- European Commission: Green Paper on expanding the use of e-Procurement, COM(2010) 0571 final, October 2010, Available at: http://europa.eu/documentation/official-docs/green-papers/index_en.htm (2010c)

- European Commission: Evaluation of the 2004 Action Plan. 18.10.2010. SEC(2010) 1214 final. http://ec.europa.eu/internal_market/consultations/docs/2010/e-procurement/evaluation-report_en.pdf (2010d)

- European Commission: The European e-Government Action Plan 2011-2015. Brussels 15 December 2010. http://ec.europa.eu/information_society/activities/e-Government/action_plan_2011_2015/index_en.htm. (2010e)

- European Commission: Summary of the responses to the Green Paper on expanding the use of e-procurement in the EU. http://ec.europa.eu/internal_market/consultations/2010/e-procurement_en.htm (2010f)

- European Commission: Decision 2011/130/EU: COMMISSION DECISION of 25 February 2011 establishing minimum requirements for the cross-border processing of documents signed electronically by competent authorities under Directive 2006/123/EC of the European Parliament and of the Council on services in the internal market (notified under document C(2011) 1081) (2011a)

- European Commission: The e-Procurement Map, A map of activities having an impact on the development of European interoperable e-Procurement solutions, August 2011, available at http://www.epractice.eu/files/The%20e-Procurement%20Map%20-%20Fifth%20Edition%20-%20A%20map%20of%20activities%20having%20an%20impact%20on%20the%20development%20of%20European%20interoperable%20e-Procurement%20solutions.pdf (2011b)

- European Commission: Europe's Information Society Thematic Portal, Main undertakings under the Action Plan. 2011. Available at: http://ec.europa.eu/information_society/policy/esignature/action_plan/undertakings/index_en.htm (2011c)

- European Commission: Proposal for a Directive on public procurement, replacing Directive 2004/18. Brussels, 20.12.2011, COM(2011) 896 final. http://ec.europa.eu/internal_market/publicprocurement/modernising_rules/reform_proposals_en.htm (2011d)

- European Commission: Proposal for a Directive on procurement by entities operating in the water, energy, transport and postal services sectors. COM(2011)895 final. Brussels, 20.12.2011. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0895:FIN:EN:PDF (2011e)

- European Commission: Proposal for a Directive on the award of concession contracts. COM(2011)897 final. Brussels, 20.12.2011. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0897:FIN:EN:PDF (2011f)

- European Commission: IMPACT ASSESSMENT. Accompanying the document "Proposal for a Directive of the European Parliament and of the Council on Public Procurement". SEC(2011) 1585 final of 20.12.2011. http://ec.europa.eu/internal_market/publicprocurement/docs/modernising_rules/SEC2011_1585_en.pdf (2011g)

- European Commission: Current rules, thresholds and guidelines. Access 12 May 2012. http://ec.europa.eu/internal_market/publicprocurement/rules/current/index_en.htm (2012a)

- European Commission: e-Government Factsheet - Portugal - National Infrastructure. 2012. http://www.epractice.eu/en/document/288346 (2012b)

- European Commission: eInclusion Factsheet - Portugal – Areas. 2012. http://epractice.eu/en/document/5255950 (2012c)

- European Commission: A strategy for e-procurement. COM(2012) 179 final, 20.4.2012. Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions. http://ec.europa.eu/internal_market/publicprocurement/docs/e-Procurement/strategy/COM_2012_en.pdf (2012d)

- European Commission: Delivering savings for Europe: moving to full e-procurement for all public purchases by 2016. Press release of April 20, 2012. http://europa.eu/rapid/pressReleasesAction.do?reference=IP/12/389&format=HTML&aged=0&language=en&guiLanguage=en (2012e)

- European Commission: Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on electronic identification and trust services for electronic transactions in the internal market. COM(2012) 238/2. http://ec.europa.eu/information_society/policy/esignature/docs/regulation/com_2012_2038_en.pdf (2012f)

- European Commission: Electronic identification, signatures and trust services: Questions & Answers. http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/12/403&format=HTML&aged=0&language=EN&guiLanguage=en (2012g)

- Falliere, Nicolas; O Murchu, Liam; and Chien, Eric: W32.Stuxnet Dossier, Version 1.4 (February 2011), Symantec Security Response, available at http://securityresponse.symantec.com/en/id/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

- Ferger, Julia: Putting the "e" in public procurement. State of play, challenges and ways forward. Presentation given at: 6th PEPPOL Nordic conference, Stockholm, May 26, 2011.

- General Dynamics: TVE for Desktops and Laptops. 2011. http://www.gdc4s.com/content/detail.cfm?item=35a995b0-b3b7-4097-9324-2c50008b3a75.

- Graux, Hans; Lambert, Guy; Jossin, Brigitte; Meyvis, Eric: European e-Government Service: Study on mutual Recognition of eSignatures: update of Country Profiles, Analysis & Assessment Report, October 2009, available at http://ec.europa.eu/idabc/servlets/Doca7bf.pdf?id=32436

- Graux, Hans; Delos, Olivier; Lacroix, Sylvie: Common Solution Model - Completion of the framework for Signature Validation Services. 2010. http://ec.europa.eu/idabc/

- Grawrock, D. The Intel Safer Computing Initiative. Intel Press, 2006.

- Hange, Michael: Presentation given at: Zukünftiges Internet, Berlin 2011

- HEISER, G., ANDRONICK, J., ELPHINSTONE, K., KLEIN, G., KUZ, I. and LEONID, R. The Road to Trustworthy Systems. Communications of the ACM, 53(6), 107–115, June, 2010.

- Kang-il Seo: PPS's e-Procurement Support for SMEs. 2009. http://www.epractice.eu/files/KANG%20PPS%27s%20e-Procurement%20Support%20for%20SMEs.pdf

- Kang, Hoin: The experience of the Republic of Korea. Presentation given at: Electronic Procurement – Challenges and Opportunities. 26 June 2012, Brussels.

- KPMG: Öffentliches Beschaffungswesen. Gutachten für den Deutschen Bundestag. Berlin 2002.

- Kuhlmann, D.; Weber, A. OpenTC Final Report. The Evolution of the OpenTC Architecture Illustrated via its Proof-of-Concept-Prototypes. Bristol, Karlsruhe 2009, http://www.opentc.net/.

- Langenbach, Christian; Ulrich, Otto (eds). Elektronische Signaturen. Kulturelle Rahmenbedingungen einer technischen Entwicklung. Berlin 2002.

- Langner, Ralph: Stuxnet: Dissecting a Cyberwarfare Weapon, IEEE Security and Privacy Vol. 9 2011, http://doi.ieeecomputersociety.org/10.1109/MSP.2011.67

- Merkle, R.: Secure Communications over Insecure Channels (1974). With an Interview of 1995. Edited by A. Weber (2000). http://www.itas.fzk.de/mahp/weber/weber.htm

- Meyer, Thomas: E-procurement. Public procurement worth two trillion euros needs smarter spending. Frankfurt 2011. http://www.dbresearch.com/MAIL/DBR_INTERNET_EN-PROD/PROD0000000000269867.pdf

- Moon, Sung Eun: The Practical use of Electronic Signature in PKI, February 4, 2010, available at http://www.jipdec.or.jp/project/anshinkan/doc/20100204/07-1.pdf

- Nader, R. Unsafe at Any Speed. Grossman Publishers, New York 1965.

- National Information Society Agency: 2010 Informatization White Paper Republic of Korea, available at http://crosshub.tistory.com/attachment/cfile1.uf@19314B3C4EF3F8CC13C8FF.pdf

- OECD: Integrity in Public Procurement. Paris 2007. http://www.oecd.org/dataoecd/43/36/38588964.pdf

- Official Journal of the European Community: EC Procurement Thresholds. 2012. http://www.ojec.com/Threshholds.aspx

- Ovum Consulting: Broadband Policy Development in the Republic of Korea, October 2009, available at http://www.infodev.org/en/Document.934.pdf

- Pedersen, Torben: Non-interactive and information-theoretic secure verifiable secret sharing. In: Advances in Cryptology - CRYPTO '91, LNCS 576, 129–140. Springer, 1992

- PEPPOL Initiative (website): http://www.peppol.eu.

- Pfitzmann, B., James, R., Stüble, C., Waidner, M. and Weber, A. The PERSEUS System Architecture. IBM Research Report RZ 3335, IBM Research – Zurich, April 2001. http://www.zurich.ibm.com/security/publications/2001.html.

- Place de Marché Interministérielle www.marches-publics.gouv.fr

- Portuguese Citizen Card: Backgroun[d] http://www.cartaodocidadao.pt/index.php?option=com_content&task=view&id=17&Itemid=26&lang=en (2008)

- Posch, Reinhard: Presentation given at: CAST-Forum „Public Key Infrastructures", Darmstadt, Germany, Jan. 27, 2011

- Prins, J. Fox-IT. Interim Report. September 5, 2011. DigiNotar Certificate Authority breach "Operation Black Tulip". http://www.diginotar.nl/Portals/7/Persberichten/Operation%20Black%20Tulip%20v1.0a.pdf

- Quiring-Kock, Gisela: PKI für Bürger – transparent, sicher, datenschutzgerecht? In: Datenschutz und Datensicherheit, 7/2009, 396-398. http://www.springerlink.com/content/d16g77507t677118/fulltext.pdf.

- Rannenberg, Kai: Research and Innovation. Presentation given at: Stakeholder Workshop Electronic identification, authentication and signatures in the European digital single market. Brussels, 2011. http://ec.europa.eu/information_society/policy/esignature/docs/workshop_10_03/12_kai_rannenberg.pdf

- Reimer, Helmut; Lapp, Thomas: Signaturen und kein Ende. Datenschutz und Datensicherheit 11/2009. http://www.springerlink.com/content/u53027126677208r/fulltext.pdf

- Reuters: VeriSign Hacked, Successfully and Repeatedly, in 2010. February 3, 2012. http://www.reuters.com/article/2012/02/02/us-hacking-verisign-idUSTRE8110Z820120202

- Ricou, Manuel: Public e-Procurement in Portugal. Presentation. Brussels, 2010. http://ec.europa.eu/internal_market/publicprocurement/e-procurement/consultations/open_hearing_de.htm

- Riehm, Ulrich et al.: TA-Projekt E-Commerce. Endbericht. Berlin, TAB 2002. http://www.tab-beim-bundestag.de/de/pdf/publikationen/berichte/TAB-Arbeitsbericht-ab078.pdf.

- Rosenkötter, Annette; Hoffmann, Anja; Gyulai-Schmidt, Andrea; Fritz, Aline; Kühn, Elke: Digital Internal Market. Internal Market and Consumer Protection Committee (IMCO), Directorate-General for Internal Policies, European Parliament 2011. Available at http://www.europarl.europa.eu/document/activities/cont/201108/20110825ATT25260/20110825ATT25260EN.pdf

- Schwemmer, Jürgen: Presentation given at: CAST-Forum „Public Key Infrastructures", Darmstadt, Germany, Jan. 27, 2011

- Sealed, DLA Piper, Across communications: Study on the standardisation aspects of eSignature, External study for the Commission, November 2007, Final Report, Available at: http://ec.europa.eu/information_society/eeurope/i2010/docs/esignatures/e_signatures_standardisation.pdf.

- Sealed, time.lex, Siemens: Study on Cross-Border Interoperability of eSignatures (CROBIES): Guidelines and guidance for cross-border and interoperable implementation of electronic signatures. 2010. Available at http://ec.europa.eu/information_society/policy/esignature/crobies_study/index_en.htm

- SECORVO: Security News, June 2010. http://www.secorvo.de/security-news/secorvo-ssn1006.pdf.

- Secunet: Sina. 2012. http://www.secunet.com/en/products-services/high-security/sina/

- Siemens, time.lex: Preliminary Study on the electronic provision of certificates and attestations usually required in public procurement procedures. 2008. http://ec.europa.eu/internal_market/publicprocurement/docs/e-Procurement/ecertificates-study_en.pdf

- Siemens, time.lex, Study on mutual recognition of eSignatures: update of Country Profiles, Analysis & assessment report, October 2009, Available at: http://ec.europa.eu/idabc/servlets/Doca7bf.pdf?id=32436l (2009a)

- Siemens, time.lex, Study on electronic documents and electronic delivery for the purpose of the implementation of Art. 8 of the Services Directive, February 2009, Available at: http://www.epractice.eu/en/library/314375 (2009b)

- Siemens, time.lex: Study on the evaluation of the Action Plan for the implementation of the legal framework for electronic procurement (Phase II). Analysis, assessment and recommendations. Brussels 2010. http://ec.europa.eu/internal_market/consultations/docs/2010/e-procurement/siemens-study_en.pdf. (2010a)

- Siemens, time.lex: CROBIES-Study – cross-border interoperability of eSignatures: definition of common requirements, External study for the Commission, July 2010 Available at: http://ec.europa.eu/information_society/policy/esignature/crobies_study/index_en.htm (2010b)

- Siemens, time.lex, Study on European Federated Validation Service (EFVS), External study for the Commission, 2009/2010, Available at: http://ec.europa.eu/idabc/en/document/7764.html (2010c)

- Siemens, time.lex, Completion of the framework for Signature Validation Services, Common Solution Model, D 3.4, D 3.5, D 3.6, Final Report, March 2010, Available at: http://ec.europa.eu/idabc/servlets/Docf934.pdf?id=32633 (2010d)

- Simons, Barbara: Internet voting. Presentation given at STOA workshop "Can e-voting increase electoral participation?" Brussels 17 March, 2011. http://www.europarl.europa.eu/stoa/events/workshop/20111703/barbarasimons_en.pdf.

- Smit, Robbert: NAMSA – NATO's Logistics Agency of Excellence. Slovak industry day. 2011. http://www.mzv.sk/App/wcm/media.nsf/vw_ByID/ID_FA84A7F5D82B216EC12579210037AD38_SK/$File/3%20-%20NAMSA.pdf

-

- Soontiens, Werner; Miyamoto, Tadayuki; Egan, Victor; Schapper, Paul ; McDermont, David, and Vargas, Enrique: *Multilateral development bank international survey of e-procurement systems.* Bentley, Perth, Western Australia: CBS, School of Management and International Governance Solutions Ltd, 2007. http://www.business.curtin.edu.au/index.cfm/business/staff-directory?profile=Victor-Egan

- Spalka, Adrian/Cremers, Armin B./Langweg, Hanno: The Fairy Tale of „What You See Is What You Sign" – Trojan Horse Attacks on Software for Digital Signatures. IFIP 2001. http://www.cs.kau.se/~simone/ifip-wg-9.6/scits2/adrian.pdf.

- SPOCS (website): http://www.eu-spocs.eu

- STORK (website): https://www.eid-stork.eu

- T7 e.V. http://www.t7ev.org/

- T7 & TeleTrust: Common PKI Specifications for interoperable Applications [Common-PKI_v2.0.pdf]. 2009. Available at http://www.t7ev.org/uploads/media/Common-PKI_v2.0.pdf

- TeleTrusT: European Bridge CA. Access 15 May 2012. www.teletrust.de/en/european-bridge-ca

- Thai, Khi: International Handbook of Public Procurement. CRC Press. Boca Raton 2009. http://www.sate.gr/nea/international%20handbook%20of%20Public%20Procurement.pdf

- United Nations 2011. Expert Group Meeting. E-Procurement: Towards Transparancy and Efficiency. http://unpan1.un.org/intradoc/groups/public/documents/un/unpan047627.pdf

- Vergabeblog 2011: "Anfang 2012 wird eine neue Zeitrechnung beginnen für die eVergabe in Deutschland". Interview mit Marc Schmidt. Interview by Marco Junk, February 23, 2011.

http://www.vergabeblog.de/2011-02-23/anfang-2012-wird-eine-neue-zeitrechnung-beginnen-fur-die-evergabe-in-deutschland-interview-mit-marc-christopher-schmidt-projektleiter-xvergabe-beschaffungsamt-des-bmi

- Vishik, Claire: Presentation given at Zukünftiges Internet, Berlin 2011

- Weber, Arnd: Enabling Crypto. How Radical Innovations Occur. In: Communications of the ACM. Volume 45, Issue 4 (April 2002), 103-107.

- Weber, Arnd; Weber, Dirk: Verifizierte Virtualisierung für Sicherheit und Komfort. In: Datenschutz und Datensicherheit 1/2012, 43-47.

- XVergabe: Many eTendering Platforms–One Bid-Client. 2011. http://www.xvergabe.org/confluence/download/attachments/1703938/xv_web_presentation_v004_20110708_en.pdf?version=1&modificationDate=1310031411295

Appendix: Experts Interviewed Regarding eProcurement

A small number of workshops and conferences were attended, and a few explorative, informal interviews conducted, including some email exchange. The following events were attended:

1. Zukünftiges Internet (Future Internet; Berlin, Germany, July 5-6, 2011; http://www.future-internet-konferenz.de/).
2. Tag der IT-Sicherheit (IT security day; Karlsruhe, Germany, July 14, 2011; http://www.ka-it-si.de/presse_doc/pm-55ka-it-si.pdf).
3. CAST-Forum „Public Key Infrastructures", Darmstadt, Germany, Jan. 27, 2011.
4. 6th PEPPOL Nordic conference, Stockholm, May 26, 2011.
5. Electronic Procurement – Challenges and Opportunities. 26 June 2012, Brussels.

Individuals communicated with include:

1. Beergrehn, Thomas. EU-Supply
2. Esterle, Alain. Partner of PEPPOL
3. Ferger, Julia. European Parliament
4. Hange, Michael. BSI
5. Klein, Stefan. Bremen Online Services
6. Lioy, Antonio. Politecnico di Torino
7. Ølnes, Jon. DIFI
8. Pascoal, Alcino. Madan Parque
9. Schäfer, Peter. BDI
10. Thölken, Lars. Bremen Online Services
11. Vidigal, Luis. APDSI
12. Waidner, Michael. Fraunhofer SIT

3 CASE STUDY: EHEALTH AND ELECTRONIC HEALTH RECORDS

Authors: Soeren Duus Oestergaard and Kristian Duus Oestergaard, Duus Communication, Denmark

3.1 Introduction

This chapter focuses on the security aspects of the collection, storage and use of health data in eHealth applications such as Electronic Health Records and electronic health cards. Currently, these tools attract major attention in relation to the development of the European eHealth sector. From 2004 when the European Commission launched its first eHealth action plan, almost all European countries have focused on developing national eHealth platforms and solutions based on the original policy definition, stating that:

"e-Health covers the interaction between patients and health-service providers, institution-to-institution transmission of data, or peer-to-peer communication between patients and/or health professionals. Examples include health information networks, Electronic health records, telemedicine services, wearable and portable systems which communicate, health portals, and many other ICT-based tools assisting disease prevention, diagnosis, treatment, health monitoring and lifestyle management".[2]

eHealth is considered a cornerstone in alleviating the challenges faced by European health care systems. Demographic ageing, rising numbers of people suffering from chronic conditions, shortages of health care professionals and heightened expectations from patients and citizens towards connected health care systems will be a continuous financial and organisational challenge in the provision of health and social care in the coming years. Examples of eHealth applications include the above mentioned services and tools, but also health portals, as well as secondary usage of non-clinical systems such as research registers, or support systems such as billing systems (e-Health Task Force 2007, p. 10). At the same time the scientific progress in the medical field promises progress in individualised treatments to a level that requires very precise personalised information, for instance on genetic patterns. Also the increased political interest in preventive treatments and the focus on changes of lifestyle behaviour may lead to an increased storage of personal information as a by-product of telemedicine for chronic patients living at home. These data may soon be seen as a natural extension of traditional EHR content.
Electronic Health Records are envisioned to improve accessibility and continuity of care, reduce the risk of medical errors, reduce costs to the system of repeated diagnostic testing and redundant record keeping, and improve workflow efficiencies through the improved transmission of clinical information. In addition, use of EHRs is seen as a source of accurate statistical data for quality improvement of health care systems and medical research (secondary use of health care data).

Despite the advantages of a more uniform way of documenting medical care and coordinating care among different health care providers, there are also drawbacks to the use of electronic health care records. Personal health data is extremely sensitive, and its theft, loss or unauthorised use or disclosure can have very serious consequences for the individuals involved. Malware attacks, denial-of-service attacks, fake documents created by error or attack, and crafted attacks on medical documents and prescriptions are serious security threats facing patients relying on the accessibility and accuracy of EHRs. In addition to privacy and data security risks there are economic disadvantages e.g. high start-up costs (equipment to retrieve and store data, expenses to the conversions of paper charts to electronic records), health care professional training on the use of EHRs and the rearrangements of workflows.

[2] See http://ec.europa.eu/information_society/activities/health/whatis_e-Health/index_en.htm).

Other dangers include financial risks (unmet expectations of cost reductions, billing errors in software) and software breakdowns. According to an ENISA study (ENISA 2009) one of the biggest challenges in implementing eHealth concepts is convincing the public that their electronic health records will be safe and secure. Thus, adequate privacy and data protection, and the trust these support, are crucial for realising envisioned benefits of EHR systems.

3.1.1 Outline

This chapter examines existing national and pan-European eHealth records initiatives enabling access to cross-border health care. It looks into the implementation and execution of eHealth systems in The U.K's National Programme for IT (NPfIT), an initiative by the Department of Health in England to move the National Health Service (NHS) towards a single, centrally mandated electronic care record, and the eHealth system in Estonia. These eHealth projects were selected due to the differences between the countries (Eastern vs. Western and large scale project vs. small scale project) in order to get a broader perspective on this subject. The fact is that Estonia is one of the first countries in the world to implement a nationwide EHR system and the perceived success of the Estonian project (Willemson & Ansper, 2008) compared to the fate of the NPfIT project that suffered from many problems leading, at least partly, to a cancellation of the project in 2011, although significant elements are regarded as successful and further sub-projects may continue (National Audit Office 2011).

We also analyse two European cross-border eHealth projects: the epSOS and the Baltic eHealth. The epSOS project aims to design, build and evaluate a service infrastructure that demonstrates cross-border interoperability between electronic health record systems in Europe. The aim of the Baltic eHealth project was to illustrate that eHealth is an effective means for increasing access to healthcare of high quality in rural areas, thereby contributing to counteracting rural migration. Five countries participated in Baltic eHealth: Denmark, Estonia, Lithuania, Norway and Sweden. The project came to an end in 2007.

These two projects have helped us understand the difficulties and the security challenges involved in conducting cross-border eHealth projects. A cross-cutting concern in the country studies as well as in the EU studies is to review the previously identified interrelated security challenges facing the design, roll-out and operation of cross-border eGovernment systems. They include network security, interoperability, identification, usability, privacy, access control and function creep/secondary use of data.

In Section 3.2 the current status of EHR implementation in Europe is addressed. In section 3.3 EHR technologies are introduced. Section 3.4 provides an overview of security issues in EHR systems while section 3.5 presents the European policy and regulatory framework of eHealth and EHRs in particular. Section 3.6 constitutes the country studies and the EU studies. Section 3.7 synthesises/discusses the findings of the cases and engages with the seven security challenges. Conclusions are drawn in section 3.8. In appendix 1 a list of experts consulted during the knowledge-building phase of the project is provided. Appendix 2 contains a brief summary of the issues and challenges observed in the 4 studies.

3.2 EHR implementation in Europe

Electronic Health Record systems (EHRs) are central in the eHealth strategies of most Member States and in recent years they have been adopted at increasing rates at local and regional Member State levels, whereas few countries have as yet fully implemented large-scale EHR systems (Stroetmann et al. 2011). A number of studies have been carried out to track and assess the progress made towards the goals set by the eHealth Action plan. Moen et al. (2012) conclude that although the broader aim of eHealth originally focused on supporting health professionals and securing that sufficient data was available at the time and place of need, they noted that for future development privacy, security, common standards

as well as active integration to allow participation by all citizens would be of growing interest. The assessment carried out by Stroetmann et. al. in 2010 covered the progress made by the Member States towards realising the key objectives but also monitored a number of best practices examples from national programmes on eHealth across Europe. The final assessment in 2011 contains details on progress in the respective countries (Stoetmann et al., 2011). Among the key findings we can observe that by 2010 all 27 member countries had either implemented or planned to develop an Electronic Health Record summary for the patients. Likewise, all countries had (pilot) projects implemented or in a planning phase for tele-Health care and were aware of the need for (national) standards to allow for interoperability. Similarly almost all countries (26) were regarding Patient Identity as a crucial factor and 25 countries were developing or had implemented citizen cards. Thus, on the surface it seems that the European countries are trying to meet the jointly developed strategies for eHealth.

The eHealth Governance Initiative, supported by DG INFSO and SANCO, has a specific focus on interoperability and provide a long term vision in developing the second eHealth Action plan for 2012-2020 (envisioned for release in 2012). In the public consultation on the second eHealth Action Plan the following objectives are stated:

1) Increase awareness of benefits of eHealth and empower citizens, patients and professionals

2) Address interoperability issues

3) Improve legal certainty for eHealth (including support for privacy)

4) Support innovation and research in eHealth with a focus on developing a competitive European and global market.[3]

It should be noted that eHealth as described above is more than Electronic Health Recordsand also covers specialty solutions, radiology, laboratory test results, adjacent support systems like epicrisis/dismissal letters, booking and patient administrative systems and workflow systems supporting professionals in performing defined tasks. On top of this, connected home care via telemedicine and remote surveillance of chronically ill patients add yet another dimension to the type and amount of data related to a single patient. Individualised medicine depending on human genetic pattern as well as preventive treatments will eventually lead to more detailed information on individual patients, reflecting lifestyle, personal behaviour and habits.

3.3 Electronic Health Records: The technology

The historical development of EHR systems began with almost exclusively paper-based records kept by GPs and at hospitals; originally these records kept track of actual diagnostic information, treatments and prescriptions. The next level of sophistication occurred with the introduction of ICT used for basic, though disparate solutions storing information on vital patient data - blood type, allergies, immunisation etc. – also typically in separate systems for GPs and individual hospitals and specialists. The next level of maturity of Electronic Health Records are typically regionalised data bases for the sharing of patient data between hospitals, GPs and specialists, and the development of independent systems for patient administration, laboratory test results, radiology, and dismissal letters (epicrisis) in a more and more complex interaction with the basic patient data.

[3]See http://ec.europa.eu/information_society/activities/health/e-health_ap_consultation/index_en.htm.

An Electronic Health Record is defined as 'an evolving concept defined as a systematic collection of electronic health information about individual patients or populations. It is a record in digital format that is capable of being shared across different healthcare settings, by being embedded in network connected enterprise-wide information systems' (Gunter 2005). Another often cited definition is that EHR is 'digitally stored healthcare information about an individual's lifetime with the purpose of supporting continuity of care, education and research, and ensuring confidentiality at all times' (Iakovidis 1998).

An EHR is an electronic repository of a patient's electronic medical record shared by different health care organisations involved in the patient's individual care path. EHRs may include information such as medical observations, laboratory tests, diagnostic imaging reports, treatments, drugs prescribed, dispensed and administered, legal permissions, allergies and the identities of the healthcare professionals and provider organizations who have provided healthcare as well as billing information. EHR technology may include the possibility of giving patients access to some portion of their electronic record allowing them to view their medical data, contribute information on symptoms to their record and communicate with their health care providers.

In terms of access to health care when travelling abroad, the European Health Insurance Card (EHIC) enables access to health care services for insured European citizens. The EHIC is mostly realized as a printed version of the national health insurance card or as an electronic data set stored on a national electronic health insurance card. The EU funded NETC@RDS pilot project aims at achieving an 'electronification' of the European Health Insurance Card (eEHIC) in 16 participating EFTA/EU countries (NETC@RDS project website). It establishes an online service for the EHIC to authenticate a patient's health insurance chip card and/or a patient's entitlement to health insurance benefits abroad. An online verification provides assurance to support acceptance procedures for both health insurances and health care providers (ibid.). (For full description and risk assessment, see ENISA, 2010). It must be noted that the European Health Card as well as the NETC@RDS project aim solely at securing the citizen's right to treatment. There is neither information on actual health status, nor information on for instance allergies, blood type etc. The NETC@ARDS project, however, may be regarded as a stepping stone towards interconnectivity across borders, as it comprises a secure network of national service portals and databases, accessed from authorized and identified health professionals. In the NETC@ARDS project certificates are stored in various devices depending on the national scheme (e.g. workstation hard disks, health professional cards, USB keys). The NETC@RDS project utilizes state-of-the-art technologies, directly suited to the requirements of service in the following areas: web interfaces, end-to-end security over networks of national service portals, data repositories and access point workstations, data protection, individual authentication and provision for back-end integration and auditing services. Each portal can be connected to one or multiple national/regional registries in order to provide an online checking service. The infrastructure enables any health professional using the system to check that the patient's card or any other presented proof of entitlement is still deemed valid by the issuing organization (for further details, see the NETC@ARDS project website).

While NETC@ARDS' objective is to ensure legibility of a patient's entitlement to treatment, the infrastructure actually could be used as a stepping stone towards real access to remote databases and health records. As some countries - Spain, Belgium, Finland, Austria, Estonia - are combining their national identity cards with Health Insurance, the use of Health Smart Cards in combination with the implementation of National Public Key Infrastructures will become an important tool to ensure proper identification of patients (Frost & Sullivan Market Insight 2010).

National plans for connected EHR systems and smart health cards call for a number of joined-up activities: the development of patient ID-systems, professional access systems, standards for interchange of subsets of records etc. The pressure for cross-border exchange of health care data occurs simultaneously with the financially initiated pressure on medical staff accelerating the introduction of telemedicine, tele-home care and ambient assisted living for elderly and/or chronically ill. This will lead

to other types of security threats and introduces new categories of stakeholders including municipality services, neighbour and family carer support etc.

3.4 Security issues of EHRs

Any ICT system aimed at providing public services to citizens through private networks or via the internet will have to establish means and barriers to protect network components, applications and data from malicious intrusion, theft, disclosure, and destruction. Most Government ICT strategies recommend implementation of a Public Key Infrastructure as a necessary prerequisite to obtain a secure infrastructure.

The American Institute for Standards and Technology has provided an in-depth set of guidelines particularly aimed at protecting public ICT systems in its Federal Information Security Management Act (FISMA) implementation project[4]. These guidelines cover standards for categorisation of systems by mission impact, minimum security requirements, guidance for selecting proper security controls as well as guidance for security authorisation and security monitoring. The European Security Research and Innovation Forum (ESRIF) in its final report[5] from December 2009 discussed the so-called security cycle - preventing, protecting, preparing, responding and recovery for security breaches (p. 20), and gave an overview of means to counter different types of attacks (p. 23), and methods to secure critical assets (p. 26).

While these guidelines are generic by nature, the US Health Insurance Portability and Accountability Act (HIPAA) has developed a series of recommendations and guidelines that are particularly aimed at the Health sector. The guidelines for the technical safeguards cover the key aspects of the security infrastructure items that we would find in best-of-class eHealth systems.[6]

The main recommendations cover key aspects such as:

Access Controls - to provide users with rights and privileges to access and perform functions, access info systems, applications, programs, files. This calls for requirements of Unique User Identification, Emergency Access Procedure (in case of patient risk), automatic logoff, encryption and decryption of personally identifiable information.

Audit Controls - to implement HW, SW and/or procedural mechanisms that record and examine information system activity that contain or use EHR.

Integrity - Implementation of policies and procedures to protect health information from improper alteration or destruction.

Person or Entity Authentication - to implement procedures to verify that a person or entity seeking access to EHR is the one claimed.

Transmission Security - Implementation of technical security measures to guard against unauthorised access to electronic health information being transmitted over an electronic communications network.

For each of these 5 key areas a set of standards is defined.

---

[4] See http://csrc.nist.gov/groups/SMA/fisma/index.html.

[5] Http://www.eurosfaire.prd.fr/7pc/bibliotheque/consulter.php?id=1507.

[6] Http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/securityruleguidance.html.

In EHR systems, safeguarding the confidentiality, integrity and availability of patient data is pivotal. Confidentiality means that the data contained in the EHRs should not be disclosed during its transmission and used by unauthorised people. This is the most important requirement that systems handling EHRs must satisfy. Patients' personal and health information must be encrypted to avoid unauthorised access. Integrity means that data in the EHR cannot be created or altered without proper authorisation. Integrity involves both users and systems. Availability is as essential as integrity because the information in EHRs might be necessary for adequate treatment. In essence, the main characteristics that a healthcare network security system should provide (as defined in the HIPAA Guidelines) are:

1. User/entity authentication to verify requests for access to data
2. User/entity authorisation to permit access to data
3. Ensured confidentiality of data transmitted over the communications network
4. Integrity of data
5. Ability to audit access and changes to EHR

Following these main requirements, different security solutions are implemented in European ERH systems. However, a standardised approach to the development of EHRs is still lacking.

In addition to the security threats described in relation to eProcurement in the preceding chapter (section 2.4.2) electronic health recording systems pose risks in several areas including failure to comply with informed consent legislation, failure to comply with data protection legislation, data breaches and identity theft, e.g. doctors being impersonated by hackers. Data confidentiality in EHRs must also entail safeguards against unauthorised medical access, i.e. doctors working with employers and reading records of employees. An additional security risk in EHRs is that they may render second opinions in health care unfeasible. A shared electronic record system might reproduce medical errors in individual treatment pathways or deter health professionals from querying alternative treatments for their patients.

Security concerns are also related to different storage models of EHR systems. EHRs may be stored centrally, locally, host-based or in the cloud. According to the eHealth Strategies study (Stroetmann 2011), Belgium and the Netherlands have chosen a decentralised system with specific laws to install a national 'traffic control' platform. Spain has also chosen a decentralised storage model enforcing it with national data protection legislation. Finland and the Czech Republic have a centralised system with legislative changes implemented to install a central repository. France has chosen a host-based EHR system where citizens can determine a third party data host for their health record. French data hosts require certification. Overseas e.g. in Australia, EHR data models are discussed as centralised versus federated. Cloud based EHR architectures are eagerly discussed in vendor and supplier communities, but to our knowledge not implemented in Europe yet.[7]

Privacy issues concerning EHR and personal identifiable health information represent a special issue and must be dealt with even in more detail than for other eGovernment ICT systems, since disclosure of health related information may incriminate persons and distortion of key personal information may endanger patient life. Examples are many: From insurance companies gaining insight into lifestyle and health indicators for individuals to employers checking health status of applicants and newspapers revealing data on politicians etc. The particular issues surrounding health related information have resulted in a number of negative cases and the reporting of disclosure or loss of health data are also quite numerous. Furthermore the risk of identity theft has increased criticism of for instance the German

[7] The UK G-Cloud project is envisioned to address e-Health applications in the coming years), see http://www.cmswire.com/cms/customer-experience/gcloud-cloudstore-launches-with-1700-services-for-uk-government-014579.php.

Health Card[8], if not for other reasons then because citizens do not see the benefit of having to reveal all personal information - name, sex, date-of-birth, address, registration ID - every time the card is presented to obtain treatment or collect medicine.

These attitudes lead to the conclusion that any citizen or patient could have the option to obtain a number of pseudonyms, in order to self-monitor how much and which information he wants to disclose in a particular situation and to which entity/organisation.

This was the idea behind the EU project PRIMELIFE[9], and in particular the follow-up project ABC4Trust[10] (Architecture for Attribute-Based Credential Technologies), which has developed some very interesting technical proposals for ensuring controlled access and enhanced privacy.

In other countries, e.g. the Nordic, the general trust in the Public Sector Entities and their dealings with citizen information do not seem to call for pseudonyms on a large scale. Instead, other privacy-enhancing technologies might be used (see for instance the description of the Dutch discussions on EHR in 2009[11]). One example of other types of privacy-enhancing technologies could be the so-called Hippocratic Database project[12] that introduces cell-based policy-enforced access to data.

Based on access roles/authentication and match against a policy file, the user will see different fields in a database, depending on the character of his authorisation. This means, for instance, that only authorised persons will ever get to know whether a patient has been examined for HIV or not. Similarly the solution also supports privacy-enforced data mining, which is helpful to anonymize patient identities while allowing health data to be used for medical research. At this moment, this type of solution has been introduced in the Dutch Academic Medical Centre, Amsterdam, and for the National Health Network in India. Also this approach will enhance the auditing as all attempts to circumvent policy will be tracked.

3.5 Policy and regulatory frameworks for EHR systems

Although health care systems and health care policy remain the responsibility of Member State governments under the EU's subsidiarity principle, the European Commission has actively pursued legal and regulatory means of promoting eHealth adoption across Europe as well as invested in eHealth projects in the last two decades. Following the just released European Commission initiated eHealth Task Force expert report, eHealth and telemedicine are considered vital in supporting European health care systems' response to pending challenges by providing more efficient use of services and capacities in the health sector (e-Health Task Force 2012).

A core ambition of the EC's eHealth strategy is to enable access to the patient's electronic health records across sectoral and national boundaries. With the eHealth Action Plan (European Commission 2004) and the one forthcoming in 2012, Member States are committed to develop and issue national eHealth strategies and implementation roadmaps and plans for the deployment of eHealth applications addressing policy actions identified in the action plan. The European Commission's Innovation Union and the Digital Agenda for Europe (European Commission 2010b), both published in 2010 as flagship initiatives of the EU Europe 2020 strategy for "smart, sustainable and inclusive growth", define specific measures to use ICT to address societal challenges including rising healthcare costs and aging

[8]Http://www.spiegel.de/wirtschaft/soziales/elektronische-gesundheitskarte-mega-flop-im-massentest-a-755464.html.

[9] Http://primelife.ercim.eu/.

[10]https://abc4trust.eu/

[11]Http://ojs.ubvu.vu.nl/alf/article/view/93/167.

[12] Http://www.almaden.ibm.com/cs/projects/iis/hdb/hdb_projects.shtml.

populations (European Commission 2010, p. 6). More specifically, the Digital Agenda underlines "the right of individuals to have their personal health information safely stored within a healthcare system accessible online" as a cornerstone of a successful uptake of eHealth and calls for actions "to remove legal and organizational barriers, particularly those to pan-European interoperability, and strengthen cooperation among Member States" (ibid., p. 29). Under Pillar 7 of the Digital Agenda (ICT for Social Challenges) the following key actions relate to eHealth (Digital Agenda web portal, Pillar VII: ICT for Social Challenges):

- Action 75: Give Europeans secure online access to their medical health data by 2015 and achieve widespread telemedicine deployment by 2020;
- Action 76: Propose a recommendation to define a minimum common set of patient data to be accessed/exchanged across Member States by 2012;
- Action 77: Foster EU wide standards, interoperability testing and certification of eHealth systems by 2015.

In eHealth, electronic identity management and interoperability of electronic health record systems ensuring protection of personal data and confidentiality have long been EC policy goals. Thus, the Council Conclusions on eHealth of December 2009 reaffirmed the EC Recommendation on cross-border interoperability of electronic health record systems issued in 2008 (European Commission 2008). eHealth interoperability is defined as "the capability for independent and heterogeneous health information systems to exchange health-related data for use by doctors, healthcare providers and patients" (European Commission Thematic Portal ICT for Health).

The European Commission has been funding interoperability projects for several years – following a stated EU ideal to make available a range of common eHealth standards by which data can be organised nationally and across borders. However, according to Danish Programme Manager Anni Buhr, interoperability in terms of proper transfer of meaning between systems is still largely unresolved (semantic interoperability). In the ongoing European eHealth project epSOS, translating electronic prescriptions from one country to another is experienced as problematic. Brand names of medications vary from Member State to Member State, and dosages are documented differently across the EU. Buhr stresses that in order to reach semantic interoperability in the field of medication, a common EU terminology for drugs is needed (Anni Buhr, personal communication).

At the EU level an accompanying concern for enhanced privacy and data protection in online environments is currently being addressed in the reform of the European data protection framework. With recognition of the right to the protection of personal data in the Charter of Fundamental Rights of the European Union, data protection is embedded in the evolving legal framework of the new data protection regulation replacing the 1995 Data Protection Directive and supplementing the Directive on privacy and electronic communications (Directive 2002/58/EC) from 2002 with amendments in 2009 (Directive 2009/136/EC).

The following main European Commission regulatory initiatives pertain to the operation of EHR systems:

- European Commission. Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).
- European Commission. Proposal for a Regulation of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market.
- European Commission. Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare.

3.5.1 European data protection regulation

In January 2012, the European Commission proposed a revision of the European data protection regulatory framework (European Commission 2012b). The main objectives of the new regulation replacing a less coercive directive is to allow for increased pan-European alignment of conflicting Member State data protection laws and to enhance individual data protection. The key proposals related to eHealth and the collection and storage of personal data in EHR systems are as follows:

Binding steps towards rule harmonization: A collective set of rules will replace the current varieties of Member State data protection legislation. Differences among Member States are considered a serious vulnerability in current regulatory data protection frameworks. Penalties for non-compliance will be significant. This is expected to strengthen incentives to uphold data protection rules.

Provisions for improved protection of individual citizens include a new definition of 'consent' under the proposed regulation whereby consent must be explicitly obtained (opt-in). Further, the regulation introduces a new notification requirement of data security breaches involving personal data within 24 hours.

With the regulation, new privacy rights are introduced, including data subjects' "right of portability" and the "right to be forgotten". The "right of portability" will allow individuals to transfer data from one provider to another upon request, whereas the "right to be forgotten" will allow data subjects to delete digitally stored data from e.g. social media profiles. Exactly how these rights will be implemented in practice remains to be seen. According to legal expert Charlotte Bagger Tranberg they will be extremely difficult to realize in practice (Charlotte Bagger Tranberg, personal communication). Also of note in the proposed regulation is the provision of data protection by design requirements (Article 23) and the requirement to conduct privacy impact assessments in the course of system development (Charlotte Bagger Tranberg, personal communication). This is foreseen to prompt businesses to incorporate privacy by design principles into business operations at an early product development stage.

3.5.2 European electronic identity regulation

The proposed regulation on data protection is accompanied by the just released proposal from the European Commission for a Regulation on electronic identification and trust services for electronic transactions in the internal market (European Commission 2012a). The proposed regulation is intended to foster security and trust for Internet based services through increased incentives towards the application of eIdentification, eAuthentication and eSignature measures across the EU. This legislative proposal also aims to harmonise conflicting Member State practices of recognising identity electronically. The legislative proposal aims to facilitate cross-border transactions through the adoption of harmonised eSignatures, eIdentities and electronic authentication services across Member States. The proposed regulation replaces the eSignatures Directive 1999/93/EC with increased security demands for electronic identification/digital signatures. The current electronic signature directive covers only electronic signatures. According to the new legislative text, "the aim is to enhance existing legislation and to expand it to cover the mutual recognition and acceptance at EU level of notified electronic identification schemes and other essential related electronic trust services" (Ibid., p. 2).

Electronic identification is seen as an important step towards the realisation of a European single market. Currently, there is no system of mutual recognition of electronic identity cards and far from all Member States have national electronic identity (eID) cards. The regulation proposes to make electronic certificates compulsory and stimulate Member States to accept electronic identity cards (eIDs) from other Member States. Mutual recognition of existing national eIDs and common standards for trust services and eSignatures will benefit European citizens working or residing abroad. For patients seeking health care abroad, eSignatures and eAuthentification will be relevant. As stated in the draft regulation "Mutual

recognition and acceptance of electronic identification and authentication is key to make cross border healthcare for European citizens a reality. When people travel for treatment, their medical data needs to be accessible in the country of treatment. This requires a solid, safe and trusted electronic identification framework." (Ibid., p. 13).

3.5.3 Patients' Rights Directive

The Patient's Rights Directive codifies European Court of Justice case law in provisions related to the prior authorization of health care in another Member State and the reimbursement of such health care. As such the Directive is intended to help patients exercise their right to reimbursement for health care received in another EU country and to establish formal cooperation between European health systems and health authorities. Thus, the Directive is a legal step in the provision of healthcare in the European Single Market. Currently, Member States are figuring out how to inform patients of their rights and entitlements to reimbursement for health care received in another Member State. The Directive states that Member States must set up National Contact points to help patients seeking health care abroad.

The foreseen mobility of patients may in some form be accompanied by patient data flows, although this is not the direct focus of the Directive. However, according to the Directive, Article 5 (d), patients seeking medical treatment in another Member State are entitled to a copy of their health record or to have remote access to it from the Member State of affiliation. The Patient's Rights Directive also supports the creation of a system of mutual recognition of prescriptions allowing prescriptions to be recognized in another Member State. The technical infrastructure for enabling these data exchanges, which data will be exchanged and the security standards and formats required are, however, far from settled (Asger Andreasen, personal communication). The eHealth network foreseen in the Directive article 14 is intended as a platform for such discussions and agreements. Article 14 of the Patient Rights' Directive establishes a voluntary eHealth Network replacing the former eHealth High Level Governance Group, an informal body affiliated with the European eHealth governance initiative (eHGI) that comprised state secretaries and director generals from the national ministries of health. According to Article 14,2 of the Directive, the newly formed eHealth Network of National Competent Authorities will develop common governance principles to:

A. "Work towards delivering sustainable economic and social benefits of European e-Health systems and services and interoperable applications, with a view to achieving a high level of trust and security, enhancing continuity of care and ensuring access to safe and high-quality healthcare";
B. "Draw up guidelines on 1) a non-exhaustive list of data that are to be included in patients' summaries and that can be shared between health professionals to enable continuity of care and patient safety across borders; and 2) effective methods for enabling the use of medical information for public health and research";
C. "Support Member States in developing common identification and authentication measures to facilitate transferability of data in cross-border healthcare."

The eHealth Network of National Competent Authorities has recently adopted a set of conclusions on a common eID and authentication Governance for eHealth Services stating among other things (e-Health Network of National Competent Authorities 2012, 1):

"That the overall vision for better health and citizen-centred health delivery requires that governments recognize every person's need for a personal electronic identification to enable the support of equity of access to healthcare services in the Information Society".

"That a first step towards eID interoperability is to ensure a mutual recognition and acceptance of Identification and Authentication to enable interoperability for continuity of care and improve patient safety;"

"That the twin functionality of eID identification (who you are) and authentication (proof that you are who you claim to be) mechanisms provides the basis for eHealth services for patients and health professional and authorization processes that are critical to access health information and will build upon this proposed eID identification and authentication governance."

Despite the current EC harmonization efforts towards data protection and electronic identity, functional security levels among Member States and different health care organizations are far from aligned or thoroughly regulated. In its conclusions, the Legally eHealth study calls for a definition of duties and rights of all actors involved in eHealth as well as "a proper balancing between the patient's right to privacy and the need for adequate data sharing in a modern eHealth enabled healthcare system" (Doosselaere et al. 2008, p. 18). In addition to a call for greater interoperability and assessment of the impact of competition legislation on the uptake of eHealth products, the report calls for "a formal standardization of the security requirements for both the infrastructure and the eHealth products and services" (ibid. 35). The safeguarding of health data is a responsibility of all Member States; however, there is not yet an agreement on appropriate security levels for healthcare within the EU, which could be applied in cases of health care data exchange. Practical implementations of provisions in the proposed Regulations on data protection and electronic identification and Directive on Patients' Rights will most likely underscore the need for interoperability of formats and standards and ways of ensuring high levels of data protection and privacy for European citizens.

3.6 Case Studies

The following sections contain case studies of eHealth systems projects carried out at national (3.6.1) and European (3.6.2) levels. Following the overall description of the individual cases section 3.5.3 focus specifically on the different security measures taken in the exchange of health data in each case following the 7 security challenges.

The two country case studies (UK and Estonia respectively) represent divergent strategies with regard to system infrastructure. The UK system (NPfIT), which is built on an already existing private but unencrypted network, aims at a central storage of detailed records, and follows a piecemeal security approach. The Estonian system (EHR), on the other hand, rests on a dedicated encrypted network, stores records in a decentralised manner using multiple databases, and follows an overall security policy in line with the country's overall ICT security strategy and based on the Estonian Public Key Infrastructure.

The European case studies examine systems that in different ways seek to provide interconnection between national eHealth systems. From a security point of view, the main difference between the cases are the choices made regarding the methods for establishing data transfer connections between national systems. The first, (epSOS), makes use of a common connection architecture, whereas the second, (Baltic eHealth), allows users to exchange data to establish point-to-point secure connections (VPNs). In both cases, establishing legal agreements between participating countries is crucial. As a test of progression in this area, both cases point towards future development potential, specifically in the areas of central security policy implementation and potential use of cloud computing services.

Section 3.6.3 contains detailed observations regarding the seven central security challenges identified elsewhere in this report. Appendix 2 contains a summary table of the findings in order to establish an overview of the comparisons between the cases.

3.6.1 Country studies

3.6.1.1 NHS National Program for IT

The NHS National Program for IT (NPfIT) (NHS Connecting for Health website) is an initiative by the British Department of Health aimed at moving the National Health Service (NHS) towards a single, centrally-mandated electronic care record for patients, and to connect 30,000 general practitioners to 300 hospitals, providing secure and audited access to these records by authorised health professionals. When the project was launched in 2002, it was the largest civil ICT programme worldwide and the initial budget was more than 15 bn €.

The overall objective was to implement standardised ICT solutions at a national level across diverse regional and local solutions and across private and public actors, GPs and hospitals.

This programme included several projects, described below.

- NHS Care Records Service (NCRS) - The NCRS was made up of a group of systems with different functions and purposes:
    - *The Personal Demographics Service (PDS)* - an application that contains basic demographic details about every NHS patient including name, address and date of birth, NHS number and current GP.
    - *The Summary Care Record (SCR)* - a high-level record of key clinical information including allergies, prescriptions, summary medical history, operations and procedures. An SCR was created for every NHS patient, although patients can choose to opt out, and is available throughout England.
    - *Local record systems* - on which comprehensive patient records will continue to be stored in hospitals, GP surgeries and other organisations. Many of these systems needed to be replaced or upgraded as part of NPfIT to achieve the required functionality of the NCRS and to reduce and eventually eliminate the use of paper systems.
    - *The Detailed Care Record (DCR)* - created by combining information from local systems and thus holding significantly more detailed clinical information than the SCR. The DCR uses shared information from the local providers systems (GPs, hospitals, community providers and others) to produce a single, detailed electronic record, which supports the NPfIT standards.
- The Secondary Uses Service (SUS) - provides a single point of access to aggregated data for purposes of management, commissioning, clinical audit and research. The SUS can collect, manage and analyse electronic health data from a range of sources including the new NCRS systems.
- Choose and Book - a service that allows the patient to pick a hospital or clinic and book his appointment himself. When a patient and his General Practitioner agree that an appointment is needed, the patient can choose which hospital or clinic he wants to go to. Choose and Book will also provide the ability to: Plan and manage your existing appointments if you are currently undergoing treatment, fit the treatment in with other commitments at home and at work, choose appointments that fit your caregivers schedule, easily check the status of your referral and change or cancel your appointments on the phone or the internet.

- GP2GP project - is the shared name of three of the four publicly funded healthcare systems in the United Kingdom. They provide a comprehensive range of health services to residents of the United Kingdom. GP2GP enables GPs to transfer a patient's electronic medical record to another practice when the patient moves to another district.

- Electronic Transmission of Prescriptions (ETP) - The Electronic Prescription Service enables prescribers such as GPs and practice nurses to send prescriptions electronically to a pharmacy of the patient's choice.

- It was the clear intention from the launch of the NPfIT that the main objectives were to improve access to information, but also to increase the level of data security and privacy.
  The New National Network N3 was defined to provide the IT infrastructure to meet these challenges. For the patient data, use of a central database containing patient information, the Spine, was centrally mandated and the messaging between the underlying systems supporting also interoperability standards for workflows were based on the HL7 recognised international standard (based on XML exchange of data).
  During the implementation serious critics were raised, and as early as 2006 23 computer scientists wrote an open letter focusing on lack of usability, patient confidentiality and overall reliability (e-Health Insider 2006)[13]. Some hospitals objected to new systems and claimed that what they had was more advanced and more suited to their local needs.
  Following a number of delays and shortfalls by the industrial partners and the massive criticisms of this centrally controlled approach, the programme was forced to suspend its roll-out of patient summary records in 2010, because citizens objected to the lack of an opt-out option. It was later resumed once this option was established.
  Following the change in Government in 2010 and a serious critical report by the National Audit Office in may 2011, the centralised approach has now been abandoned and increased autonomy to local stakeholders are now introduced together with more operational freedom for hospitals.
  The analysis of the project as a whole was put forward in March 2011 by Wendie Curri et al. (Transforming the NHS using Information Technology - the story so far) and concluded that "the centrally coordinated, shared IT services ... were typically created before precise usage needs were known", and that the entire project suffered from a lack of management focus, a lack of a clearly defined IT architecture, a lack of defined principles for IT investment and priorities, including a lack of transparency of the contract negotiations with the local service providers.

3.6.1.2 Estonia: Electronic Health Record System (Leego et al. 2005)

The Estonian Electronic Health Record System (EHR) covers the entire country. It was launched on December 17, 2008. It is an important part of the e-Estonia strategy, which also includes services for tax, schools, commercial registration, as well as online election services using a common Identity system, which is also used by the Estonian financial sector. The Government services are based on the principle that data is stored where it is collected and availability of data is granted to those who need it.

Already in 2001 the Estonian Government started implementing the infrastructure to ensure this principle and developed what is called X-Road. The 'crossroad' infrastructure aims at enabling connectivity even to quite disparate information systems established in different part of the Estonian

[13]Http://www.e-health-insider.com/news/item.cfm?ID=1822.

government. By 2010 more than 360 different databases and 2000 eServices were available over the X-Road.[14]

The current eHealth strategy in Estonia is described at the Ministry of Health's website.

The Estonian eHealth system includes several major projects:

The digital health record is the most extensive eHealth project and has been divided into four sub-projects:

- The digital record – The main document combined all the relevant patient data in the different databases and built a standard health report of the patient. All institutions offering health care services must file information about their patient into the digital health record reference register. They also need to create links to the information in the IT systems. These links allow retrieval of detailed information about the patient through ordinary inquiries. The central element in the Digital Health Record is the reference register (See Figure). Time-critical information (like patient sensitivity to drugs) must be forwarded to emergency care no more than 30 seconds from request. The Digital Health Record allows doctors to improve the health treatment and minimise the risks for mistakes.

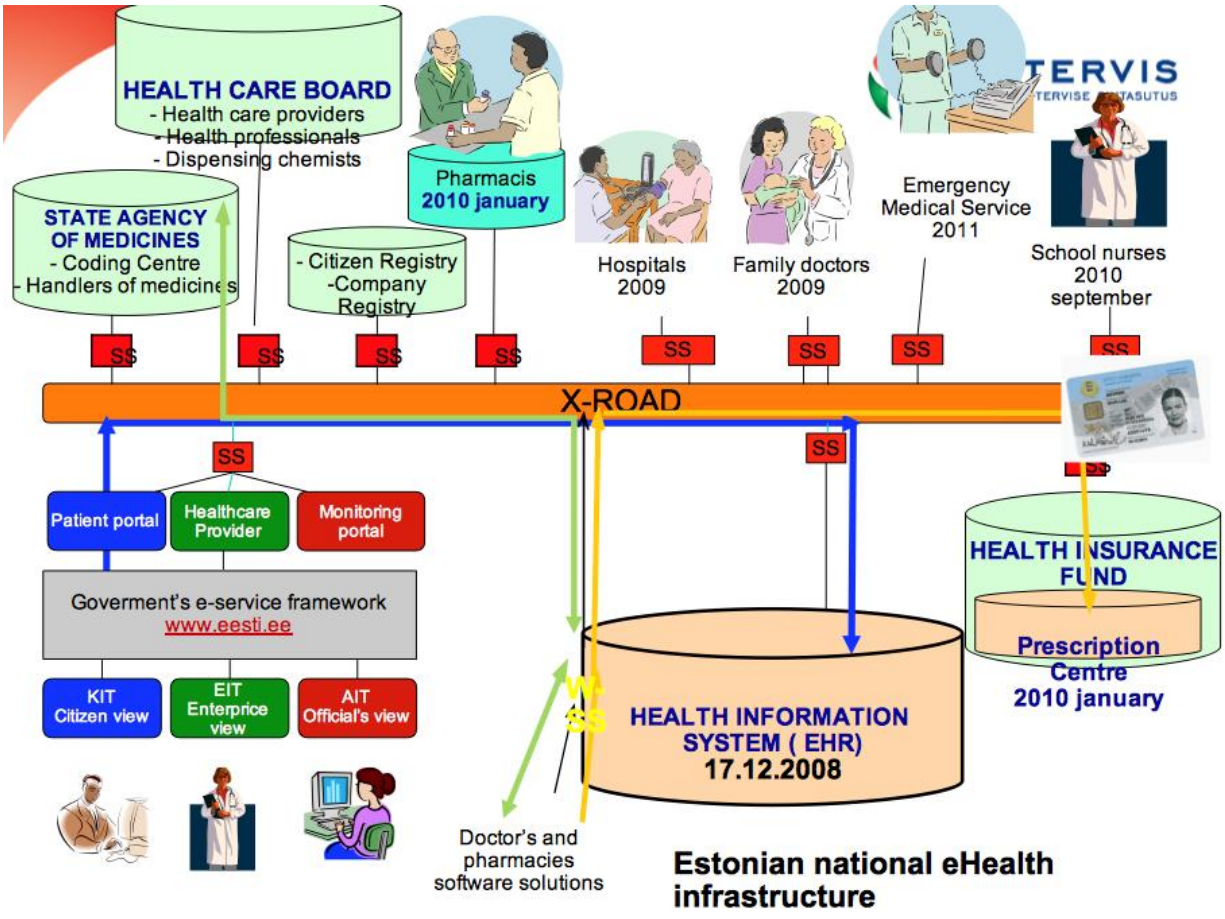
- Digital Images - The information system for digital images allows doctors to access electronic images of a medical and diagnostic nature (See Figure). Modern X-ray equipment, computer tomography and other diagnostic devices can store electronic images. The digital images system allows radiologists to split up their workload. A specialist doctor can assess an image from other health care institutions saving time and money.

- The Digital Reservations - The digital reservations information system allows patients to book an appointment to any doctor at any hospital and allows the healthcare professional to manage the queues to the doctors. This digital reservation system helps distribute the medical insurance money to the different institutions according to their performance.

- Digital Prescriptions - The system is also meant to make the writing of prescriptions on paper a thing of the past (See Figure).

  The system allows doctors to prescribe medication to the patient. The system checks the Health Insurance Fund to see if there is any discount percentage for the prescription. The prescription is then confirmed by the doctor and submitted to the register. The patient can collect his medicine from any pharmacy. The purchase is submitted to the Digital Health Record, which allows doctors to review if the patient has actually bought the medicine.

[14] Http://www.epractice.eu/en/news/5306722.



(Source: The Status of National e-Health Initiatives in Estonia, Madis Tiik 2010).

The current state of the use of the Estonian eHealth system is, according to http://www.epractice.eu/en/news/5306722: (Tiik, May 2011):

> "All end users of Estonia's EHR system can access their full personal health records. Physicians and patients have equal viewing access. And with nearly half the country's residents using the system within two years of its launch, the project appears viable for the long term."
>
> "To date, the rate of ePrescriptions in Estonia's healthcare system is around 80 %. A full 100 % of radiological images, excluding dental, are now stored in the picture archiving and communication system (PACS). More than 95 % of the country's doctors are currently using the EHR."

Also according to Mr. Tiik, in 2011 47% of the Estonian residents had actually used the eHealth system (as compared to 25% in 2010 (Madic Tiik, Eurorec.18.06.2010)).

3.6.2 European studies

3.6.2.1 epSOS Cross-border eHealth system

The main European interoperability eHealth project epSOS, Smart Open Services for European Patients, is a project that aims to design, build and evaluate a service infrastructure that demonstrates cross-border interoperability between electronic health record systems in Europe. The epSOS project provides a digital infrastructure that makes it possible to access electronic patient data stored in another country in case a patient falls ill while abroad. The basic concept is that medical institutions use a patient identifier to contact the "National Contact Point". This NCP sends a request to the NCP in the patient's home country, which then retrieves the requested document from where it is stored. EpSOS focuses on improving medical treatment of citizens while abroad by providing health professionals with the necessary patient data. The goal of the epSOS Large Scale Pilot (epSOS project website, 2012) is to:

> "Enable patients to receive medication (ePrescriptions) when they are in another European country. The medication must initially be prescribed in one of the epSOS health professional in the patient's home country."
>
> "Permit health professionals to receive the relevant, translated clinical information stored in the patient's home country ("Patient Summary"). This is only possible in case of consultation and when the patient gives his/her consent."

The connection between the different countries is gained by creating a trust between participating countries by using a common Framework Agreement (FWA) and establishing the epSOS Trusted Domain among the National Contact Points (NCP).

The agreement creates the security standards that each country would need to follow based on the ISO 27002 standards. (ISO/IEC 27002 is an information security standard published by the International Organisation for Standardisation (ISO) and by the International Electrotechnical Commission (IEC), entitled Information technology - Security techniques - Code of practice for information security management.) Each country is also required to audit their system to insure that the standards are obtained. The epSOS staff can run their audit process, but the common procedure is that each country is running independent audit processes.

The epSOS project currently allows sending Patient Summary: access to important medical data for patient treatment and cross-border use of electronic prescriptions ("ePrescription" - or "eMedication" systems), the access to the patient summary allowing only reading the record. The professional healthcare providers cannot update the records and must write their diagnostics and treatment and physically deliver it to the patient so this data can be updated in his file in his origin country (if the patient so requires). The ePrescription allows the doctor to write the prescription and the pharmacy to update the record when the patient purchases his medicine.

The epSOS project does not allow saving any data in their systems and does not create any local databases (except for the users' identities and a database containing patient consent). All data is saved locally and deleted after use.

The service providers should not be exposed to any private data. This is obtained by the legal agreement between the epSOS project and the providers. The fact that there are no databases or storages that contain private data makes it easier to enforce security. The epSOS project audits the providers to ensure that the security requirements are strictly maintained. The current status of the project is that nothing has been transferred from the Danish network over the epSOS systems due to certain technical and legal

issues. The only two countries having exchanged real data over the epSOS network so far are Greece and Italy.

The Danish coordinator for epSOS states that a number of National Contact Points are being established and that the Danish participants plan to be ready to exchange ePrescriptions in September 2012. Also in Spain, France, Austria, Germany, Italy and Greece the National Contact Points are ready for operations, although not in all countries operating in a '2-way' mode, that is, supporting both visitors from other countries (outbound mode) or supporting requests from other countries' NCPs on home land citizens.

The current discussions in the epSOS consortium suggest that the results of the STORK 2 project is used as an infrastructure to authenticate identities of Health Professionals as well as individual citizens. This requires that more countries will participate in the STORK 2 project.[15] Currently 19 countries participate, but some of the key partners in epSOS, like Denmark, are not yet part of STORK 2.

3.6.2.2 The Baltic eHealth Cross-Border eHealth system

The objectives of the Baltic eHealth project[16] were to promote the use of eHealth in rural areas of the Baltic Sea Region by creating a large transnational infrastructure for eHealth, the Baltic Sea Healthcare Network and "to illustrate that eHealth is an effective means in increasing access to healthcare of high quality in rural areas and thereby contribute to counteracting rural migration". Five countries participated in Baltic eHealth: Denmark, Estonia, Lithuania, Norway and Sweden. The Baltic eHealth project ended in September 2007. pilot project, electronic communication over the Baltic Health Network was tested in two different medical specialities: eRadiology between the Funen hospital (Denmark), the East-Tallinn Central Hospital (Estonia) and the Vilnius University Hospital (Lithuania); and eUltrasound between Norrlands University Hospital (Västerbotten County Council, Sweden) and the St. Olav's Hospital (Mid-Norway).

The infrastructure of the Baltic Health Network

The creation of the Baltic Health Network aimed at exchanging data across boundaries even if the local parts of the network had their own firewall, security, administration, and access control mechanisms. The solution to this problem was to connect the different participants' national and/or regional networks through what was called 'an agreement system'. This system was adopted from the Danish eHealth system and described in the paper The Baltic Health Network – Taking Secure, Internet-based Healthcare Networks to the Next Level (Vossa et al. 2005). The purpose of the agreement system was to ensure that an owner of an eHealth IT-system should be able to control who and on which conditions any external user could access the system.

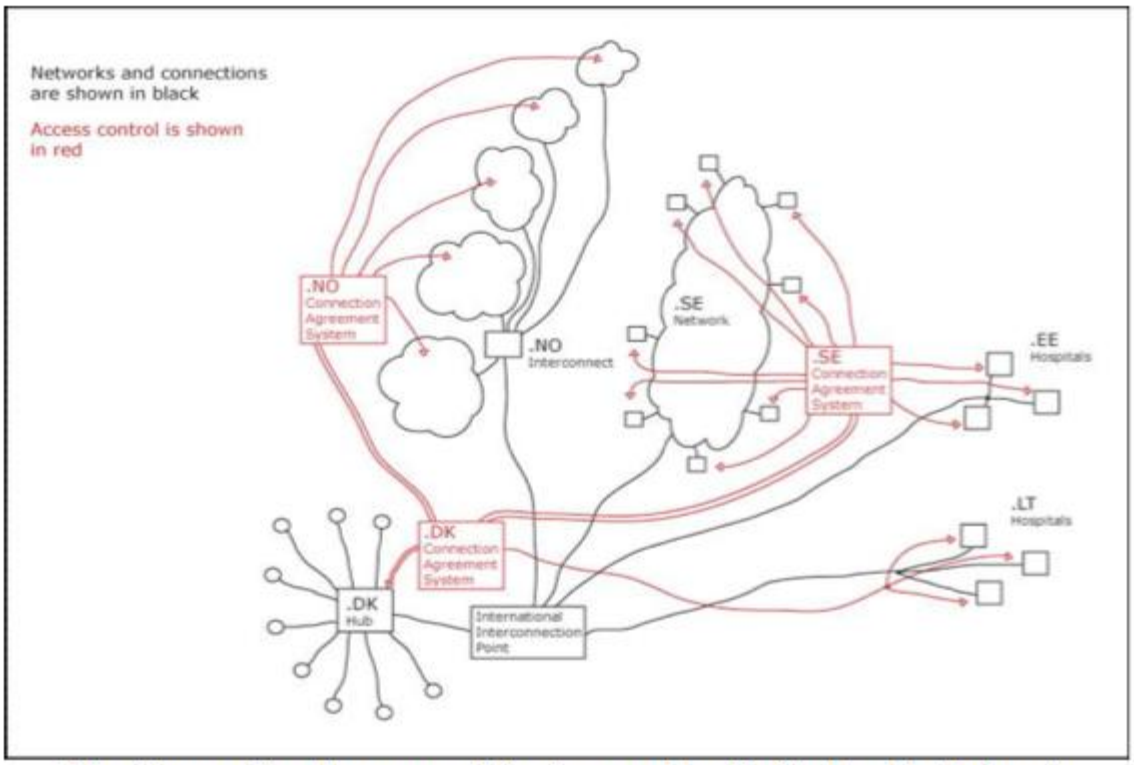
The choice to base the project on the Danish system was made due to the fact that it was running on the internet, which was not very common back then (the Swedish and Norwegian systems were private networks). The Danish system has been developed over a long period and was led by the MEDCOM organisation[17], which is the owner of the Danish Health Network. It is a joint effort between ministries, national municipal and regional organisations, and regions. MEDCOM has been pivotal in developing standards and securing interoperability across the disparate Danish EHR-systems and among other key results developed the so-called eJournal, which is a summary health record containing medical summary information on almost every Danish citizen in spite of the differently detailed systems. This has been a

[15]Http://www.eid-stork2.eu/.

[16]Http://www.baltic-e-Health.org/default.htm.

[17]http://www.medcom.dk/wm109991

substantial factor in giving every Dane access to his/her own health record through the portal Sundhed.dk[18] (sundhed=health) using the Danish Unique ID-card, NemID



The Connection Agreement System on the Baltic Health Network

(Source: Baltic e-Health, Newsletter 2, august 2005)

The security aspects of the Danish Health Network are based on a 3-level structure:

The use of VPN tunnels is the first level of security. This means that the parties can re-use the existing IP structures as the IP-addresses will be translated to a unique, national address creating the VPN-tunnel. The second level of security is an agreement system, which makes it possible for 2 parties, who want to exchange data, to open up a connection via a central hub. This connection is closed for other participants in the network. The third level of security is user identification and password. Local rules for identification and authorisation are used, which makes it possible to operate with different, local authorisation rules and access mechanisms. As the Danish Health network has been operational since 2003, it was clearly the most advanced system among the participants and was used as a model for the cross-national exchange of health data for the 2 pilots.

The Baltic Health Network (BHN) consists of more than 200 hospitals, which now very easily (from a technical point of view) can initiate collaborations with each other using the BHN. Although this project exchanges a limited type of data it was a breakthrough in several fields, the most important being the legal field in which the project demonstrated that cross-border exchange of data is possible even by using internet based platforms.

[18]https://www.sundhed.dk/

The outcome of these pilots resulted in the creation of additional follow-on projects, and especially the R-Bay project[19] is a logical extension of the radiology pilot. The R-bay EU-project under the e-Ten programme ran from 2007 to 2009 and demonstrated how an internal service market for image/radiology services could be established. The participating countries in this project were Denmark, UK, Finland, the Czech Republic, the Netherlands, Estonia, Norway, and Lithuania. Like in the Baltic Health Network, the Health Network was based on the Danish Model, and the agreement/hub services were operated by UNI*c, the Danish ICT organisation serving research and education (R-Bay report D3.2 Security and Responsibility).[20]

3.6.3 Key Security Challenges

In the following section each of the seven security challenges will be described for each of the cases. In this way it will be possible to identify key similarities or differences between the systems.

3.6.3.1 Network Security

In the network security section we will try to identify how communication between the involved parties is supported and which methodologies are used to secure this communication.

3.6.3.2 Network Security in NPfIT

The NPfIT system is built on a network called N3, which is the NHS national broadband network, facilitating the flow of information between key stakeholders in the healthcare sector in the UK. However, N3 is an 'untrusted' network, which was never designed for the transfer of patient identifiable data (PID). Because N3 was never designed to be a medium to transfer patient data, adequate security measures (such as data encryption) were never built into the network, and the security is mostly based on the physical security controls.

We can learn about the N3 network security perception from the statement at the NHS N3 website (NHS N3):

'The N3 network is a private data network which means that it is owned, run and secured by the NHS and designed to ensure*':*

6. *Confidentiality* with physical and logical restrictions to network access: The security of the infrastructure is based on the physical security that is achieved by the fact that the system is private and the network devices (routers, switches etc.) are physically secured. The second layer of defence is achieved by the usage of Firewalls that secure the network connection to external networks like the internet and other third party networks. The network is not encrypted by default and any users that want to create a secure channel between them (VPN channel) needs to create it by themselves.

TK *Integrity* – The main effort is aimed at preventing unauthorised users to access the network under the assumption that authorised parties would not damage the system or at least would always be identifiable.

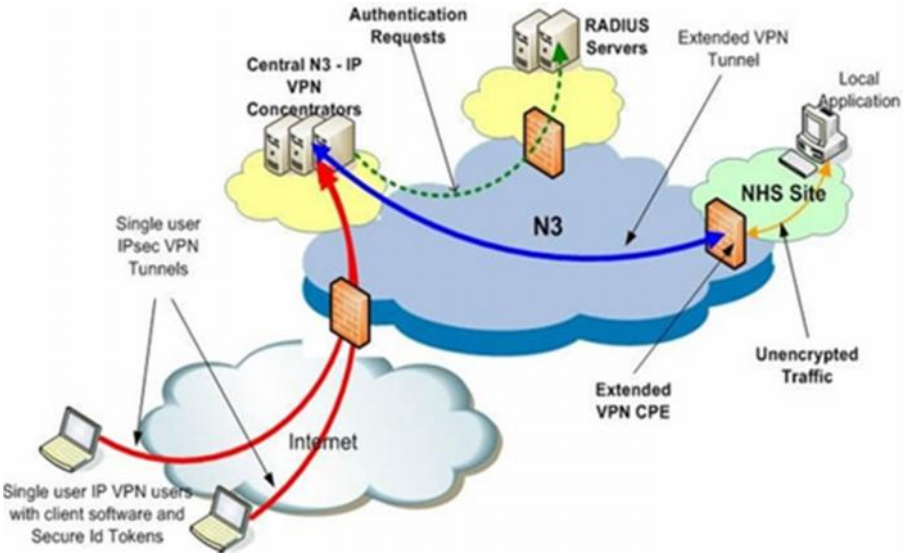
8. *Availability* **-** with resilience and fall-back built into the core network design and access services:

[19]Http://www.r-bay.org/.
[20]Http://www.r-bay.org/pages/3.

Anti-virus/Anti-worm/Denial Of Service Attack Measures

Monitors and audit the network for attacks.

The limited ability to secure the network Integrity is demonstrated from the quote at the NHS website: "The network owners and N3 service providers will make every reasonable attempt to prevent any malicious data traffic from entering the N3 network. However it is not possible to monitor and verify all data traversing N3 due to the sheer volume of traffic".



3.6.3.3 Network Security in EHR

To support the EHR, the Estonian government created a scalable Infrastructure for Inter-Organisational Data Exchange and eGovernment Applications called X-Road. This infrastructure was designed to address the need to protect the confidentiality, integrity and availability of information that is transferred by this network.

(See figure in section 3.6.2, description of the Estonian eHealth System.)

The X-Road system is run by the public internet with several security controls implemented to prevent attacks. The software layer (or application layer) most susceptible to malware attacks and the local network of the health care service provider is not part of the x-Road and is the responsibility of the health care service provider to implement securely. Health care providers access the X-road via the internet using standard PCs. Willemson & Ansper (2008) review the security aspects of the X-Road infrastructure and its ability to address the three information security attributes: Confidentiality, Integrity and Availability:

9. Confidentiality - All data exchanged through X-Road is encrypted. A standard SSL protocol is used for encryption and a two-level access control mechanism is used to prevent both external and internal attacks.

10. Integrity - Messages going out from the registers are signed. In order to be able to sign anything, certified signature keys are needed, and these are provided by a special third party – X-Road Central Agency. "All messages received over X-Road are logged and the logs are linked together using a cryptographic hash function. The intermediate hash values are periodically time-stamped.

This allows detecting the message log tampering attempts."

11. Availability - There are three security-related central services provided by the X-Road Central Agency: Certification, log management time-stamping and Directory service which secures the distribution of addresses and certificate validity information.

3.6.3.4 X-road Central Agency

The Central Agency acts as a certification authority and ensures the legal status of the information exchanged via X-Road by enforcing the stated policies. It is also responsible for planning the further development of X-Road and maintaining the security of the system.

The Central Agency is common to all Estonian eGovernment systems.

Databases

When the X-road infrastructure was developed, the question regarding the architecture of the database was raised and the Estonian citizens feared what they considered a "super database" containing all the information in one central location. The consequences of the risk that this "super database" would be compromised led to the decision of creating a distributed system with a large number of small databases and a minimum of central services.

The decentralised database approach was founded on the policy that the different ministries could collect only the relevant data necessary to operate and provide the services for the public. The approach was not to build a large database for each ministry office but to make sure that access is granted to the relevant data only if and when needed. For example the ministry of social care need only a limited amount of data in order to provide child support payments. The benefits of the system can be demonstrated from the fact that to receive child support in the past, the citizen needed to get a written approval from several ministries which meant that he needed to visit each of them, while today he can apply just by filling out a form in the national portal and the data is collected from the different databases over the X-Road infrastructure.

End user security

The end-user machine and the end-user network used to access the network is vulnerable to attacks which can affect the network itself. The security controls against those kinds of attacks are based on the authentication process by using smart cards. The usage of smart cards as an authentication method could indicate that the communication in EHR is encrypted and hence has full end-to-end security, but this is not specified in the available references. Another control mechanism is the fact that there are a limited number of services the citizen can run and the view of the data is limited to the personal data. The Web portals are used as an interface to externalise the data to the end-user. This prevents direct user-access to the databases.

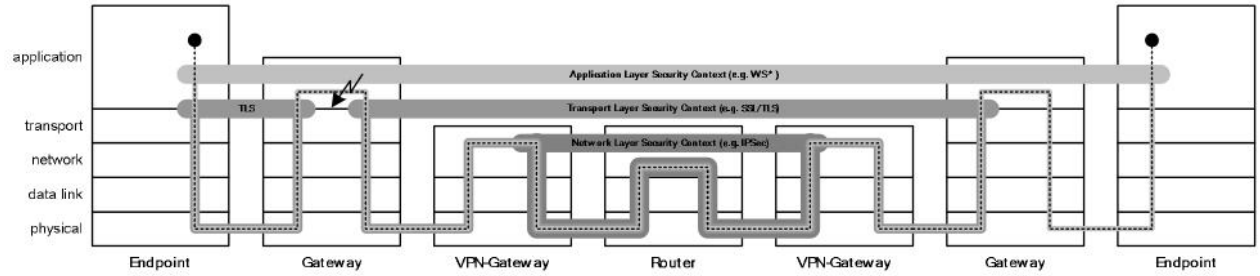
System Administrators

The inside threats from the system administrators did not change when the X-road was created and still had to be addressed. Due to the fact that the data in the network is divided between many different service providers, the potential damage is limited because no super database was created and because each database is secured independently. Another security measure implemented in X-road is a throttling of connection to key resources. This will not be a perfect counter measure to a full-blown DDoS attack but the attacker will need a substantially larger network in order to make an impact.

3.6.3.5 Network Security in epSOS

The epSOS architecture enables the use of cross-border services - such as the Patient Summary (PS) and ePrescription (eP) - and offers flexible interfaces in order to connect the eHealth infrastructure of every Participating Nation (PN)."

The epSOS architecture includes several building blocks. Some of the blocks are under the responsibility of the Participating Nation (PN) and some are developed by the project.



EpSOS - Security Realized on Different Layers of the OSI Reference Model

As epSOS is intended to connect web services between member states, the highest level of security is complete end-to-end security using Web Service Security at the application level, which can be seen in the illustration. Less sensitive data can travel unencrypted at the National level, but when crossing NCP boundaries over the internet it will still be encrypted using IPSEC.2 (Detailed description of the OSI Reference model[21] can be found here).

3.6.3.6 Network Security in the Baltic Health Network

The Baltic Health Network (BHN) is a secure cross-national network routed over the internet using VPN tunnels. The BHN is implemented using a hub-system where each involved get an IP-address on the BHN and one or more administrators are assigned at each site. The administrator has the authority to grant access from clients at their own site to the BHN or data requests from the BHN to data at the site. This is done using a web-based management interface where a client at one site can request information from a different site. In order for the connection to be established, an administrator at each end has to accept the connection and put a time frame for the connection as well. This connection is established using GRE-tunnels (Generic Routing Encapsulation) encrypted with IPSEC3. The topology makes the networks connected to BHN appear to be on a single network, but access to data will be controlled using the management interface. From the available resources it cannot be concluded how the private networks connected to the BHN is secured and if they are using encryption internally.

3.6.3.7 Conclusion

It is evident that some similarities exist between the four cases. They all implement security by creating a private network where all parties can communicate. In terms of technology, the NPfIT is the oldest and relies on perimeter defence and legal rules to protect the network. This is no longer enough to protect networks as most people have powerful network devices and can easily connect any available network port at a hospital. This reliance on perimeter security and legal rules is also seen in the BHN but with

[21]http://www.hardwaresecrets.com/article/The-OSI-Reference-Model-for-Network-Protocols/431/2

BHN the communication is encrypted and transferred on the internet. The last two solutions, EHR and epSOS, have both implemented the infrastructure in a way that makes it possible to do end-to-end encryption, by using smart cards (EHR) and encryption from data requester to data provider.

3.6.4 Interoperability

In the following section we will highlight how the systems interoperate and what standards have been implemented.

3.6.4.1 Interoperability in NPfIT

The primary means to achieve interoperability in the NPfIT system is the Interoperability Toolkit [ITK]. The ITK is a set of standards, frameworks and implementation guides to support interoperability between organisations and local health institutions.
The NHS establishes a market for individual application developers, which allow them to develop interfaces or variations of standard interfaces. This was done to deal with the major problem of many legacy local health care systems that could not communicate and share data with each other.

The ITK is based on the Health Level Seven International (HL7) standard, which is the global authority of standards for interoperability of health information technology with members in over 55 countries.

Responsibility for implementing Detailed Care Record (DCR) systems falls largely to the Local Service Providers (LSPs). In order to enable Interoperability for their system, they need to upgrade a large number of local IT systems. All hospitals in the UK were required to replace their hospital Patient Administration System (PAS), because the system needed to communicate both with national NPfIT systems and with local systems, like GP systems.

3.6.4.2 Interoperability in EHR

The Estonian IT Interoperability Framework (2006) sets out recommendations on how organisations have agreed or should agree to interact with one another. This is not a static document; it can be updated annually. This allows for adaptation of emerging standards and security measures as well as general technological progress. Adherence to the policies and specifications, however, is mandatory. It describes the underlying infrastructure, which means that public sector organisations can spend more time on building eServices (immo, 2011).

1. Integration through Central system (Opt-out)
2. HL7 v3 (extended)
3. Documents are kept in XML format (HL7 CDA)
4. All structured data fields have OID-s
5. Only final versions of clinical documents are sent into the central system

- Re-use of national infrastructure ID card for authentication and digital signature
- X-road for secure communication

The objectives of the architecture and interoperability framework are the following:

- To cut down on the expenses of public administration systems through centrally implemented middleware;
- To help achieve interoperability through the use of open standards, the Estonian PKI infrastructure and ID card, the middleware X-road for the integration of databases, and the citizens' environment KIT
- To improve coordination of the development processes of information systems for public administration and to accelerate the development of Services to achieve the independence of public information systems by following the principles of organisational, semantic and technical interoperability that are described within the framework
- To create facilities for free competition among IT companies in the area of public procurement.

The joint pan-Estonian architecture includes the following elements:

- Joint co-ordination: The Ministry of Economic Affairs and Communications will co-ordinate the development of public administration information systems
- Agreements: Common methodologies, concepts and description standards for architecture, common choices regarding standards, infrastructure, common architectural principles
- Common tools: Common software and middleware

Key policies

These are the key policy decisions which have been made (Simmo 2011):

- Public services are provided free of charge throughout the public sector. Adoption of common specifications on the Internet and WWW for all public sector information systems, as well as use of standards from the World Wide Web Consortium (W3C), the Internet Engineering Task Force (IETF) and OASIS
- Adoption of XML as the primary standard for data integration and data management for all public sector systems
- The use of multilateral solutions at the technical, semantic and organisational level for accessing of services
- Use of open standards – to reach interoperability, public sector systems need to focus on open standards
- Adoption of the browser as the key interface – all public sector information systems are to be accessible through browser-based technology; other interfaces are permitted, but only in addition to browser-based solutions
- Use of the Estonian PKI infrastructure and ID card in all authentication and authorisation processes, with the use of Internet banking authentication facilities permitted for the authentication of local residents

- All services use the secure middleware X-road (X-tee in Estonian) for data transport
- The benefits of open source software are to be considered by all public sector systems, and open source software should be considered favourably alongside proprietary alternatives
- Single point entry for citizens, entrepreneurs and officials, with additional links to eServices highly recommended.

3.6.4.3 Interoperability in epSOS

The purpose of the epSOS Interoperability Framework is to provide support and resources as necessary to enable the consistent and interoperable implementation of epSOS LSP specifications. The epSOS Interoperability Framework (2012) considers that standards implementation needs to be approached from two angles:

- Interaction with existing standards organisations – locally and internationally
- Interaction with industry including jurisdictions, international equivalents and vendor community

The epSOS project were faced with a number of interoperability issues as the countries are using different local classification systems, and also the different languages used added to the problems of semantic interoperability. To overcome these problems, the epSOS semantic utilities were developed as part of the core components. These utilities are:

Clinical Document Architectures, a so-called Master Value Set Catalogue and a Master Translation/Transcoding Catalogue to ensure proper translation of the most commonly used terms.

To complete the issues of semantic interoperability the project develops the epSOS ontology, which is a linguistic reference of all the terms used in the epSOS value sets to facilitate new participants' work in filling in their respective Master Value Set Catalogues.

3.6.4.4 Interoperability in the Baltic Health Network

The intention of the Baltic Health Network (BHN) (See Nohr et al. 2006) was to make use of specialists in other countries or regions due to the lack of local specialists or a heavy workload leading to long waiting lists for diagnosis of patients. The 2 concrete cases were the use of specialists for Radiology and for Ultrasound imaging diagnostics, where DICOM images are being transferred from e.g. a radiographer to a radiologist in a different country.

The biggest interoperability issue identified in the project was to agree on a common language and use of standard phrases used in the diagnosis. To transfer the actual health records HL7 is used.[4]

3.6.4.5 Conclusions on interoperability

Interoperability within countries as can be seen in the NPfIT and EHR is a matter of making the individual systems talk to one another, and both countries have chosen the HL7 standard. The issue for NPfIT was to make old legacy systems deliver and receive data according to HL7.

The major differences between NPfIT and EHR seems to be the decentralised approach in UK for local development of interfaces to the common system combined with a fixed definition of the contents of the central Summary Care Record, whereas the Estonian case demonstrates a built-in stepwise, much more agile approach that will include emerging standards and gradually also new types of stakeholders. This is a major difference in design as well as in implementation strategy.

When doing interoperability between countries, as can be seen in epSOS and BHN, the primary issues are common language and legal safeguards so that the patient's data is treated according to the laws in the patient's country of origin. The actual transfer of health records in both BHN and epSOS is using HL7 so the technical issues involved are limited to the issues NPfIT encountered in making the MS legacy systems understand HL7 records.

3.6.5 Identification

This section will try to establish how the individual projects have chosen to implement the identification of patients and Healthcare professionals.

3.6.5.1 Identification in NPfIT

The identity check is done according to the government-recommended standard 'e-GIF Level 3' (NHS Smart card Application Identity Verification Guidance) and includes a mandatory face-to-face meeting. It requires the individual to provide at least three forms of evidence (photo and non-photo), including proof of address. A Smart card and a passcode are issued to the healthcare professionals by the Registration Authority.

3.6.5.2 Smart Cards

The smart card contains a photo, name and a unique ID for each user. The photo is stored in a central database and is available for each health institute for verifying the user identity. Sharing passcode and smart card between users is one of the vulnerabilities of the system and the healthcare workers are warned that it is a disciplinary offence to do so. In 2011 The NHS Smart card Working Group was set up to assess the principles and policy underpinning how smart cards are used for updating and viewing electronic records. This was in response to the Ministerial review into the Content of the Summary Care Record in October 2010.

In the report (Report of the NHS Smart card Working Group – The NHS. 2010) they emphasise the importance of providing an audit trail of each user's actions. In order to satisfy this requirement each user must uniquely and securely authenticate their identity to the clinical system prior to use. They also address the following technical and operational challenges:

- For audit purposes, there should be no difference between viewing and updating records.
- User authentication should be mandatory and based on a two-factor authentication.
- They recommended using Smart cards for authentication because they are considered to be user-friendly and secure.
- The main challenge is to ensure unique authentication and therefore a clear audittrail when multiple users want to access the same machines.

The working group also identified that the time taken to authenticate the different users (mainly on the same machine) is a critical point in the cases where there are:

- more users than terminals
- enough terminals, but each is used consistently for a single purpose and a staff member moves frequently between them (e.g. fracture clinics)

- a high tempo of use (e.g. A&E) where members of staff require short but frequent accesses to different applications, using different terminals

Computer Weekly has published evidence of a culture in the NHS that is incompatible with tight security (Ritter 2007). Smart cards have been shared so that busy doctors can share PCs without having to log on and off each time, which means it can prove difficult to establish who has accessed confidential patient information. This demonstrates that a high level of security standards is not enough if the system design is cumbersome and the priorities of the staff is to take care of the patient before complying to access control mechanisms.

3.6.5.3 Identification in EHR

Unique identification of patients (Doupi et al. 2010) is an overall objective for all Estonian services. In Estonia, the Personal Identification Code (PIC) functions as a unique identifier for citizens and residents in all eGovernment services, including health. Also the Financial Sector uses this solution. Every Estonian has a PIC number, which is included in the certificates of the eID cards. PIC is provided by the Population Register. Identification or authentication processes are all done in connection to the Estonian eID Card

3.6.5.4 Unique identification of healthcare professionals

Whereas the patient is identified with the eID card, the healthcare professionals have a unique registration. For every professional, status confirmation can be requested through the MISP server (Mini Info System Portal). This portal enables professionals to identify as registered professionals and thereby obtain access to patient medical information.

Electronic ID card (eGovernment Fact sheet - Estonia - National Infrastructure)

Estonia started issuing national ID cards in January 2002. The card, which fulfils the requirements of Estonia's Digital Signatures Act, is mandatory for all Estonian citizens and residing foreigners over 15 years of age.

It is meant to be the **primary document** for identifying citizens and residents. It is used in any form of business – governmental or private communications. It is furthermore a valid travel document within the EU. Since January 1st 2007, the card issued by the Citizenship and Migration Board, has become valid for 5 years (instead of 10 years in the past). In addition to being a physical identification document, the card has advanced electronic functions facilitating secure authentication and providing a **legally binding digital signature** for public and private online services.

An electronic processor chip contains a personal data file, a certificate for authentication (along with a permanent email address Name.Surname@eesti.ee for eCommunications with the public sector), a certificate for digital signature, and their associated private keys, protected with PIN codes. The certificates contain only the holder's name and personal code (national ID code). The data file is valid as long as the identity card is, and so are the certificates, consequently they must be renewed every five years.

Common Digital Signature System

The Estonian government has implemented and released for free use a common digital signature system and was trying to play a proactive role towards the interoperability of electronic signatures in the EU (Graux et al. 2009). The framework allows signed files. The digital signature system covers: time-stamping and Online Certificate Status Protocol (OCSP); long-time validity of Digital Signature;

document format and DigiDoc, a **universal system** for giving, processing and verifying digital signatures inside Estonia. The system follows international standards (XAdES).

3.6.5.5 Identification in epSOS

The epSOS policy is that the identification (and authentication, see 6) of the users in the system is under the responsibility of the participating Member States. The Identification of the healthcare professional follows the standard of the European Health Professional Card project (HPRO Card, 2009).

The identity of a patient must be authenticated in his/her home country, even if the process is started from a service point abroad. This is directly based on the results obtained in the STORK-project[22], which was the first trans-national electronic identity project in EU, where the participating countries offered an infrastructure to ensure mutually recognised national identity cards. Currently the patients cannot take active part and do not have any access to the epSOS system, although this is part of the extensions planned for 2013.

3.6.5.6 Identification in BHN

Identification is only managed by BHN as a legally binding contract promising that the data requester is the person that he or she claims to be. Any misuse on the part of the data requester will result in the organisation being excluded from use of the network.

3.6.5.7 Conclusions on identification

Two distinct identification problems exist: one is the identification of Health Care Professionals (HCPs); the other is the identification of patients.

In order to prevent misuse and to make the proper healthcare professional accountable for any errors in treatment of patients, it is critical that the HCP can be identified and tracked.

As can be seen in the NPfIT it is of vital importance that the identification systems do not hinder the normal workflow as this will result in either sharing of identification credentials or wasting time logging in and out of systems. The first will invalidate any auditing made while the second might result in treatment of fewer patients. This problem could be addressed in the design phase of the solution, and should at least be identified and changed in the implementation phase.

Combining smart cards with efficient single sign systems can make the systems safe and efficient as can be seen in a Danish pilot project in the capitol region. Also the Estonia solution underpins the observation that identification and access control systems that are widely used and commonly accepted will help ensure compliance.

3.6.6 Usability

3.6.6.1 Usability in NPfIT

In their Independent Evaluation of the Implementation and Adoption of the National Health Service Care Records Service [2] the authors review Usability issues in the system:

[22] https://www.eid-stork.eu/

- The new eHealth system created changes in the work practices of the health care professionals. The entry of data in the system was transferred from administrative staff to clinicians, from nurses to doctors and vice versa.
- Work practices did not become "paperless" which meant that the doctors needed to write everything twice (on a paper form and to the system).
- The administrative layer added to the system in order to maintain standardisa tion created bottlenecks.
- The NHS CRS was usually portrayed as a set of clinical systems for primarily clinical users, but the direct users of the software systems studied were frequently allied health professionals and administrative staff. Their interests and concerns, however, seemed less likely to be captured or acted on as implementations went forward.

The NHS CRS systems often failed basic usability tests, which reduced the user commitment to the systems.

3.6.6.2 Usability in EHR

The Estonian health system has gained a high level of trust from the public. The main reason for that is that the system allows the user access to the citizens' information system equal to that of a ministry, a city government, or a bank.

In his article eGovernment Architecture and the Interoperability of Information Systems – Estonia's Example, Uuno Vallner, the director of Development Division, Department of State Information Systems, Ministry of Economic Affairs and Communications, Estonia, describes The Citizens' Environment (Vallner, 2004): 'Estonia's citizens' portal (KIT) provides access to restricted or confidential information that requires user authentication. The citizen portal allows people to access their personal information system. The citizen communicates with all other information systems in the state via his or her personal information system (office).'

This is supported by official data published on the Estonian website describing the level of adoption of the system by the Healthcare Professionals:

eHealth Statistics (01.05.2011)[23]

Availability of digital documents on the EHR

- Discharge letters (epicrises)- 90%
- Out-patient consultation notes - around 15%
- 4886,891 ePrescriptions were issued in 2010, which is more than 80% of all prescriptions issued in 2010
- 100% of radiological images (excl. dental) are digital and stored to the PACS
- More than 602,379 citizens have digital medical records in EHR – which equals 47% of the population

[23](Madis Tiik, 2011)

- 29,105 citizens have viewed his/her data in EHR (Patient Portal)

Individual doctors have raised concerns about parts of the the system (Digilugu) being too complicated as can be seen in

(http://www.ifg.cc/index.php?option=com_content&task=view&id=35623&Itemid=93).

As this concerns only one part of the EHR and is more focused on data entry than general usability problems with the infrastructure, this can probably be dismissed as something that will eventually be fixed.

3.6.6.3 Usability in epSOS

The epSOS project is part of the large Scale Pilot Project. On the 13th of April 2012, the epSOS piloting phase was initiated, testing the technical, semantic and legal solutions that have been developed in the epSOS project in a real-life environment over a one-year period. At this stage we cannot evaluate the level of usability of this project due to the fact that Italy and France are the only two countries that exchange data via the system. However, as the project has been prolonged to 2013 and extended to include more services, it is likely that the usability of the demonstration models has proved successful. The Danish epSOS coordinator informs us that 3 sites in Denmark are ready to go live in September 2012, and so are several other countries.

3.6.6.4 Usability in BHN

Based on the traffic graphs from "The Baltic Health Network – an important step towards cross-border inter-operability" by Claus Duedal Pedersen, it is clear that the system have been used, but the level of usability of the network and the solution as such cannot be judged. The fact that the R-Bay Radiology network project has been built on the experiences from the BHN gives us an idea of the usability of at least that part of the system.

3.6.6.5 Conclusions on Usability

Comparing the cases of NPfIT and EHR, we can see the impact of including the users of the system when designing large-scale projects such as the eHealth system. In the case of NPfIT, too strong security procedures at the HCPs end of the system resulted in no real security as HCPs ended up sharing credentials ruining the concepts of smart cards and eventually leading to the scrapping of NPfIT.

In EHR the smart cards have been adopted by the entire country and are used by professionals and patients alike, as well as for other purposes such as banking. This makes all citizens comfortable with the use of the cards and the security infrastructure. When combined with intelligent login systems that make the life of the HCPs easier, the net result is a safe and usable system.

3.6.7 Privacy

3.6.7.1 Privacy in NPfIT

NPfIT had been criticised for inadequate attention to security and patient privacy, with the Public Accounts Committee noting that "patients and doctors have understandable concerns about data security", and that the Department of Health did not have a full picture of data security across the NHS (The National Programme for IT in the NHS: Progress since 2006 (2008-9).

The main problem was the fact that the National Programme for IT in England does not have a one-document strategy for the information security of the Care Records Service, which is the national EHR system.

In their paper The NPfIT strategy for information security of care record service, the authors state that "there is no one written strategy document that clarifies how information will be secured during and after implementing shared electronic health records in the National Programme for Information Technology (NPfIT) in England (Yara & Lampros, 2011). In the paper "TRANSFORMING THE ENGLISH NHS USING INFORMATION TECHNOLOGY: THE STORY SO FAR" (Currie et al. 2011) the authors refer to the lack of faith regarding the data protection legislation and public awareness of large scale IT applications, which jeopardised data privacy and security and fuelled scepticism of the level of confidentiality of patient data stored in electronic records. They also suggest that the NPfIT project was forced to suspend its roll-out of Summary Care Records (SCRs) in 2010 when the public objected to the lack of an opt-out option.

One of the key areas examined during the House of Commons Health Committee's inquiry about The Electronic Patient Record in July 2007 was the degree to which patients will be able to control what information is contained in their SCR and who is able to access it. This has proved a complex and controversial subject with considerable media and public debate surrounding the first trials of the SCR.

Concerns over confidentiality, and the security of medical data uploaded to the NPfIT systems have also led to opposition from civil liberties campaigners such as NO2ID, the anti-database state pressure group and The Big Opt Out Campaign who provide patients with a letter to send to their doctor so that their records are withheld from the database.

3.6.7.2 Privacy in EHR

In the European Patients' Forum's publication Patients' Rights in the European Union (2009), the patient's rights are documented as they are reflected in the Estonian privacy Legislation (National Patient Rights Legislation, 2002).

"The rights and obligations of patients are laid down in the Law of Obligations Act 2001 which entered into force on 1 July 2002. Instead of focusing on the obligations of the healthcare providers, this Act specifically grants the patient clearly defined rights.

- Right to informed consent: Estonian law states that informed consent is required. Medical actions may thus only be done when the patient gives his/her consent.
- Right to information concerning own health: This right is a part of the right to informed consent. Furthermore there is no provision in the Estonian law regarding the therapeutic exception.
- Right regarding the medical records: A healthcare provider is obligated to document all health services provided to the patient. However there are no legal provisions regarding the contents of the medical file.
- Right to privacy: The obligation to respect medical secrecy is laid down in the Estonian Criminal Code. The Law of Obligations Act 2001 contains the obligation to respect the confidentiality. Providers of healthcare services shall maintain the confidentiality of information regarding the identity of patients and their state of health.
- Right to complain and compensation: Independent review of complaints of patients and compensation for damage due to malpractice is only possible through the court system, which is very complex and time consuming"

To address this legislation the following policy was implemented:

- All healthcare providers must send agreed data to EHR.
- All access rights and data usage is regulated by the law.
- ID-card for authentication and digital signature for both doctors and citizens.
- Access is enabled only to licensed medical professionals.
    - The attending doctor concept – an attending physician is a healthcare employee currently associated with patient's treatment and registered with the Health Care Board.
- Citizens can access their own data through the Patient's Portal where they can also declare their intentions and preferences. The patient has a right to set access restrictions to documents, cases of illness, and to all his/her information in the EHR. The access ban can be set to one specific document or applied to the complete data in the EHR.
- Patient's Portal allows patient representatives (adult patient, parent of an underage, legal representative, trustee) to browse a patient's health record, download documents, submit consents, update demographics data, book an appointment, and review the patient's health record usage logs via the Web.

The EHR will record information about when, how, and why the data was used (logging information), enabling citizens to monitor who has viewed their health data.

3.6.7.3 Privacy in epSOS

In the case of epSOS, privacy is addressed by design, which is implemented by designing all processes involved in the delivery of services (human as well as technical processes) around a set of 100 legal privacy requirements. In particular the patient consent has been a central point in the design of the epSOS infrastructure, following the guidelines of Privacy by Design as specified in the PRISE-project 2009.[24]

It is stated on the epSOS web site that the patient must give his/her consent before any personal data is made available to the network. The control feature of the data-controlling country is used for this process so it will follow the national policy of the specific country. This requires a privacy protection mechanism to be implemented at the national eHealth infrastructure level and not in the epSOS network per se.

The new privacy regulation may lead to a more uniform approach where eventually all countries will follow the same rules making a centrally enforced privacy protection feasible in the years to come.

Privacy enforcement and user accountability requires the existence of proper auditing and the existence of valid audit trails. The Audit Trail permits a security officer in an institution to audit activities, to assess compliance with a secure domain's policies, to detect instances of non-compliant behaviour and to facilitate detection of improper creation, access, modification and deletion of Protected Health Information (PHI).

The Danish epSOS coordinator informs us that epSOS is also in liaison with the STORK-2 project[25] - Secure idenTity acrOss boRders linKed 2.0, and that this is a follow-up on the first pan-European eID project, aimed at developing a single European electronic identification and authentication network. A number of concrete cases will be tested in the new STORK 2 project, and eHealth is one of the key application areas.

[24]http://www.prise.oeaw.ac.at/
[25]http://www.eid-stork2.eu/

It is stated in STORK 2, that WP 5.4, eHealth[26] contains the following items:

- Using the STORK eID infrastructure as the secure eID and authentication means to access the epSOS eHealth infrastructure, thus forming a bridge between the two domains of eGovernment-IDs and eHealth-IDs.
- Enabling patients to access their health data in a foreign country using their local eID mechanisms.
- Supporting mandates, i.e. patients delegating their access rights to someone else. Expanding the standard role-based situation with health care professionals (organisations or natural persons) acting on behalf of patients, the pilot will allow for explicit representation also by other persons like family members or lawyers, as applicable. Representations can be restricted for e.g. certain purposes or time periods.
- Allowing access by health care professionals from foreign emergency services to a patient summary from his home country in a "break the glass"-procedure where e.g. the patient is unconscious and the healthcare professional needs access to the patient summary without formal consent by the patient.
- Using STORK as a source for authorisation attributes from local health IT-infrastructures and applying them for authenticating Health Care Providers.
- Fostering mobile eID support as a concept that considerably facilitates eID usage at points of care.

3.6.7.4 Privacy in BHN

Privacy in BHN is accomplished primarily by policy and legally binding contracts that make the parties liable in the case of breach of the patient's privacy. Since the BHN is mostly a hub-system for connecting individual healthcare institutions, it must be assumed that privacy is ensured by the data provider only giving access to healthcare professionals who have a need-to-know requirement.

3.6.7.5 Conclusion on privacy

Privacy in the eHealth system is a critical demand from citizens in order to accept the storage of data in an electronic storage of any kind. Legislation across Europe has sought to regulate this to protect the individual.

EHR and epSOS have implemented many mechanisms to let the citizens be in control of their data, whereas the NPfIT project's primary focus was to gather as much information as possible in a central database, without identifying the proper criteria for storing, revoking the data or properly identifying who should be given access to the data. As identified previously in the network security section, NPfIT does not use encryption, which is a clear requirement to protect the privacy of patients.

BHN seems to some extent to rely on some of the same legal repercussions as NPfIT, to deter users from circumventing the security measures put in place.

In contrast to NPfIT, EHR and epSOS both have interfaces that allow the patients to control what each individual HCP can access and what is available to different government agencies.

In order for privacy by design to be implemented in practice, already from the time of decision the scope and purpose of Health solutions must clarify and specify the intentions and objectives in a clear and

[26]http://www.eid-tork2.eu/index.php?option=com_content&view=article&id=30&Itemid=31&lang=en

meaningful way; otherwise the lack of buy-in by the general public or by practitioners may jeopardise the solution.

3.6.8 Access control

3.6.8.1 Access control in NPfIT (Becker 2007)

The Access to the British health system is role-based which means that all job roles are associated with specific competencies or areas of work such as "GP" or "Psychiatry". Any healthcare professional that accesses the system must log on with one and only one job role.

In order to access the system the users need to authenticate themselves using a smart card. The smart card contains the digital job role and credentials signed by NHS-approved registration authorities (RA). Patients can access the services, for instance in order to make a clinic appointment through the web portal (HealthSpace).

Users accessing the healthcare system will only be able to view information relevant to their job role. This security control is termed a role-based access control. Users can only access information about a patient, if they have a legitimate relationship with the patient. A full audit trail will be maintained by the system, including the name of the persons who has accessed the patient information and for what purpose. This information can be viewed by the patients on request.

Registration Authorities (RA)

Any Healthcare Organisation that needs to access electronic healthcare information must set up Registration Authorities, and their rules are defined by NHS policy. The RA is responsible for verifying the identity of the healthcare professional and provide access to the relevant data on a "need to know basis".

3.6.8.2 Access Control in EHR

To enable secure access to the EHR, the Estonian countrywide data exchange platform X-Road is used. X-Road creates a user interfaces that run queries on the different relevant databases and presents them. This eliminates the need for a transition of all databases to centralise their management system (Doupi et al. 2010). A key prerequisite for the establishment of an eHealth infrastructure is the ability to uniquely identify citizens/patients and healthcare professionals by way of the Identification paragraph.

The system is divided into service providers that hold the data and service customers requiring data.

The first level of authentication is that all service customers must produce a valid certificate. In order to get access to the databases each institution needs to create an agreement with the service providers. In this agreement the service provider presents his security requirements from the consumer institution. Only if these requirements are met, will he grant access to the database.

Each provider creates his own requirements, usually based on best practices created by the state. And each provider is held legally responsible for the security of the data provided.

In eGovernment Architecture and the Interoperability of Information Systems – Estonia's Example, Uuno Vallner describes The two-level Authentication and Authorisation framework (Vallner, 2004):

Authentication Rules

The framework includes a two-level authentication. One is for the information systems and the other for the user's authentication. The information system is authenticated by a certificate that is issued by the X-road certification authority. The authentication of the users is done with the ID card, using the Internet banking (only citizens) or through certificates (only officials).

Authorisation Rules

The framework involves two levels of authorisation, one for the information systems and one for the users. The information systems are authorised by the service provider. Each service contains a list of institutions and groups of institutions that can grant access. This transfers the security responsibility from the service provider who was originally responsible for all the users in the system to the individual institutions, which are now responsible for authorising their own users.

3.6.8.3 Access control in epSOS

Authorisation

The HPRO CARD project[27] is concerned with strong authentication of health professionals and the interoperability of different Member State authentication systems. According to the ENISA study on security issues in cross-border electronic authentication, the lack of a common electronic smart card with strong authentication hampers the establishment of trust in the identity of a health professional across borders (ENISA, 2010, p. 41) and results in varying levels of confidence and security among Member States. The health care professionals in Denmark are authenticated by using NIST level 3 (2 Factor authentication), while the patients' identification is conducted by using EU's Health card or Passport number.

Access control

Access to patient Data is governed by The epSOS Access Control Policy and based on a need-to-know basis. The professional users are categorised according to their tasks and positions in the epSOS environment. There is a standard set of privileges for each role. The epSOS also uses a Policy-Based Access Control (PBAC) mechanism for decisions that are not only based on roles, but also on attributes (e.g. "Purpose of use", "Locality") as well as other modified restrictions following from patient consent.

Connection Authentication -

(See http://www.epsos.eu/technical-background/systems-standards/auditing.html)
The Audit Trail and Node Authentication Integration Profile requires the use of bi-directional certificate-based node authentication for connections to and from each node.

The DICOM, HL7, and HTML protocols all have certificate-based authentication mechanisms defined. These authenticate the nodes rather than the user. Connections to machines that are not bi-directionally node-authenticated are either prohibited or designed and verified to prevent access to Protected Health Information (PHI).

For instance, Denmark's requirements (as required in Article 29 as well) for authentication of professionals are addressing the requirements of The NIST level 3 authentications standards (a software based authentication, which requires two-factor authentications but do not enforce the usage of hardware like smart cards or token for authentication).

[27] http://www.hprocard.eu

3.6.8.4 Access control in BHN

Access to data is done through a web based request system where a data consumer can send a request to establish a connection to the data provider. System administrators at either end accept the request and establish a tunnel with an end date. Control of what the consumer can access is not the role of BHN but of the data provider.

3.6.8.5 Conclusions on access control

In three of the cases, NPfIT, EHR and epSOS we see access control implemented by using Role-based access control where each HCP is associated with a given role in order to establish which parts of the patient records they have a need-to-know requirement for. In epSOS the RBAC model used is an evolution called Policy-Based Access Control where the requested resource has a policy attached to it. As can be seen from the cases at hand a Role-based access control model is the minimum requirement, but without a clear security policy (NpfIT) this is not safe by itself.

In both EHR and epSOS policies it is defined what uses are valid for which roles and the patient is in control of which data is stored and shared.

3.6.9 Function creep

3.6.9.1 Function creep in NPfIT

The House of Commons' Health Committee's Sixth Report of Session 2006–07 regarding The Electronic Patient Record addressed the benefits of the electronic health records as "secondary uses" (SUS). In the report the committee also addressed the question of public privacy and the official policy to protect this data:

Descriptions of the "secondary uses" (SUS) including both their current and intended future form, and a discussion of the potential offered by the SUS;

- The existing governance and consent arrangements, which regulate access to data for "secondary" uses, and how these could be improved.

The House of Commons Health Committee stated that the framework for regulating access to information through the SUS was set out by officials April 26th 2007. They commented that the legal framework for the use of data for health research currently permits access through three different routes:

- Explicit consent from the patient.
- Access is permitted if information has been pseudonymised i.e. if data, which could allow an individual patient to be identified, has been removed.

Specific permission could be granted by the Patient Information Advisory Group, a body established by the 2001 Health and Social Care Act.

In spite of these regulations it seems that there is an ongoing discussion in the NHS about the extent to which the new drive for Open Government Data could apply to Health data. It is obvious that provided a patient can access his own medical record, he could benefit from second opinions from other GPs or hospitals, but since the Open Government Data will be used for private comparisons of death rates, linking of demographics to diseases etc., the discussion on function creep seems to be very real. The

recent article on 'NHS in talks to US Government about opening up Patient data'28 clearly indicates a need for a European wide discussion on conflicts between the new privacy regulation and the EU drive for 'Open Data'.

3.6.9.2 Function creep in EHR

Personal data protection art

The Personal Data Protection Act (PDPA) from 1996 protects the fundamental rights and freedoms of persons with respect to the processing of their personal data, in accordance with the right of individuals to freely obtain any information that is disseminated for public use. When conducting research on healthcare, we want to make sure that we can identify certain data that are relevant to the subject (age, sex, etc.) of the research. But at the same time, we want to prevent a full identification of the person (such as name, address, Personal Id's, etc.).

The Estonian eHealth project introduces an extension of the X-Road data exchange platform to support pseudonymisation. The extension does not rely on any centralised services, but rather uses the existing key management capabilities of the X-Road security servers.

Dr. Jan Willemson, project manager at Software Technology and Applications Competence Center has written a paper on the security of the Estonian national infrastructure, the X-road, and was a lead figure in the pseudonymisation (Willemson, 2011). In an interview we conducted with Dr. Willemson, he suggested that the security guaranties given by pseudonymisation are not very strong, as pseudonymisation just hides the identifiers of each record but all the rest of the data is kept clear. Depending on the size of the database it might be possible to identify a specific person just from the other entries in the database. Especially in a country like Estonia with a population of only 1,3 million people, your place of residence, age, education and gender may easily identify you. In many cases a full identification is not even needed, for example if an attacker wants to blackmail a person who is assumed to be on the drug addict list, a 10% assurance could be enough.

Pseudonymisation can be used in some cases where data leakage is considered bearable. For example, when the ministry of social affairs wanted to analyse the labour market in Estonia in order to take steps to lower the unemployment rate. The fact that a person is unemployed is not considered private from a legal point of view, but from the citizens point of view they might still consider it sensitive data (which they prefer not to have revealed to their immediate or their close environment). In this case, the pseudonymisation was considered an efficient method to protect privacy. In other cases when health care databases were needed for research, the solution was not satisfying and other controls were put in place. Those controls included the demand that researchers asking for access to the databases were part of a medical research institute and could prove their identity. On top of that an ethics committee must approve the research and the researches. The medical institute is required to make sure that researchers have the ability to provide a secure environment for downloading the databases. In the past such researchers gained access to the original databases but today they are given access only to the pseudonymised ones.

The process of obtaining access to the database is internet-based via the X-road infrastructure. The researcher must prove that he has the relevant credentials. When the credentials are verified, a flag is raised in all the relevant databases that are part of the researcher's query, which indicates that this

[28] http://www.computerworlduk.com/news/public-sector/3381935/nhs-in-talks-with-us-government-about-opening-up-patient-data/?goback=%2Egde_62895_member_165580511

should be pseudonymised material. All the service providers share the same private key and use it to encrypt the identifier fields (by using the same key the ID's encrypted result is kept secret but with the same value so it can be accessed through the query).

3.6.9.3 Function creep in epSOS

Function creep in epSOS is quite unlikely since the only data logged in the epSOS Framework is information about which professional connected to what and when he/she was connected. Any patient PII will be left out of this logging and hence not accessible for other purposes.

3.6.9.4 Function creep in BHN

Since the purpose of BHN is to broker the connection between involved parties/health professionals, it is unlikely that any function creep will occur from this part of the system. But from the available references it has not been clear whether any procedures have been put in place to counter this.

3.6.9.5 Conclusion on function creep

With the electronic access to citizens data there is a factual risk that data gathered for one purpose might be used in another area for which it was not intended. To prevent this, it is paramount that legislation exists to control this area and that proper safeguards are put in place such as policies on data, proper identification of data requesters, audit trails that monitor who have used the data and the ability for citizens to see this (EHR). The concept applied in EHR of splitting the electronic records up helps mitigate the risk of secondary uses as it requires acceptance from multiple data providers to aggregate all data for one citizen, and unless the requester has a legitimate reason this is unlikely to be granted.

The current discussion on opening up Government Data to private companies, merge with other sources and invite private companies to make use of hitherto publicly controlled data represent yet another possible threat to very personal information such as health, lifestyle and behaviour. The new privacy regulation should include special caveats in this respect

3.7 Observations on identified challenges - Summary

Based on the case studies of national and international eHealth experiments and solutions, the reception of these, and the broader discussion of eHealth and its governance uncovered in the beginning of this chapter, the authors wish to make a number of observations regarding the central security challenges of eGovernment as they pertain to eHealth, and discuss merging security challenges in the eHealth domain.

3.7.1 Security Challenge 1: Network security

As with all governmental ICT systems, data protection and privacy are crucial elements of any viable eHealth systems solution, putting even greater pressure on network security than in many private applications. Adding to this pressure is the fact that threats to the integrity of healthcare data are in a very literal sense a matter of life and death. This pressure translates into the necessity of a very high sense of urgency, when it comes to fundamental choices in network design for the infrastructure of eHealth systems.

Ten important points to be considered are:

i) Private vs. Public Infrastructure

One of the key elements of any eHealth system is the connection of separate systems in a safe manner. A national system connects hospitals and other health related companies like pharmacies to each other, and a cross-border system connects different countries' eHealth systems. In the National case studies, we have reviewed two private (i.e. separate, non-Internet) infrastructures, while the cross-border eHealth systems reviewed were based on the Internet as infrastructure.

In the review of the NPfIT system, which uses a private secure network based mostly on physical isolation for security, it seemed that this approach was unable to provide an appropriate level of network security. To reach a satisfactory level, any network infrastructure supporting an eHealth system must as a minimum provide centrally implemented encryption managed by the infrastructure administrators. In the case of the NPfIT, the lack of central encryption measures means that any local Hospital or General Practice will need to create their own secure connections, since the N3 network does not supply encryption. And this means that by default, data is transferred via non-secure connections, leaving the system open for digital eavesdropping. As an example of a contrary approach, the X-Road network supports full encryption at an infrastructural level, and all messages going out from the registers are signed, providing built-in data protection at an infrastructural level.

However, even in the Estonian system the local network of a hospital system also need to be protected and data on the intranet likewise encrypted to avoid eavesdropping.

ii) Application security

In all the reviewed projects there is wide usage of web applications and web services. As the application layer is the layer subjected to most attacks from malevolent outsiders, application vulnerabilities translate directly into system vulnerability.

Application layer security is difficult to attain without a strong central application security policy. Such an approach means that security is made inherent in the whole developing life cycle from the requirement stage through to design, implementation and final acceptance testing, and that training criteria are established for all developers involved. Again, establishing such a strong link between application development projects and overall network security policy requires a strong sense of urgency with regard to network security.

iii) End point security

The user end of any network makes up one of the weakest links in its security chain. User workstations are vulnerable, and can be exploited by attackers. In eHealth systems, the kinds of workstations used by professional healthcare workers and the patients, respectively, require two different sets of security considerations.

Healthcare professionals use network workstations for which it is possible to enforce strict security policies and implement security controls like anti-virus software and personal firewall systems. Another approach is to use thin clients that are less exposed to attack and easier to manage safely. This solution is doubly beneficial if the healthcare professionals need to connect to a main system as demonstrated in the Estonian case study.

Patients connecting to the eHealth system use workstations that are not part of the system and do not adhere to system security policies. They thus make up unpredictable elements in the system and import threats to it. Methods exist to decrease these threats, but with limited efficiency. One method is to check the security of the user station - e.g. whether OS and anti-virus are updated - during the connection to the system, alerting the user if he or she is not protected. The most important thing, however, is to consider this vulnerability in the course of systems design, ensuring that user access to the system is limited so that network attacks from the user end become near impossible (i.e. security by design).

No matter the technical measures taken to protect the system from user end attacks, interviewees at ENISA suggest that users' security awareness is the most essential element in any network security policy; firstly an awareness of the security risks inherent in the system and the risk on their personal data; secondly an understanding of security requirements and how to operate the system correctly. The organisation around the workstations need to take into account that the professional users are occupied with health issues and may not have neither time nor capabilities to check for status of systems protection.

The use of tele-medicine, remote surveillance of patients living in their own homes, and many projects intending to assist people with chronic diseases using medical devices, will introduce new needs for security controls, as the idea is to have these devices connected to the internet, where patient data can be stored at a hospital or with the GP.

This generates a need for new guidelines protecting the devices from eavesdropping and securing the (typical wireless) networks at the user site, preferably by encrypting the information.

Similar precautions must be taken for direct implants that can be accessed and controlled via wireless networks. The CONTINUA alliance (providers of medical devices) is aware of these issues and is developing a range of standards and guidelines[29] used to certify devices used in tele-medicine.

iv) Databases – Central vs. Decentralised

Databases are at the heart of any eHealth system. From a security point of view, the architecture of the database in the system has a major effect on overall network security. In Dutch government planning for a national electronic patient record (EPR), for example, two models of database architecture was discussed (Munnichs et al., 2012).

The first model was a Central Database, which stores all the records of the entire system. Due to the fact that any failure in the system, whether due to a malfunction or a malicious attack or even unintentional mistakes by users or IT professionals, potentially puts the entire system's integrity at risk, this model was considered unsuitable.

A second model was a decentralised architecture in which different types of data would be stored in different databases and could be joined only at the application level. In this architecture, the patient would manage the access privilege. Eventually, a third model was implemented striking a balance among the two extremes: It was decided that medical data should be managed by the health care providers concerned and made accessible by means of a national referral infrastructure. This means that a network of connected computers is created within which various fragments of the patient's record are transmitted via encrypted connections.

v) Audit Trails and Network Security

The data held by an eHealth system is a major asset, which will undoubtedly attract attackers. And while much can be done to implement security at both infrastructural and policy levels, systems developers must be prepared and able to learn from the experience of concrete attacks along the way. To this end, a centrally dictated policy for maintaining audit trails (audit logs) is an indispensable tool. The principle of security and privacy by design must include strict guidelines on audibility and surrounding procedures for new Health applications, preferably already as part of the specification of purpose and decision phase.

[29] http://www.continuaalliance.org/products/design-guidelines.html

vi) Redundancy and Scalability

In eHealth systems, data availability is critical. Systems must be able to survive and keep functioning in extreme scenarios (like natural disaster, war incidents etc.) but also distributed Denial of Service (DDoS) attacks. To achieve this, the eHealth infrastructure could be built with a redundancy of network components from communication line to storage and backups etc., and a periodically tested Disaster Recovery Plan (DRP) could be developed. As disaster situations are likely to produce extreme peaks in systems access, there is good reason to consider building scalable resources into the system architecture. (Where cloud computing may come into consideration, either as a 'private cloud' or when sufficiently safe methods have been built into a 'Public Cloud'.)

vii) Service Oriented Architecture (SOA)

Designers of eHealth systems will most likely make use of Service-Oriented Architecture (SOA), which is a set of principles and methodologies for designing and developing software in the form of interoperable (web-) services. This architecture is perfectly suited to eHealth systems that need to supply services to the users (transferring files, creating queries from databases etc.) supporting interoperability. From the case studies we learned that the epSOS project is based on a service-oriented architecture and the Estonian project has migrated to SOA as well.

However, SOA creates security issues that need to be addressed. The main premise of SOA is to erase application boundaries and technological differences. As applications are opened up, it becomes an issue how we can combine these services safely. Traditionally, security models have been hardcoded into applications and when capabilities of an application are opened up for use by other applications, the security models built into each application may not be good enough.

To deal with those issues several standards were developed. One example - WS-Security -describes three main mechanisms:

- How to sign SOAP (**Simple Object Access Protocol)** messages to assure integrity. Signed messages also provide non-repudiation.
- How to encrypt SOAP messages to assure confidentiality.
- How to attach security tokens to ascertain the sender's identity.

Open to various security tokens models, such as: X.509 certificates, Kerberos tickets, UserID/Password credentials, SAML (Security Assertion Markup Language) Assertion, Custom defined token.

Other standards to be taken into account are:

> **Security Assertion Markup Language (SAML)** an XML-based open standard for exchanging authentication and authorisation data between security domains, that is, between an identity provider (a producer of assertions) and a service provider (a consumer of assertions).
> **Extensible Access Control Markup Language (XACML)** Declarative access control policy language implemented in XML and a processing model, describing how to interpret the policies.

viii) Cross Border eHealth system and Cloud Computing

A central requirement for cross border eHealth systems is to allow users from different nations to access a large range of documents and databases. Since building infrastructure for cross border networks could be both expensive and difficult, cloud computing holds great potential in this area. Cloud computing makes it possible to outsource infrastructure build-up and maintenance to service providers while gaining a flexible model that allows rapid elasticity. Economically, the cloud model could suggest

reduced costs and a reduced length of the project. However, it also creates a wide range of critical security issues.

An interview at the National Board of eHealth indicated that Cloud computing as a solution for cross boarder eHealth system was never discussed in the epSOS project. The main reasons for not considering the cloud as a solution are the security and regulation issues that cloud computing create. Interviewees at ENISA, however, indicated that while cloud services certainly produce new types of risk (see also ENISA, 2009) and new demands for individual risk assessments, these risks should not be seen as ruling out altogether cloud based solutions to eGovernment systems, nor even in the case of vital assets such as health data. The emerging so-called hybrid cloud solutions, where sensitive data are stored in protected, private clouds and the rest in a public cloud, may prove to be useful.

While the epSOS project in practice has sought to address most of the main issues of cross-border eHealth systems, e.g. legal agreement, creation of trust between participating countries, and solving interoperability issues, the project seems to have avoided tackling important security issues, while turning security responsibilities over to the participating countries. This makes the creation of confidence in the system a potential issue that each country must solve in its communication with other countries. However, the users in epSOS are so far professionals and the general set of agreements on (minimum) security standards have to be signed by the participating countries. The European countries have different security requirements and privacy regulations which may make it difficult to attain a lasting, general confidence once patients and citizens are allowed accessing the services. Germany, for example, with its strict requirements regarding privacy, is so far prevented from actively taking part in the epSOS large scale pilot even if it is the responsibility of the (German) NCP to enforce compliance with national legislation.

This indicates that a 'baseline' of security measures should be considered across Europe, and that this baseline eventually will be raised as technology, organisation and national ICT infrastructure (such as PKI ID Mgmt) allows. An independent certification of whether this baseline has been attained could be used to lesson the burden of mutual investigations and negotiations.

We suggest that it might be wise to look at alternative approaches including implementation of the security control as part of the cross-border eHealth system. With such an approach, it would be possible at the network level to secure compliance with the highest EU security requirements, which would in turn allow each country to join the system, confident that security policies (incl. infrastructure security, identification authentication, audit trails etc.) are maintained throughout the system.

ix) Service Providers and System Administration

An eHealth system is complicated and needs fast flexible networks, large databases, and largescale storage and development of software. Some of the projects reviewed here have consulted service providers and asked them to build the eHealth system or part of it. In connection with such outsourcing, project leaders must ensure that all the project aspects are covered and properly responded to, not least what concerns security.

There are multiple ways to ensure that the service provider address the security requirement: comply with security standards like the ISO 27000 family or similar, run risk assessment process by a third party on the system and finally conduct a penetration test (i.e. practical simulation of an attack on the system) by a qualified professional for testing the security level of the system. Those kinds of tests are important not only in outsourced projects and should be part of any eHealth project.

Such projects involve many sub-contractors, including developers, advisers and network administrators, many of whom hold high level privileges that could allow undetected access to private data. Such positions need to be taken under consideration (as part of the risk assessment process) and measures

should be taken to mitigate those risks, e.g. separation of duties to eliminate the possibility for one individual to create high scale damage to the system and reliability tests for those in sensitive positions (Kowalski et al., 2008).

x) Advanced Persistent Threats

As mentioned earlier, an eHealth system could be the target of high level attacks. *Advanced Persistent Threats* (APTs) denote organised cybercrime organisations and foreign countries' military cyber-units. Attacks from APTs are characterised by their sophistication and the scale of the attack (for example getting full access to any record in the system).

Mitigating those kinds of threats involves an assessment of their relevance. Interviewees from ENISA suggested that APTs must be part of the threats model of any sensitive system. However, efforts to deal with these treats will not only represent a significant resource burden to projects, but could also complicate the operability of systems. Any project therefore needs to decide as part of its risk management whether to prioritise securing the system from APTs, considering the consequences (security, budget and operational) for the project.

One of the problems when dealing with APTs is that much of the risk assessment easily becomes speculation based. One way to minimise the influence of baseless speculation on security efforts is to ensure the inclusion of ICT professionals with direct experience in countering ATPs. The proportionality principle should be used as a guideline evaluating the potential risk of a particular type to take place as well as the potential damage that this could create. In many cases back up systems and fall back to local, isolated solutions may be the answer.

3.7.2 Challenge 2: Interoperability

Interoperability is a key factor in ensuring that eHealth data and files can be used in different member states. Any system must support a wide range of languages and different types of eHealth data. In order to achieve those goals, the system in turn needs to support a wide range of open standards.

From the case study we learned that all projects were using a wide range of available standards like the Health Level Seven (HL7). In the Estonian eHealth system we found adoption of common specifications on the Internet and WWW for all public sector information systems, as well as use of standards from the World Wide Web Consortium (W3C), the Internet Engineering Task Force (IETF) and OASIS, and adoption of XML as the primary standard for data integration and data management for all public sector systems.

The main problem, as we learned from the NPfIT project, was that some of the local systems do not support the common standards and needed to be changed. The replacement of hospital Patient Administration System (PAS) software is a vital step in creating Detailed Care Records (DCRs). These changes created usability problems due to the fact that the new system could not fully replace the old system and was not fully adopted by the users.

When implementing cross-border ePrescription system, it seems important to avoid a "digital Prescribing Babel" by safeguarding the semantic interoperability of all medication related information (substances, dosage etc.) One way to avoid this could be to establish universally accessible, uniform medicine databases taking into account the existing approaches in support of the safety and semantic interoperability of ePrescribing (INN, Drug Dictionary (WHO), and European Public Database on Medicines (EMEA)). Further measures include ensuring certification and quality labelling of ePrescribing and Medication Management software to provide the professional user with guidance and support.

3.7.3 Challenge 3: Identification

In both national eHealth system case studies smart cards have been implemented to identify the users in the system. In the NPfIT project only the health care professionals are identified in the system with a smart card dedicated to this system, while the Estonian eHealth system also identified the patients with the national ID Card.

In the Estonian case study, the main advantage of using a national ID card proved to be the great importance Estonians have come to ascribe to their personal cards due to the fact that they are used in Estonia to access both health records and bank accounts. This prevents the situations, which arose in the UK, where medical staff – attaching no particular importance to the smart cards - shared them to spare doctors from having to log on and off network workstations at each use, thereby compromising system safety at a fundamental level (Ritter 2007). (This situation could of course have been avoided by using one desktop virtualisation per professional that could only be activated by use of touch free smart cards used as standard ID cards.)

Different methods exist to authenticate the user in the system. A standard approach is to use at least two out of three independent factors (the choice being between something you know, something you have, and something you are) for authentication. With this approach, however, a second chain of security is always necessary, as each factor needs to comply with its own appropriate security standard. For example, smart cards (something you have) need to be hard to forge and to contain visually apparent safety features just as the chip on the card containing the user's sets of cryptographic private keys must comply with security standards. Any mechanism connected with the two identifying factors used, needs to be security tested to make sure it complies with the system's security requirements.

When creating a cross-border eHealth system, the main problem is creating a unified authentication system. The epSOS project addressed this problem by delegating the authentication responsibility to each member state. This solution is simple to employ and reduces the complexity of the system. However, from a security point of view it creates different levels of identification in the system according to the level of security that was used in the national system and thus adds to the overall risk inherent in the system, possibly to a level that would prove unacceptable in an overall risk assessment (see also ENISA 2010).

To counter such risk, it would seem wiser for a future cross-border eHealth system to contain a robust policy and standards regarding the identification of users in the system as well as requirements for Member States to ensure national compliance with the policy and standards as a precondition for joining the system. This is exactly the purpose of the STORK 2 project described in section 3.6.2, and the liaison between epSOS and STORK 2 sounds promising.

3.7.4 Challenge 4: Usability

Usability concerns two aspects of the eHealth systems: First, the usability of the access and identification mechanisms used to log on to the system, and second the actual usability of the applications and services. These differences should be taken into account and not mixed up, particularly when we may see the emergence of a common identification and authentication infrastructure across business domains.

One of the great challenges of developing an eHealth system is to preserve and even improve the usability of the systems. To achieve that, EHR technology must be "fit for purpose", with acceptable levels of reliability and utility in the clinical setting. All trusts adopting eHealth systems faced trade-offs between standardisation and localisation. Administrative, technical and clinical users need to provide a balance reflecting the needs of individual organisation and the national or international requirements, which are more general.

The Estonian eHealth system appears to have gained a high level of trust from the public and has been a success as far as usability is concerned. Two main factors seem to have influenced user adoption: first, strict legislation that forced all health organisation in the country to use the eHealth system, and second, the citizens' portal (KIT) which provides holders of ID cards and Internet banking clients with additional access to restricted or confidential healthcare information. Transparency, which is a part of the Estonian eGovernment policy, has helped build trust between users and the government, which is critical for maintaining high levels of systems use and acceptance. For the professionals in Estonia, however, the introduction of new applications, PAS, EHR etc. may not have been just a walk-over, but due to the relatively small number of hospitals, these types of usability problems seem to have been overcome.

Usability for the epSOS services is hard to judge at this time, as most of the pilots are just going live in September 2012. The usability of the identification/authorisation part of the system is currently based on the HPRO card (Health Professional Card, 2009). This should be part of our recommendations for a Europe-wide security baseline as this card is connected with a health professionals' certification and authorisation to practice.

For the Baltic Health Network, however, it seems that the exchange of medical imagery was quite successful, repeated during the spin off project R-Bay[30] under the eTen program.

3.7.5 Challenge 5: Privacy

Healthcare records are protected by privacy legislation and privacy will be among the highest priorities for any healthcare system, because privacy breaches equals breaches of doctor-patient confidentiality or lack of trust in Health service organisations.

Two main threats exist to data privacy. Firstly, hacking of the system by an external malicious *adversary* has always been a threat to government ICT systems. This underlines the need for network security (see "Challenge 1: Network Security" above). Secondly, threats also exist from malicious insiders with access rights to the system, who seek to get access to data with no direct relevance to their role in the system. To deal with this issue, a robust policy of access to patient data is needed for determent along with the controls that enforce this policy (See "Challenge 6: Access Controls" below). From the NPfIT case study we learned that the National programme for ICT in England did not have a one-document strategy for its information security of the Care Records Service, which is the national EHR system (Yara & Lampros 2011). That led to the NPfIT programme's bad reputation regarding the level of privacy, but much worse, it led to an invasion of privacy of celebrity patients hospitalised in the UK.

Privacy can also be increased by use of pseudonyms, as described in section 3.4 (ABC4TRUST)[31] or by introducing a policy-based filter between applications/web services and the Database as illustrated by the Hippocratic solution.[32]

Another key security control is auditing. The system must allow the administrator to audit any access to a patient record and this log should be protected in a manner that makes it impossible to delete it from the system. The audit trail needs to include a strong identifier to the person that commits the transaction and could be identified in a manner that he could not deny his responsibility for his action (accountability, non repudiation). One of the strengths that we found in the Estonian eHealth system was the ability of the patient to view the list of the healthcare professional that had entered their records.

[30] http://www.r-bay.org/

[31] https://abc4trust.eu/

[32] http://www.almaden.ibm.com/cs/projects/iis/hdb/hdb_projects.shtml.

This functionality improves the ability to detect privacy breaches and at the same time increases transparency and patients' trust in the system.

3.7.6 Challenge 6: Access Control

Access control includes several processes of **identification and authentication (A&I)**, which is the process of verifying that an identity is bound to the entity that makes an assertion or claim of identity. **Authorisation** determines what a subject can do in the system and **accountability** uses audit trails (records) and logs to associate a subject with its actions.

We already made certain observations on the A&I and accountability (see "Challenge 3: Identification") aspects. In this paragraph we will focus on authorisation. The NPfIT project is based on Role-Based Access Control (RBAC) principles. This means that users can only see those parts of the record relevant to their responsibilities and/or have limited access to certain functionalities. For example, administrative staff, in principle, would not be able to see clinical details of a patient. There were, however, a range of difficulties arising from a strict allocation of roles and workgroups determining access to the record. For instance, receptionists needed to be given the same access to all records as doctors on some occasions. The reason is that receptionists need to get some data from the electronic health record, which in this system requires full access to the record. Individuals also often moved from one workgroup to another and a range of teams worked together to provide care for one patient in multilayer and complex team arrangements that did not necessarily match the initial profile model. Thus more flexibility was required, together with individually defined access profiles.

The access control in the Estonian Health system is based on the general national ID-infrastructure, which reduces the complexity for the individual and makes it easy to apply standardised mechanisms. The use of smart cards may eventually lead to addition of more attributes that could support pseudonyms (See ABC4TRUST) or help to define roles in a role-based access system.

In the epSOS Large Scale Pilot (LSP) environment, authorisation provides information for access control mechanisms, controlling the entity's access to patient health data or other sensitive data. Access to patients' data in the epSOS LSP is governed by the epSOS LSP Access Control Policy, based on the need-to-know principle. Active entities (actors) of the epSOS LSP are categorised with respect to their tasks and positions in the epSOS LSP environment; standardised sets of privileges are assigned to each category (role). The epSOS LSP will use parts of a Policy-Based Access Control (PBAC) mechanism for decisions that are not only based on roles, but also on attributes (e.g. "Purpose of use", "Locality") as well as other modified restrictions following from patient consent. Again it should be noted that epSOS currently is focused on the Health Professionals, and that the use of a common ID infrastructure, like STORK 2, may be needed when citizens/patients are given access.

3.7.7 Challenge 7: Function creep/Secondary Use of Health Data

Health care databases help improve the health service by providing access to and analysis of data for commissioning, management and audit purposes. Specific types of research which would benefit from improved access to electronic health data include: Research into public health including both risk factors and interventions; studies looking at the side effects of particular drug treatments; and research linking maternal health with children's incidence of disease in later life.

However, the development of the Electronic Health record (EHR) will allow access to clinical data, which are timelier, better integrated and of a profoundly higher quality than those currently available. On the other hand, while conducting the research, the privacy of the patient could be compromised. In some cases, the patient will be unable to decide about being in the database. In the Estonian eHealth

system citizens can access their own data through Patient's Portal where they can also declare their intentions and preferences. The patient has a right to set access restrictions to documents, cases of illness, and to all his/her information in the EHR. The access ban can be set to one specific document or applied to the complete data in the EHR. ('opt out')

In the case studies we identified that both the NPfIT and the Estonian Health System might be enhanced by using pseudonymisation as a way to protect the privacy of the data subjects when using healthcare databases for research (e.g. secondary use of EHRs). Pseudonymisation is a procedure by which the most identifying fields within a data record are replaced by one or more artificial identifiers. There can be a single pseudonym for a collection of replaced fields or a pseudonym per replaced field. The purpose is to render the data record less identifying and thereby reduce customer or patient objections to its use. Data in this form is suitable for extensive analytics and processing in clinical or health economy research and for quality development purposes.

In the US, a legal distinction has been drawn between fully and partially pseudonymised data. Fully pseudonymised data, from which 18 specific identifiers have been removed and from which the risk of re-identification is extremely limited, is known as "de-identified" information. According to Pommerening and Reng (2004), pseudonyms represent "the golden mean between perfect anonymity and exposing the identity data" (ibid., 442). Pseudonymisation is required in cases where the correct association between a single patient's data from distinct sources is essential. Pseudonymisation also allows for re-identification in cases where a patient participating in a randomised clinical study desires information about a genetic disposition. Thus, the authors distinguish between irreversible one-way pseudonyms that allow record linkage and reversible pseudonyms that allow the re-identification of the individual (ibid.).

The Estonian project implemented an extension of the X-Road data exchange platform to support pseudonymisation. The implementation was in X-Road version 5 and thoroughly tested. The testing has shown that the users experienced virtually no performance drop because of the added pseudonymisation[33]. The provided security guarantees work in the passive model, but the researches argue that it only makes sense to consider pseudonymisation in the passive model, since open data fields do not withstand active attacks anyway.

Since the epSoS system clearly is supposed to help individual patients while abroad, and since the solution as such will not implement any databases, the risk of Function Creep is almost non-existing. The only information logged is the access log, which does not contain any sensitive data.

The Baltic Health Network aims at exchanging concrete, individual imagery for the particular patient, and the only function creep/secondary use may be the re-use of the radiology images and the ultrasound pictures for educational and research purposes. In this case it should be relatively easy to avoid storing any personal identifiable information in connection with the images, as soon as the original purpose has been fulfilled.

3.8 General Conclusions from the Study

Personal health data is sensitive information and its theft, loss, or unauthorised use or disclosure entails serious consequences for the individuals involved. The introduction of full-scale eHealth solutions, including transition from paper-based records with EHRs, supporting administrative and professional systems and the use of tele-medicine to monitor patients remotely, raises a number of important

[33]Jan Willemson, A secure and Scalable Infrastructure

questions. What are the social and economic costs, and are they acceptable? What safeguards are and should be in place to promote privacy and security? This discussion becomes more complicated when we consider cross-national health care applications, which is a consequence of greater mobility of citizens as well as professionals and the emerging use of doctors and specialists operating from other countries. This requires at least an acceptable and commonly agreed security baseline to be obtained by the European countries, and it becomes a common policy issue to ensure alignment among Member States in obtaining common security standards.

In this chapter we have provided an overview of technology related to eHealth and its European governance context. Through detailed country and European pilot studies we have analysed security challenges facing the use of electronic health records and options to mitigate the risks. The main lines of diversity investigated in the country studies pertain to

- System architecture: The use of private networks versus the internet to create a common national or international health information exchange system, and the differences between implementing a central health database versus a decentralised storage model of electronic health records

- Privacy and security governance: The adoption of a piecemeal security approach versus a centrally implemented security policy in line with an overall ICT security strategy

The UK system (NPfIT) is built on an existing private but unencrypted network, aims at a central storage of detailed records, and follows a piecemeal security approach that was not well defined nor commonly understood at the time of the decision to launch the project. The Estonian system (EHR), on the other hand, rests on a dedicated encrypted network, stores records in a decentralised manner using multiple databases, which was part of a generally accepted strategy to modernise the entire public administration where careful selection of the basic building blocks were made before an irreversible implementation plan was started.

Whereas the NPfIT signed 10 year development contracts with originally 5 local service providers which were all had strong incentives to stick to the original plan, the Estonian strategy was to allow for gradual implementations involving all the key stakeholders in a foundation, which secured mutual commitment to the progress of the EHR.[34]

The national projects illustrate the need for a precisely formulated strategy and purpose as well as well-defined and accepted security and privacy set of guidelines from the outset.

In a security perspective the main differences between the European cases are found in methods for establishment of data transfer connections between national systems. The first (epSOS) makes use of a common connection architecture transmitting encrypted data while the second (the Baltic eHealth) also allows users to exchange data to establish point-to-point secure connections (VPN channels).

An important conclusion from the cross-European eHealth projects is that the establishment of a binding security agreement between participating entities is vital.

The epSOS project in particular has spent a lot of effort in defining 'baseline' - not only for the practical interoperability aspects of prescriptions and treatments, but also for the design of security aspects for ID management, access and logging of data. The principle of NOT storing anything relating to patient data longer than practically necessary should be considered part of a baseline suggestion, along with the use of the HPRO-card for identification of health care professionals. These principles have been accepted by

[34]See http://www.e-tervis.ee/index.php/en/2012-07-22-13-35-31/organization

all participants in the (very large) epSOS network. The Baltic Health network preceded the epSOS and likewise relied on mutual recognition of agreements.

Further research will look into practical considerations of developing a central security policy baseline, how to stimulate the implementation of this and the necessary means of supporting such endeavours, for instance by inspection, certification or by other means. A related observation is the necessity of embedding privacy and security concern in the early design phase of any EHR system, and as seen in the Estonian example, preferably based on a general ID infrastructure. Also, epSOS is looking to the pan-European ID infrastructure as proposed and tested in STORK 2. It seems that a common identity structure will be much more acceptable that any ID-scheme developed domain by domain or sector by sector.

The diversity of Health systems in Europe with regard to privacy legislation, policies and local procedures and different level of compliance with EU policy recommendations - both in regard to interoperability and to data protection - represents major barriers for deployment of cross-border health services and exchange of EHR. Although there is a commonly accepted belief in the benefits of easy exchange of health data, the privacy and security risks must be addressed properly to ensure citizen trust and hence acceptance of the services.

In both pan-European projects, the actual management of the security of the system (i.e. protection of EHR records) is left to the individual members states. This evades the difficulty of handling differences in legal requirements and may potentially hamper the creation of mutual trust and confidence. This underlines the importance of building privacy, data security, data protection and auditing capabilities into the eHealth system in a proactive way and ensure that all aspects of the proposed system is taken into account, from overall architectural design and alignment with well-defined objectives and purposes to the design of applications and user interfaces to the design of network and infrastructure including databases.

We have a number of international references where privacy and security assessments are an integral part of the design, implementation and operation of a new solution. The best described cases of making these PIA (Privacy Impact Assessments) based on a well a defined security policy come from Canada - The Canada Health Infoway[35] - and from Australia where a new national Health Reform[36] was launched recently. In the Australian case, for instance, the Privacy Impact Assessment that took place before the opening of the system, and a lot of effort was put into resolving issues and communicating results to the public. (See YourHealth.gov.au)

A privacy assessment however, is not a one-time effort. Since technology improves, systems morph and functionality and data may be added, this must be a continual exercise. Also, informing citizens and politicians about possible and potential breaches, near-misses and other errors made by the hospital system must be just as much a matter of routine as airport safety reporting.

It is hardly surprising, then, that the objective of achieving technical and semantic interoperability among health information and communication systems and standards remains a challenge to the individual Member States and at EU level. As noted by the recently released eHealth Task Force report, market fragmentation in eHealth is aggravated by the lack of common approaches (e-Health Task Force Report 2012). It may be comforting to observe that almost all countries now have based their EHR on standard HL7, but still a lot of translation work needs to be done, and the epSOS efforts, however

[35] https://www.infoway-inforoute.ca/

[36] http://www.health.nt.gov.au/Health_Reform/National_Health_Reform/index.aspx

thorough, are but a small step in the right direction. As far as the technical standards are concerned, the CONTINUA alliance for tele-medicine and 'mHealth', and also the Tele industry in general, are increasingly committed to adopt common standards, although particularly in the area of mobile connectivity we still seem to be lagging in securing for instance common use of 4G devices, which will probably play a major role in future mHealth solutions.

Of relevance also for policy development is the need to address policies and procedures for harnessing multiple functionalities of EHRs such as secondary use of health data for research purposes, population health monitoring and quality monitoring. As mentioned, the threats not only come from insurance companies, employers or pharma industry, but also from the parallel drive to support 'Open Government Data', which poses a special risk when it comes to personal health data. Minimum standards for anonymization of such use should be implemented as part as the overall concept of baseline security.

The possibilities presented by cloud computing in health care also need to be investigated from a security point of view. As government clouds are developed the public cloud may be a way to solve the 'where' challenge of data storage opening up new questions of control and ownership, including possible loss of accountability and oversight.

As cloud computing is currently discussed by almost every Data Protection Agency in Europe, minimum guidelines for use of Cloud Computing in the Health Care environment should be developed. The area is hardly mature seen from a technical point of view, but, as mentioned, some basic rules could be defined, such as use of Private Clouds, possible use of Hybrid Clouds as a step ahead.

Thus, the eHealth cases clearly demonstrate the need to address security and privacy during all phases in the life cycle of any eHealth system:

From the formulation of **need and purpose (**describing outcome and risks) across the political/administrative **decision process** (specifying guidelines, rules, measurable outcomes) and the **acquisition/implementation** phase (choice of governance tools, architectural considerations and coherence between purposes, functions, applications and infrastructures), to the **operations** and - eventually - the **morphing/scrapping/disposal** of the basic system and the need for a clear decision on the **'after life'** of data generated.

3.9 References

- Article 29 Data Protection Working Party (2007). Working Document on the processing of personal data relating to health in electronic health records (EHR), 00323/07/EN, WP 131, adopted on 15 Feb 2007.
- Baltic e-Health (2007) Available at: http://www.baltic-e-Health.org/
- Becker, M. Y. (2007). "Information Governance in NHS's NPfIT: A Case for Policy Specification". In: International Journal of Medical Informatics. Vol. 76, Issue 5, pp. 432-437.
- Canada Health Infoway. (2005). Electronic Health Record Infostructure (EHRi) Privacy and Security Conceptual Architecture. Available at: https://knowledge.infoway-inforoute.ca/EHRSRA/doc/EHR-Privacy-Security.pdf.
- Commonwealth Department of Health and Ageing, Australia:
- Privacy Impact Assessment Report - Personally Controlled Electronic Health Record (nov. 15, 2011)
- Digital Agenda web portal, Pillar VII: ICT for Social Challenges, available at: http://ec.europa.eu/information_society/newsroom/cf/pillar.cfm?pillar_id=49.

- Currie, W., Finnegan, D., Gozman, D., Koshy M. (2011). Transforming the English NHS using information technology: The story so far. European, Mediterranean & Middle Eastern Conference on Information Systems.
- Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross--border healthcare (OJ L 88, 4.4.2011, p45).
- 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 (OJ L 281, 23.11.1995, p.31).
- Doosselaere, C., Herveg, J., Silber, D., and Wilson, P. (2008). Legally e-Health - Putting e-Health in its European Legal Context, study report on behalf of DG Information Society and Media, European Commission, available at: http://www.epractice.eu/files/media/media1971.pdf
- Doupi, P., Renko, E., Giest, S., Heywood, J., Dumortier, J. (2010). Country Brief: Estonia
- e-Government Factsheet - Estonia - National Infrastructure from the epractice.eu website available at: http://www.epractice.eu/en/document/288219
- e-Health Task Force Report (2007). Accelerating the Development of the e-Health market in Europe, Brussels: European Communities. Available at: http://ec.europa.eu/information_society/activities/health/policy/lmi_e-Health/index_en.htm
- e-Health Task Force Report (2012). Redesigning Health in Europe for 2020, Brussels: European Communities. Available at: http://ec.europa.eu/information_society/activities/health/docs/policy/taskforce/redesigning_health-eu-for2020-ehtf-report2012.pdf
- e-Health Network of National Competent Authorities 2012. Conclusions on eID EU Governance for e-Health Services, e-Health Governance Initiative, internal document.
- ENISA (2009). EFR Pilot ''Being diabetic in 2011'' Identifying emerging and future risks in remote health monitoring and treatment. Available at: http://www.enisa.europa.eu/activities/risk-management/files/deliverables/enisa_being_diabetic_2011_Annex2.pdf
- ENISA (2010). Security Issues in Cross-border Electronic Authentication. Risk Assessment Report. Available at:
- epSOS project website (2012). Available at http://www.epsos.eu/.
- epSOS Technical Aspects (2012). Available at: http://www.epsos.eu/fileadmin/content/pdf/epSOS_Technical_Aspects_Factsheet.pdf.
- epSOS Interoperability Framework (2012). Available at: http://www.epsos.eu/uploads/tx_epsosfileshare/D3.3.3_epSOS_Final_Interoperability_Framework_01.pdf.
- Estonian IT Interoperability Framework (2006). Available at: http://www.riso.ee/en/information-policy/interoperability/.
- European Commission Thematic Portal ICT for Health, available at: http://ec.europa.eu/information_society/activities/health/policy/interoperability/index_en.htm, retrieved August 10, 2012.
- European Commission (2012a). Draft Proposal for a Regulation of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market, available from http://ec.europa.eu/information_society/policy/esignature/eu_legislation/regulation/index_en.htm
- European Commission (2012b). Proposal for a European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM/2012/011 final.

- European Commission (2010). A Digital Agenda for Europe, Brussels. COM (2010) 245, available at: http://ec.europa.eu/information_society/digital-agenda/documents/digital-agenda-communication-en.pdf.
- European Commission (2004). e-Health - making healthcare better for European citizens: An action plan for a European e-Health Area. Brussels: COM(2004)356 final.
- European Commission (2008). Commission Recommendation on cross-border interoperability of electronic health record systems COM(2008)3282 final, 02.07.2008.
- Frost & Sullivan Market Insight (2010). Smart Cards for Healthcare in Europe, available at: http://www.frost.com/prod/servlet/market-insight-print.pag?docid=200942088, retrieved August 24 2012.
- Graux, H., Jossin, B., Lambert, G., Meyvis E.(2009). Study on Mutual Recognition of eSignatures: update of Country Profiles. Estonian Country Report. Available at: http://ec.europa.eu/idabc/servlets/Doc7bd5.pdf?id=32323.
- Gunter, T.D. and Terry, N.P., (2005). The Emergence of National Electronic Health Record Architectures in the United States and Australia: Models, Costs, and Questions in J Med Internet Res 7(1).
- House of Commons Health Committee (2007). House of Commons Health Committee inquiry: Electronic patient record, available at: http://www.publications.parliament.uk/pa/cm200607/cmselect/cmhealth/422/422.pdf.
- HPRO Card Project website (2009). Available at: http://www.hprocard.eu/
- Iakovidis I. (1998). "Towards Personal Health Record: Current situation, obstacles and trends in implementation of Electronic Healthcare Records in Europe", International Journal of Medical Informatics vol. 52 no. 128, pp. 105 –117.
- Kowalski et al. (2008). Insider Threat Study: Illicit Cyber Activity in the Government Sector, U.S. Secret Service and CERT/SEI. Available at: http://www.cert.org/insider_threat/study.html?goback=%2Egde_1836487_member_109548276 Leego, E., Hansson, Leego & Partner. (2005). "E-Health Initiatives in Estonia" In: Baltic IT&T Review.Vol.37, no.2
- Munnichs, G., Schuijff M., Besters M. (editors) (2012) "Databases. The promises of ICT, the hunger for information, and digital autonomy" Rathenau Instituut.
- National Patient Rights Legislation. ESTONIA - Law of Obligations Act (2002). http://www.legaltext.ee/text/en/X30085K2.htm
- NHS Connecting for Health. Available at: http://www.connectingforhealth.nhs.uk/
- NHS N3. Available at: http://n3.nhs.uk/
- NHS Smartcard Application Identity Verification Guidance (eGIf Level 3 Compliance). Available at: http://www.lpc-online.org.uk/bkpage/files/145/resources/eps2010/nhs_smartcard_app_identity_verification_guidance.pdf
- Nohr, L. E. et al, (2006). Cross bordere-Health in the Baltic Sea Region – what issues should be considered? Available at: http://www.baltic-e-Health.org/intern/wp1/Guidelines/Cross_border_e-Health_in_the_Baltic_Sea%20_Region_report_june2006.pdf.
- Pommerening K, Reng M. (2004). Secondary use of the EHR via pseudonymisation. *Stud Health Technol Inform*. 103: 441-6.
- Report of the NHS Smartcard Working Group – The NHS (2010). available at: http://www.lpc-online.org.uk/bkpage/files/145/resources/eps2010/nhs_smartcard_app_identity_verification_guidance.pdf:
- Ritter, T. (2007). Smartcard sharing by an NHS trust - a breach of IT security or a practical way around slow access to the NHS Care Records Service? Available at:

http://www.computerweekly.com/blogs/public-sector/2007/01/smartcard-sharing-by-an-nhs-tr-1.html

- Patients' Rights in the European Union (2009). European Patients' Forum, available at: http://www.eu-patient.eu/Documents/Projects/Valueplus/Patients_Rights.pdf
- Simmo, P. (2011). The Estonian e-Health experience - strategy and results - Estonian e-Health Foundation available at:
- http://www.kith.no/upload/6407/HelsIT-2011_T2-5_Piret_Simmo.pdf
- Stroetmann, K.; Artmann, J.; Stroetmann, V. et al. (2011). European countries on their journey towards national e-Health infrastructures. Luxembourg: Office for Official Publications of the European Communities, 2011. Available at: http://www.e-Health-strategies.eu/report/e-Health_Strategies_Final_Report_Web.pdf.
- Vallner, U. (2004). "E-Government Architecture and the Interoperability of Information Systems – Estonia's Example" In: Baltic IT&T Review.Vol. 34, no. 3
- Vossa, H., Heimlyb, V., Holm Sjögren L. (2005). "The Baltic Health Network – Taking Secure, Internet-based Healthcare Networks to the Next Level" In: Studies in Health Technology and Informatics.Vol. 116:pp. 421-6.
- Yara, M., Lampros, S. (2011). The Npfit strategy for information security of care record service. European, Mediterranean & Middle Eastern Conference on Information Systems.
- Willemson, J. (2011) Pseudonymization Service for X-Road e-Government Data Exchange Layer, EGOVIS'11, Proceedings of the Second international conference on Electronic government and the information systems perspective. Available at: http://research.cyber.ee/~jan/publ/egovis_pseud.pdf
- Willemson, J., Ansper, A. (2008). A Secure and Scalable Infrastructure for Inter-Organizational Data Exchange and e-Government Applications. Third International Conference on Availability, Reliability and Security. ARES 08. Available at: http://research.cyber.ee/~jan/publ/xroadares07final.pdf.

Appendix 1: Experts Interviewed regarding e-Health records

A few explorative, informal interviews were conducted, including some email exchange. Individuals consulted include:

- Anni Buhr, Programme Manager, Danish National Board of e-Health
- Pia Jespersen, Special Adviser, Standards and Enterprise Architecture Division, National Board of e-Health and National Contact Point (NCP) for epSOS.
- Kenneth Bøgelund Ahrensberger, Special Adviser, Division of National Board of e-Health and Member of e-Health Network of National Competent Authorities.
- Jan Willemson, Project Manager in Software Technology and Applications Competence Center, Estonia.
- Barbara Daskala, CISSP, CISA, Information Security & Risk Management, European Network and Information Security Agency (ENISA).
- Charlotte Bagger Tranberg, Associate Professor in EU Law and Technology Law at the Department of Law at Aalborg University, Denmark
- Asger Andreasen, Chief Advisor and Head of Brussels Office at Danish Regions
- Claus Duedal Pedersen, Project Manager Odense Hospital (Baltic e-Health Project)
- Niels Rossing, MD, Consultant - Danish Centre for Health Telematics
- Vincent Tassy, Project Manager, IBM La Gaude e-Health Centre
- Marit Hansen, Deputy Privacy & Information Commissioner of Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein.

Appendix 2 : Summary table and conclusions from eHealth case studies

	NPfIT – UK	Estonian EHR	epSOS	Baltic eHealth BHN
Network Security	+ Physical and logical restrictions to N3 + Firewalls to secure network connection to Internet + Resilience and fall-back built into core network - Network is not encrypted - Auditing of data traffic 'not possible – because of volume'	+ All data exchanged through x-Road is en-crypted + All messages across X-Road are logged. Time stamped and encrypted + Distributed DM's + Throttling of connect-ion to distr. resources minimise risk of DDOS - End user machines and local networks are not encrypted - Access to local PC's not secured - Distributed Databa-ses are secured inde-pendently	+ National Connectors act as interfaces to local health networks under a common agreement scheme + Connections be-tween NCPs are encrypted IPSEC.2 + Web services proto-cols are used to ac-cess web services in other national net-works + Audit trail provided as a core element - Local network security may vary	+ Secure cross national network using VPN tunnels + An administrator at each end has to accept the VPN connection. + Time frame alloca-ted to each session + The established Danish health network used as base for NW - Local networks may have different security infrastructure. ? Unclear if local net-works use encryption
Interoperability	+ Interoperability toolkit based on HL7 + Interfaces devel-oped - Detailed care record systems left with local authorities -huge differences between local systems	+ Mandatory to adhere to common standards and inte-gration via central eID systems & PKI + HL7V3, XML, W3C as mandatory stan-dards + All services use the x-Road	+Develop Clinical Document Architec-ture and translating and trans-coding Master Value sets + epSOS Ontology, linguistic reference of terms - Different local classi- fications schemes - Huge number of participating countries and no of languages	+ Basic interopera-bility and exchange of data via defined standards (DICOM Images) + Agreement between participants to use common terminology - agree on semantic interoperability for standard phrases used for diagnosis

	need to be replaced			
Identification	+ 3 forms of evidence for issuance of ID-card (eGif level3) + Smart card and passcode for HC professionals - More prof. users than terminals, sharing of ID cards jeopardise audit trail - General citizen mistrust of centrally mandated ID-systems	+ Use of common ID-card (PIC) + Unique ID card for HC professionals + ID card contains a legally binding signature + Common infrastructure for time stamping and check of ID validity	+ ID of professional HC personal based on HPRO-card (strong authorisation) -ID of patients rely on the local authentication system that varies between countries (STORK 2 should be minimum recommendation)	+ The health professionals accessing the network are authenticated through home country authorisation systems + The Local user identification is subject to common agreement. (a minimum requirement= - Different ID-standards used in each country
Usability	- General lack of trust by citizens - Lack of buy-in by local Health authorities (centralisation) - Major change of daily work routines for all staff - Still need for paper documentation - Heavy admin tasks - Implementation did not recognise user needs and input	+ High adoption rate by the public because of common ID- giving access to banks, public records, health info for the individu- als + High usage of system (discharge, ePrescriptions, digital medical records) - Low level of patients have reviewed their data in EHR	+ Large number of partners/countries have joined the epSOS project - Few pilots - Only limited, practical experience in exchange of patient summary and prescriptions.	+ The use of the exchange of radiology and ultrasound was generally accepted by the professionals. + A follow-on project R-Bay added a large no of users to same type of infrastructure - No detailed record on usability in the BHN
Privacy	- No defined strategy for information security - No opt-Out option - Citizens lack of trust - General mistrust in UK population to	+ Consent mechanisms built into solution + Patient rights clearly defined + access rights to own data	+ Privacy by design: patient consent + Detailed set of guidelines + audit trail to detect any access to PHI + epSOS will align	+ All participants sign contract to adhere to EU Privacy rules and accept liability in case of breech(only access based on need-to-know) + BHN is mainly a hub-system to connect

	central databases	+ Opt-out option + Extended logging allow patient to view who has accessed data	with STORK 2 using a common eID-system - National privacy protection systems vary in quality	HC institu-ions - Practical solution to privacy is depending on local data provider
Access Control	+ Role based access by professionals + Smart Card for HC professionals signed by NHS RA. + Access to limited services by patients - Only one role at a time - Sharing of smart cards a major issue	+ Each institution creates agreement with central authority on use of certificates + The IT systems are authenticated by a certificate issued by the x-road authority + Authentication of users qualified by Estonian PKI and authentication done via eID card	+ the HPRO card used for strong authentica-tion of Health Profes-sionals + The HC Profs in each country are authenticated by using NIST level 3 (typically) + Patient identifica-tion via EU Health Card or passport number - Variations among countries' certification procedures - EU Health Card does not contain photo or biometrics	+ Web based request sent by user to data provider and accepted by SYSADM at either end to create VPN + Data provider ensures authentica-tion - Variations in authentication rules in each country/ data provider
Function Creep/ Secondary use of EHR	+ Governance and consent rules to allow 'secondary use' + Explicit consent from patient + Pseudymisation required to remove PI	+ Use of pseudonyms to help make research based on actual data + Researchers credentials used to check access rights - For small popula-tions use of pseudo-nyms may not be sufficient to hide ID	+ Very unlikely because only data logged in epSOS is which professional connected + Any patient PII is left out of logging	+ As purpose is to have profs assist in concrete cases, it is unlikely that function creep should occur - Cannot be judged from case if and which procedures to prevent FC are implemented

Overview - Findings from eHealth cases

Summary:

1. Network security: All aim to create private networks, UK via private network, other via VPN Tunnels. Perimeter defense (NPfIT and partly BHN) is not enough, and EHR and epSOS are both examples of (potential) end-to-end secure networks.

2. Interoperability: All cases are based on HL7, but this is only a partial step on the road. Semantic interoperability is one of epSOS's main objectives and should be promoted further.

The (limited) goal of interoperability for radiology and ultrasound in BHN seems to have been fulfilled due to common standards and descriptors.

3. Identification: Identification via smart card for professionals seem to be well on its way and based on common rules for certification of health professionals (HPRO-card). The eID of Estonia is at the forefront in the EU and should be used as a role model. It is also part of STORK 2, and the general concept of a cross-sector personal eID-system based on smart cards should be mandatory in EU.

4. Usability: Usability of the security parts of the EHR systems must be viewed separately from the application and system user interface. There is a balance between strong security controls and usability, which may jeopardise patient security if not designed properly. Single sign on is essential for fast treatments. Usability improves when similar security systems are used in a generic way, i.e. across domains, countries and applications.

5. Privacy: Privacy and general trust is a critical requirement. The new EU regulation will help gain citizens' accept by a common set of regulations, but it requires respect for transparency and citizens' access to own data. Patient control, opt-out and pseudonymisation (as in the Estonian case) is a must.

6. Access control: Access is a function of identification and authorisation. Once identification is done, the authorisation mechanism should be fast and effective and require a minimum of maintenance; hence the smart card model (for Professionals as well as for citizens/patients) should contain sufficient information regarding generic roles. NIST 3 standards should be followed. It is important that the authorisation process is coupled directly with audit logging.

7. Function creep/secondary use of data: The health record has a huge potential value for research and for general improvements of treatments. However, access to detailed data should either be granted subject to patient consent or by pseudonymisation (EHR supports Ps). Standards for pesudonymisation should be generally accepted across EU. The epSOS project seems to have only a minimal risk because no PII will be logged.

4 CASE STUDY: EPASSPORT

Authors: Max Snijder, European Biometrics Group & Linda Kool, Geert Munnichs, The Rathenau Institute

4.1 Introduction

4.1.1 Background

All European Member States are obliged to integrate biometric data into passports and travel documents. This is defined in Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States. In biometric passports, also known as ePassports, identifiers such as the facial scan and fingerprints of the passport holder are stored on an RFID chip contained within the travel document. The goal is to combat passport fraud and reach one internationally harmonized identification system. But the way in which the biometric data is gathered, stored and used, differs among Member States and it is difficult to implement the same level of data security concerning scanning devices and protocols. Some Member States opt for decentralized storage of the data for reasons of privacy and data protection; others store the data centrally. Some use the stored biometric data only for one-on-one verification to prevent fraud, while others want to use it to identify crime suspects and combat terrorism. Member states also diverge in their implementation phases: some are already fully functional, whereas others are still at the beginning stages.

The goal of this case study is to address issues regarding the European implementation of the ePassport regulation and the security challenges central to the overall research project. These include network security, interoperability, identification, usability, privacy, access control and function creep. The study considers implementation at the European level as well as within a number of individual states in order to illustrate the level of alignment and harmonization.

4.1.2 Scope of the study

This study will look into the implementation of Council Regulation EC No 2252/2004. It will not give a detailed overview of all 27 Member States, but rather will exemplify the diversity of the implementation schemes by describing several individual Member States, and address the consequences of this diversity for the research issues stated above. The selected countries are: Czech Republic, France, Germany, Italy, The Netherlands, Norway and Slovenia. The selection of countries is based on geographical diversity, differences in the implementation process as well as differences in legislation regarding the purposes the biometric data should serve.

The sources used in this study to obtain the country information have been desk research, questionnaires and interviews. The interviews have been done primarily by email. To obtain information from the selected European member states a questionnaire was sent out addressing the following topics: policy, implementation and roadmaps and future development of capabilities. In total twelve organisations have been contacted. Although contact persons of most selected countries felt free to speak about the biometric passport informally, only a few decided to respond formally. Other relevant sources are mentioned in the footers. General references and documentation is listed in Chapter 5 of the study. Contacted organizations have been:

Czech Republic	Czech National Security Agency
	University of Brno
France	Commission nationale de l'informatique et des libertés (CNIL)
	Conseil Constitutionnel
Germany	Bundesministerium des Innern (BMI)
	Bundesamt für Sicherheit in der Informationstechnik (BSI)
Italy	National Agency for the Digitalisation of the Italian Public Administration (DIGIT AP)
The Netherlands	Dutch Ministry of Internal Affairs
Norway	Ministry of Justice
	National Identity and Docuementation Centre (NID Norway)
Slovenia	Ministry of the Interior
	National Information Commissioner

4.2 European framework

Since August 2006, Council Regulation EC No 2252/2004 has required the 27 Member States of the EU to issue ePassports that contain a digital facial image. Since June 2009 the Regulation requires Member States to issue second generation ePassports that include two fingerprints (Council Regulation (EC) No 444/2009). These regulations represent the European endorsement of a global standard for machine readable passports, issued by the International Civil Aviation Organization (ICAO Doc 9303).

The policy objective was '…to achieve enhanced harmonized security standards for passports and travel documents to protect against falsification. At the same time biometric identifiers should be integrated in the passport or travel document in order to establish a reliable link between the genuine holder and the document' (EC No 2252/2004). The biometric information stored in the ePassport chip would make it easier to verify the authenticity of the passport and strengthen the link between the passport and the legitimate holder of the passport. In order to better understand the impact of this decision and the challenges it creates, a short introduction to biometrics is needed.

4.2.1 Biometrics: The technology

Biometrics is the technology that is used to identify a person based on his or her physical characteristics, such as a fingerprint or iris. There are many different biometric characteristics but this study will focus on facial image and fingerprint because the ePassport includes these characteristics. The use of biometrics stems from the domain of law enforcement, where fingerprints and faces of convicted criminals and suspects are matched against a database of biometric data in order to establish or confirm their identity. The following features characterize the use of biometrics:

Biometric systems are inherently based on probability. In a biometric system, a digital image of a physical identifier (e.g. face, finger, iris) is analysed using special software to extract its relevant

characteristics which are then stored as a digital template. But two images - the stored template and the 'live' version - are never exactly the same, while the extraction process does not always result in the same template. This can be caused by different conditions (lighting, amount of sweat, ageing) for example, or the use of different equipment. This means that a system must calculate to what extent two templates of the same person are in fact a 'match'. The system therefore returns a probability score that a match has been found. That means that there will always be a theoretical and practical chance that the system fails to make a match. As a consequence, biometric systems always have to deal with error rates. The operator of the system decides on the thresholds that determine a match. Assessing the failures and accuracy based on certain thresholds requires continuous monitoring and consideration of human oversight.

When the system can't find a match, the failure might be due to an operational malfunction, human error or fraud. That implies that, in practice, an assessment is needed to determine whether a non-match is caused by a genuine technical failure or if a failure is caused by human error. As a result a continuous interaction between the system, the data subject and the operator is needed.

These features relate to the performance of a biometric system and impact on the procedures that need to be implemented. 'Performance' is usually broken down into two major aspects: accuracy and throughput. Accuracy is expressed as a number of error rates, such as False Accept Rate (FAR), False Reject Rate (FRR) and Failure to Enroll (FTE).

False Accept Rate is the chance that the system matches two templates that are in fact no match. These are known as 'false positives'.

False Reject Rate is the chance the system does not detect a match between two templates that are in fact a match. These are known as 'false negatives'.

Failure to Enrol is the chance the system cannot successfully create a template from a biometric characteristic, for example because of a low quality photo of a face.

A high rate of mistakes will make a biometric system inefficient and unreliable. A reliable biometric system makes high demands of the quality of the biometric data. Due to the statistical nature of the biometric matching process and to the various causes of failures, the FAR and FRR need to be placed into the context of their application in order to fully understand the performance of a specific biometric system. The FAR and FRR are negatively influenced by factors as low quality enrolment, malfunction of the sensor, harsh environmental conditions, manipulation, fraud, or following wrong procedures (UK Biometrics Working Group 2002).

In principle, each acceptance or rejection should be analysed in order to judge whether they are 'true' or not. Certain applications need an instant interpretation (e.g. passport control). For other applications an offline interpretation of a match or non-match (Eurodac – the European system for comparing fingerprints of asylum seekers and some categories of illegal immigrants) is sufficient.

In practice this leads to two additional performance rates: the **True Accept Rate** (TAR) and the **True Reject Rate** (TRR). The TAR expresses the number of correct matches, the TRR the number of correct rejections. In order to determine the TAR or the TRR many technical and non-technical aspects need to be assessed. This implies that organizational aspects and human involvement have a significant impact on the performance of a biometric system (see also Ashbourn 2005, p. 10).

4.2.1.1 Identification versus verification

Biometric **identification** means the process of determining the identity of an individual, when unknown (for example if fingerprints have been found on a crime scene) or where an identity claim is considered to be unreliable. This identification process needs a central database in which the biometric templates and personal information (like name, address, race, etc.) are stored and linked. Via a so called 'one-to-many' search (1:n), the database looks for a match with the biometric data found (e.g. at the crime scene).

Biometric **verification** is the process of checking if an identity claim (e.g. by showing a passport) is correct. The biometric reference image is locally stored on a smartcard, token or passport. The verification of the biometric image takes places via a ''one to one'' (1:1) comparison of the 'live' image and the reference image. In this case the biometric data does not lead to identification; it is only used for verifying an identity claim.

The purpose of the biometric data – whether it is to be used for identification or verification – impacts other issues including data access and accuracy. In the case of verification, the reference data is normally under the control of the individual it belongs to. Once the biometric data is stored in a database, people have less control over who can access these data and for what purpose. Because of the statistical nature of biometrics and the intrinsic flaws that go along with the human involvement in the biometric process, it is significantly more challenging for large identification systems to achieve appropriate levels of accuracy and reliability than for verification systems (see also Kindt 2012, p. 26).

This illustrates that the function of biometric information is significantly different when used for identification as opposed to verification resulting in different system architectures, technical requirements and legal treatments. In addition, in the context of privacy, the sensitiveness of the biometric data will be assessed differently in both cases. Risks regarding fundamental rights will be higher and more serious when biometric data is used for identification compared to verification. For these reasons it is relevant to note that the (EC) No 2252/2004 regulation only covers biometrics for verification. Extending the function of the biometric information from verification to identification, which the regulation has left optional for individual Member States, would fundamentally change the functional and legal context of the use of biometrics.

4.2.1.2 Relevance of quality

The very foundation of every biometric system is the biometric image: the picture that is taken of the face, finger, iris or other physical characteristic. The quality of this biometric image has a major impact on the overall performance of a biometric system, especially in large scale systems with many data subjects and operators and which have a variety of operating conditions. High performance can only be achieved if the reference image (i.e. the image that is stored in the chip of the ePassport) as well as the 'live' image of the actual person, are of good quality.

The quality of the digital fingerprint image can be expressed by a standard developed by the US National Institute of Standards and Technology (NIST), called the 'NIST Fingerprint Image Quality' or NFIQ (NIST 2004). NIST currently distinguishes five quality levels from 1 (excellent) to 5 (poor). Higher quality levels, and subsequently a high performing biometric system, require significant investment to achieve a good quality of the captured images (NIST 2004). Patrick Grother, a biometric-expert from NIST, says the following about quality related to the investment and return on investment (ROI) of a biometric system:

"Lowering the quality acceptance thresholds at the point of fingerprint capture might solve the FTE (Failure to Enrol) and FRR (False Reject Rate) issue, but will definitely lead to a significantly lower performance of the central system. This will result in higher costs (because of exception handlings and

corrections of mistakes) and a lower ROI for the system as a whole, from a cost of ownership point of view, but also regarding the contribution that the system should bring to enhance the security of the overall system" (Wilson et al. 2003).

In 2009, Uwe Seidel from the German Federal Criminal Police Office stated in an article:

"In addition to technical data compliance, machine assisted identity confirmation relies on a secure, high quality enrolment process. (...) A carefully balanced enrolment process is just as important to quality as the actual enrolment hardware." (Seidel 2009)

These statements show that an interdependent relationship exists between the (desired) performance and the investment that is needed in order to achieve that performance. If a biometric system is not based on clearly specified performance criteria, it will be difficult to define the required quality level of the biometric data. And if no adequate investment into the enrolment and registration process is being done, it is unlikely that high quality identity confirmation will be achieved.

4.2.1.3 Ageing of biometric identifiers

Human beings are subject to ageing. Thus biometric identifiers, as part of the human body, are also subject to ageing effects. This complicates the identification process in a biometric system. For example, fingers grow during adolescence and therefore the fingerprint – being the imprint of the skin structure of the fingertip – 'grows' as well. It has been rightly assumed for quite some time that biometric verification and identification of children cannot be performed unless this growing effect is taken into account. Fingerprints of young children are not recognizable anymore after a certain amount of months (Schneider 2010). Children have been excluded from certain compulsory biometric registration for exactly that reason (European Commission 2006).

There are similar problems related to elderly people. Significant challenges on the acquisition of proper fingerprint images have been reported by the Dutch government (Tweede Kamer 2010). Of all biometric modalities, the face is the most vulnerable but even the iris will not remain the same during life with a dramatic fall in the performance of iris recognition matching results after only a few years (Graham-Rowe, 2012).

Other factors might complicate the ability of people being able to provide fingerprints of high quality, such as physically demanding manual labour for example (Coetzee and Botha 1993) or specific ethnic groups (Lodge et al. 2010). All these effects are at odds with the usual validity of ID documents of 5-10 years, not to mention plans for lifelong storage of biometric information in large databases.

4.2.1.4 The history of biometrics: Law enforcement to civil domain

As stated before, the use of biometrics has emerged from the domain of law enforcement. Fingerprints have been used for over a century in order to identify perpetrators from fingerprints left at a crime scene. Before the digital automation of biometric data processing, law enforcement systems were based on paper and ink. These systems were primarily used to solve national crimes. There were few standards on how data were captured and stored which resulted in local archives which were not designed for cross-matching between systems from other countries. Data exchange for a long time happened based on the original paper and ink images and it still does although in order to automatically search these repositories the fingerprint images need to be transferred into digital templates.

With increases in computer processing power, storage volumes and sensor accuracy, the physical way of using biometrics has evolved into a digital way of applying and managing biometric data. With the development of the biometric passport, there is a new context – the civil domain – rather than the law

enforcement usage with which we are familiar. With regard to the use of biometrics, there are four main differences between these two domains:

1. In law enforcement there is a closed group of data subjects. Data subjects are suspects, convicted criminals, immigrants or asylum seekers – in most cases a few million records at a national level. Public administrations and passport registers contain tens of millions of records.

2. In law enforcement the biometric data is taken under strictly regulated conditions and by educated personnel (in most cases trained police officers). Because the data subjects are obliged to submit their fingerprints, they are guided by at least two supervisors and may be forced to cooperate. Citizens can't be forced however, and the operating personnel generally have a lower level of skill and expertise compared to the trained police officers.

3. In law enforcement ten fingers are recorded in order to provide sufficient discriminative information in cases of law quality samples, whereas for the biometric passport only two fingers are needed.

4. In law enforcement, it is essential to obtain the highest possible quality of fingerprint images however long it takes. The capturing process could involve the assistance of one or two extra people. The issuance process of a biometric passport however, aims to be quick and smooth, which can easily lead to an attitude of shortening the time for fingerprint capturing process wherever possible.

Not understanding these major differences between a biometric system for law enforcement and one for citizens might lead to an underestimation of the overall efforts that are needed to capture good quality biometric data from citizens. Despite our long standing history with fingerprinting in law enforcement, we cannot simply project our experiences from that domain to the civil domain.

4.2.1.5 Standards, testing and certification

After the adoption of (EC) No 2252/2004, EU Member States have made significant investments in order to include biometrics into their new passports. However there are no commonly accepted and accredited tests that establish whether biometric software and equipment being used is meeting criteria on quality, security and interoperability.

In Europe, only a few test laboratories are capable of performing these tests. But since there is no network of accredited labs with sharable test tools, it is not easy to compare test results of different labs. There is no guarantee that the biometric information captured and stored by the various EU Member States will be of equal quality and integrity. So far European Member States do not seem to want to join forces in order to push the industry to follow a single standard on quality and performance (Breitenstein et al. 2012; Sanchez-Reillo 2012).

In terms of setting up European capabilities for testing and certification of ePassports, two new projects offer the most promising developments: FIDELITY and BEAT.

FIDELITY (Fast and trustworthy Identity Delivery and check with ePassports Leveraging Traveller Privacy) is a multi-disciplinary initiative, which will analyze shortcomings and vulnerabilities in the whole ePassport life cycle and develop technical solutions and recommendations to overcome them.

The goal of BEAT (Biometrics Evaluation and Testing) is to propose a framework of standard operational evaluations for biometric technologies. However, once quality and integrity specifications will be

introduced, it will remain a challenge for governments to verify whether a biometric vendor has delivered according to agreed specifications and standards. This requires a high level of expertise from those who procure eGovernment system.

4.2.2 European context and decision making

4.2.2.1 EU under pressure: 9-11 and the war on terror

The tragic events of September 11th and the events that followed in London and Madrid had a strong impact on discussions about safety and security in Europe. A European conference took place in 2002 in order to exchange information and to lay down a basis for European cooperation to improve passport security and combat identity fraud. The conference took place in The Hague in June 2002 under the leadership of the Dutch Ministry of the Interior[37]. Based on a proposal from The Netherlands, the conference concluded with a joint statement on the relevance of biometrics for travel documents. It was also decided by the delegates that discussions in the ICAO (International Civil Aviation Authority) that biometrics would collectively be supported and that the European Forum for Travel Documents (EFTD) should be established. Germany, the UK, Italy, France and The Netherlands (the initiators) formed the Standing Committee. This forum would facilitate information exchange and cooperation within the European Union in the field of standardization and harmonization of biometrics for travel documents. It laid the foundation for the decision of the European Council to make the use of biometrics in the passport mandatory (Böhre 2010, p. 32).

Although desk research has revealed little information concerning the workings of the EFTD (it was intended as a members only organization), some interesting insights were provided through an unclassified American telegram from the US Embassy in Berlin to the US Secretary of State in July 2003 by a US representative who was invited as an observer to the meeting[38]. It demonstrates how pressure from the US on the EU decision making process was clearly perceived as a discomfort:

"US policy concerning biometrics, machine readable passports (MRPs) and fingerprinting came under fire at the second European Forum for Travel Documents, which took place in Berlin June 30-July 1, 2003. (…) The commitment of all participants to enhanced document security in the post-9/11 world is genuine, but it is difficult to deny the uneasiness with which the Europeans and Japanese view the strict new US requirements for VWP [Visa Waiver Program] travellers. Our MRP [Machine Readable Passport] and biometrics deadlines are seen as unrealistic and a major disruption to the right of travel; our use of data collected from travellers as suspect. (…) The overwhelming sentiment of most participants was clear: US policy and regulations were forcing European countries to move too quickly to adopt policies of questionable merit."

In 2004 a former Dutch Minister stated after a European summit on identity fraud that '*biometrics are essential in the battle against terrorism and illegal immigration*'. Although this still remains to be proven, the link between biometrics and the battle against terrorism was firmly set in a policy making context. Despite the many unknowns about being introduced on such an unprecedented scale and the lack of empirical data on the performance of the current systems, it had become a common understanding that biometrics would play a strategic role in solving various issues regarding identity fraud, organized crime and terrorism (de Hert 2005, p. 37). After a period of several years without major incidents, in 2009 there was an attempted attack on an aircraft approaching Detroit, known as the 'Detroit Incident'. The

[37] European Conference for Issuing Authorities of Travel Documents: Exploring the use of Biometrics in Travel Documents, The Hague, 20-21 June 2002

[38] www.policylaundering.org/archives/ICAO/european_forum.pdf.

Toledo Joint Statement (EU 2010) that was issued following security discussions held between the US and EU after this incident, renewed this common understanding about the role of biometrics and nurtured the promise that they could play a significant role in avoiding such threats.

4.2.2.2 EC2252/2004: Purpose and limitations

In 2004 the European Union decided to endorse a new global standard for machine Readable Passports, issued by the ICAO through Doc9303. This regulation and its later amendment (EC) No 444/2009 require the facial image and two fingerprints to be stored in the ePassport chip. As mentioned above, the main objectives of the regulation were to strengthen the link between the passport holder and the passport, in order to prevent fraud. By choosing to store the facial image as well as two fingerprints, the EU opted for a stricter implementation of Doc9303 than the United States, which only stores a digital image of the face[39].

The EU regulation focuses on the passport document and its use at border control. No specifications or requirements are mentioned regarding the application, production and issuance process of the ePassport. Specifications of the quality requirements of the facial and biometric images are also missing. The next chapter shows how this has impacted the implementation of the ePassport in different European Member States.

4.2.2.3 The security of the ePassport

The personal data, the facial image and the fingerprints contained in a chip within the passport are protected by two security mechanisms: the Basic Access Control (BAC) and the Extended Access Control (EAC)[40] (BSI 2008).[41] BAC protects the personal data and the facial image on the passport via encryption. This protection is needed, because otherwise these data could easily be extracted from the contactless RFID-chip, even if the passport is closed and stowed away in a pocket or a bag. With the BAC, a passport first needs to be opened, presented to an inspector and pressed on a scanner.

The fingerprints stored on the passport are protected by another security mechanism, the Extended Access Control. This differs from BAC in that the keys to decrypt and unlock the fingerprint data does not have an analogue source, but is digitally generated through a Public Key Infrastructure (PKI) system. The digital keys are generated and owned by the government of the country where the passport is registered. In order for country A to read the fingerprint information stored on an ePassport from country B, the digital keys of country B need to be distributed to the passport control point of country A. Apart from the technical complexity of distributing and updating these keys, there also needs to be sufficient trust between the two countries regarding the way these fingerprint data is being handled and protected by the receiving country.

Due to the technical and operational problems in exchanging the digital keys for the Extended Access Control (EAC), only the Basic Access Control (BAC) protocol is currently being used for border control. Fingerprints are still not being used for verification at border control, despite the fact that they were added specifically to provide a higher level of security and reliability (ICAO 2011a). This also holds for

---

[39] http://travel.state.gov/passport/passport_2788.html#Two

[40] Extended Access Control, a PKI based system to protect the fingerprint data in the passport chip

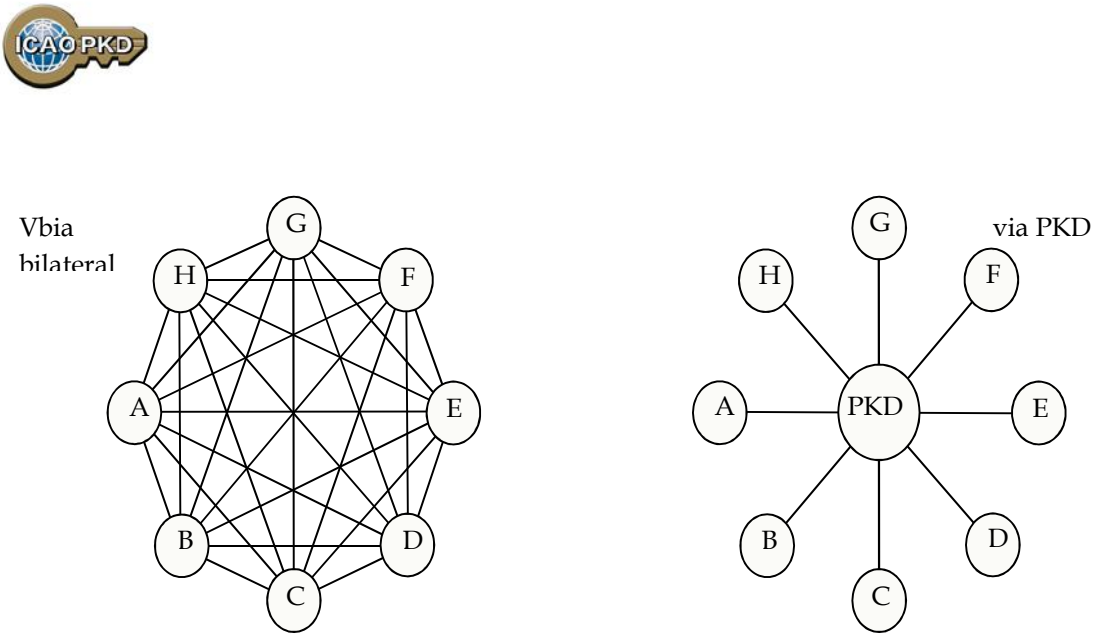
[41] In a separate non-public Commission Decision, further specifications of the e-passport are provided. These state that compliancy to the BSI Technical Report on Advanced Security Mechanisms for Machine Readable Travel Documents is required. This report describes a specific implementation to the EAC to protect the fingerprint data as mentioned in ICAO Doc9303.

most European Automated Border Control (ABC) gates (Schumacher 2012b; Frontex 2011a). But as mentioned earlier, facial recognition is more vulnerable to mistakes, as there are significant challenges in optimizing and harmonizing the quality of the facial image when applying for a new passport. This is partly due to the fact that many European countries use a pre-produced picture in the format of a passport photo instead of a live picture taken on the spot, although it is known that live pictures are more reliable (because of higher quality) and more secure (because the picture is taken when the person is actually present).

ICAO Public Key Directory

The bilateral exchange of the national keys for the Extended Access Control is complex, as shown below. Member States seem reluctant to provide the keys to certain other countries, due to a lack of trust caused by security, political or other issues. Desk research didn't reveal which countries currently exchange their keys therefore it is not clear to what extent this key element of the security chain of the ePassport is operational.

To overcome problems regarding the bilateral exchange of the national keys, the ICAO has initiated a centralized key storage and distribution system, the ICAO Public Key Directory[42], to which countries can subscribe against a yearly fee. The purpose of the PKD is to improve document checks and document security by replacing the current EAC system.



This example shows 8 States requiring 56 bilateral exchanges (left) or 2 exchanges with the PKD (right) to be up to date with certificates and revocation lists. In the case of 190 ICAO States, 35,910 bilateral exchanges would be necessary but still only 2 exchanges necessary with the PKD.

Source: German Federal Ministry of the Interior

[42] http://www.icao.int/Security/mrtd/Pages/icaoPKD.aspx

One of the main tasks of the PKD Board is to ensure that Member States are connected to the ICAO Public Key Directory. The objective is to speed up the process as agreed in the Toledo Joint Statement and to work together with the US to make sure that as many countries as possible join the ICAO Public Key Directory. However, the latest list of ICAO-PKD participants, dated 8 March 2012, lists a total of 12 EU Member States out of 30 countries worldwide[43]. These numbers are far from sufficient in order to achieve a global or even a European coverage.

4.2.2.4 The integrity of the enrolment process

The ICAO documents on ePassports and their European endorsement stated in (EC) No 2252/2004 show that current ePassport standards are mainly focusing on the travel document itself. Little attention is given to questions relating to the reliability or integrity of the data it contains and how we can trust the information stored in the chip. These matters depend strongly on the quality and integrity of the application and issuance process. That raises the question of how the higher security requirements of the passport itself, as laid down in Doc9303 and (EC) No 2252/2004, are supported by the application and issuance process. This back-bone of the passport life cycle has clearly not been taken into account by the Doc9303 standard, as the country studies will also show. Although work is in progress at the ICAO level to address the whole ePassport life cycle (ICAO 2011b), no finalized standards or guidelines are yet available.

4.3 Country studies

This chapter describes the way different EU Member States implement the Council Regulation on standards for security features and biometrics in passports and travel documents EC 2252/2004. The following countries are described: Czech Republic, France, Germany, Italy, The Netherlands, Norway and Slovenia.

The research carried out for the country studies aimed to gather and present information from the selected Member States in a uniform way. In order to do so, a questionnaire was sent to relevant partners in the various countries. However, it proved quite difficult to gather similar information from the different partners as some questionnaires were not completed in full or not at all. Therefore, additional information has been gathered from other sources including presentations and also from e-mail conversations. As a result, some information in the country studies can be compared easily, some not. Nevertheless, the overview of the country studies provides interesting findings.

4.3.1.1 Czech Republic

Policy and legislation

The EU Regulation has been implemented into Czech law under No. 136/2006 Sb. The Czech Ministry of the Interior is responsible for the production and issuance of the ePassport. The ePassports are produced by the state printing company, Státní Tiskárna Cenin. The legal preparation started in 2004 and took 1.5 years to implement.

Implementation

43 http://www.icao.int/Security/mrtd/Downloads/PKD%20Documents/ICAO%20PKD%20Participant%20Contact%20List.pdf

In the Czech Republic there are more than 200 state authorities that issue passports including 205 municipalities and eight foreign police stations. There are 22 issuing authorities in Prague alone. The ePassport project began in 2006 and consisted of two phases: implementation of the chip with a facial image (2006) and implementation of the fingerprint (2009).

In order to prepare for the technical implementation of the regulation, two studies on the testing of fingerprint systems were considered: *BioFinger*, by the German Bundesamt für Sicherheit in der Informationstechnik (BSI 2004) and *Technical Evaluation of Biometric Systems* by the Czech National Security Agency (Drahansky et al. 2008).

The *BioFinger* study showed that products from different vendors could not be combined without a significant drop in performance. Sometimes the products were not compatible at all. This illustrates the immaturity of the biometrics industry at that time and the risks of vendor lock in. Another outcome was that fake fingers could cheat almost all fingerprint sensors. It was also revealed that various skin diseases negatively impact the performance of fingerprint recognition due to lower quality or distortion of the images. Studies are ongoing to see if touchless fingerprint sensors might solve all or part of these problems.

Based on the studies, the Czech Republic has significantly invested in the quality of the biometric data capturing process, which has resulted in a dedicated booth where live facial images, fingerprints and signatures are being taken.

The acquisition of the facial images and fingerprints takes place in special cabins, so called 'eGates' (not to be confused with the eGates at airports for automated border control). Biometric data is stored for 2 months after the date of application because of warranty reasons and for validating data in case of complaints. After this period the data is erased. There is a central register for passports but no facial images or fingerprint data is stored.

The facial image is captured in real life in the eGate, which provides an image quality that is much higher than scanned images. The eGate has standardized lighting and background. It also provides a higher level of security, as no additional judgment needs to take place whether the picture is really of the person who applies for the passport. Fingerprints are acquired in three capturing sessions. The best of three is taken. The target is to achieve a quality level of at least NFIQ-3.

Capabilities

The Czech Government engaged the University of Brno and the Fraunhofer Institute for specific research and support in technical evaluations. Specially trained operators are engaged to capture the biometric features.

4.3.2 France

Policy and legislation[44]

In France, the legal implementation of (EC) No 2252/2004 was decided through a presidential decree to enable compliancy with its provisions[45]. The decree provides for a passport applicant's facial and eight-

[44] For more information see also: FIDIS, D3.14 The Privacy Legal framework for Biometrics, Chapter 4: France

[45] See http://www.cnil.fr/english/topics/regulating-biometrics/#c1543 and http://www.conseil-constitutionnel.fr/conseil-constitutionnel/english/case-law/decision/decision-no-2012-652-dc-of-22-march-2012.105428.html

fingerprint digitized images to be retained in the existing passport management system DELPHINE. Since 2004, French law requires that the automated processing of biometric data for identity control is subject to the prior authorization of the French Data Protection Authority (CNIL). The issue of biometric passports was referred by the Ministry of Home Affairs to the CNIL for review in the autumn of 2007.

Privacy

In this opinion, the CNIL expressed a number of reservations with regard to the implementation of the EU regulation (CNIL 2007). Because this would lead to the first centralized database of biometric data on French citizens for administrative purposes, CNIL noted that the processing of such data would be acceptable only to the extent that it could be justified by a compelling necessity linked to national security or public order. In this respect, the Commission considered that the purposes claimed, however legitimate (i.e. improving the procedures for issuance and renewal of passports along with combating ID fraud) failed to justify the national-scale retention of biometric data such as fingerprints, and that the type of data processing involved would cause excessive infringement to individual liberties.

This opinion of the CNIL contradicted assurances from the Ministry of Home Affairs who stressed that it would be impossible to conduct any identification search from the digitized fingerprint images or digitized facial images.

CNIL also regretted that the far reaching decision, going further than the remit of the original EU Regulation, was made by government decree instead of by parliamentary vote. According to the Commission, the scope and the significance of the issues at stake would have justified a law to be put before parliament, enabling a broad public debate on the subject.

Implementation

The CNIL's opinion did not lead to changes in the proposed decree. However, on March 22nd 2012, the French Constitutional Court ruled against several articles of the law, which includes the legal implementation of (EC) No 2252/2004 (Conseil-Constituel 2012). The most compelling decision is that parts of the decree have been dropped because they were considered to be a serious infringement of the French national constitution. This implies that the central storage of biometric data, as well as the use of these data for detection and prosecution purposes, has been judged as being un-proportional and therefore against the constitution.

4.3.3 Germany

Policy and legislation[46]

In Germany, the Federal Parliament approved the introduction of electronic passports on 8 July 2005, being the implementation of the (EC) No 2252/2004 regulation. In June 2007, the Passport Act was revised and approved by the parliament in order to lay down the legal foundation for the second generation electronic passports including two finger scans. These finger scans are only to be stored on the passport chip. The use of the biometric data is only permitted to verify the identity of the holder (a 1:1 comparison) by specific public authorities (police, customs, registration authorities).

[46] See also: FIDIS, D3.14 The Privacy Legal framework for Biometrics, Chapter 5: Germany

Privacy

In Germany the opinion of the Data Protection Authorities, parliamentarians and the general public, has been strongly influenced by the idea that a national biometric database could be used for detection and prosecution purposes. This was considered a serious infringement of people's privacy. As a result, German legislation stipulates that biometric facial data can only be stored in a local database, while fingerprint scans can only be stored on the chip of the passport thus excluding any local or central storage. A nationwide database, with data relating to the passports (not only a biometric database) is explicitly forbidden by law.

Implementation

In order to safeguard global interoperability and European regulation, Germany complies with international standards defined by ICAO and the International Standardisation Organization (ISO) with regard to ePassport technology, the biometric verification process and what biometric features are stored in the passport chip. An estimated 15 million ePassports were issued from November 2005 to April 2011.

The National ID-Card has the same security level as the passport, including the RFID chip. The facial image must be stored in the chip; the two fingerprints can be stored on a voluntary basis.

The passport and NID-card application process is decentralized and takes place at 5,300 authorities, representing a very heterogeneous IT infrastructure. The production and personalization is centralized at the premises of the Bundesdruckerei.

The German authorities took a rigorous approach to quality issues related to the enrolment of biometric images. As mentioned before, the BioFinger study from the German Bundesamt für Sicherheit in der Informationstechnik (BSI 2004) was conducted to prepare the technical implementation of the passport. The importance of quality to the performance of the biometric passport was acknowledged in the early stages of preparation before it was rolled out nationally. A central Quality Assurance Repository was established to monitor the quality of the biometric features in the German ePassports.

In 2008 the following quality scores for fingerprints were recorded (Brauer 2011):

NFIQ 1 – 73%

NFIQ 2 – 17,6%

NFIQ 3 – 7%

NFIQ 4/5 – 2,3%

This means that 90% of the fingerprints are of excellent or good quality. These marks only provide information on the quality of the images, not regarding the performance of the biometric system. In Chapter 2 of this study the relationship between quality and performance is being explained. The fingerprints are taken 'live' during the application process.

Capabilities

The German Biometric Strategy Platform was established in 2005. With this platform Germany was one of the first countries in the European Union that systematically organized stakeholders involved in biometrics. The platform brought industrial capabilities together in order to create an overview of the state of the art and to have a platform for information exchange.

The Federal Office for Information Security (BSI) and the German Federal Criminal Police Office (BKA) developed technical guidelines for the acquisition, quality assurance and transfer of production data for

passports[47]. These guidelines cover the quality of biometric data during all stages of the application process, including production, and are made generally available. A national certification scheme was developed which defines the overall qualification criteria for secure, low cost, single finger scanners.

The German authorities have gained significant experience with the enrolment of biometric data for the ePassport. Studies, pilots and tests have shown that the large scale enrolment of biometric data requires constant attention:

From an operational point of view, the enrolment of fingerprints in a civil (i.e. non law-enforcement) environment creates unexpected challenges for municipalities, citizens and government officials. Fingerprint registration has necessitated the installation of a new technical infrastructure.

Pilot programs are essential in that they highlight how to handle exceptions and point to any shortcomings in the technical processes.

Training and up-to-date information for the benefit of the municipalities and the citizens needs to be organized at a national scale.

Future plans, European cooperation

The German Government (including the BSI) is in favour of developing an EU-wide quality practice. Germany is a strong advocate of the ICAO Public Key Directory (PKD) and chaired the PKD Board in 2011.

4.3.4 Italy

Policy and legislation

The Ministry of Foreign Affairs is the owner of the passport issuing process, and responsible for issuing passports to Italian nationals abroad through Italian diplomatic consular posts. The Ministry of the Interior is responsible for issuing passports in Italy, which takes place at police offices. The *Istituto Poligrafico e Zecca dello Stato*, the national printing office, is the official government contractor for Italy's electronic passport technology. The personalization is done locally, at police stations or at consular posts.

Implementation

Decisions of the Italian Data Protection Authority regarding the implementation of (EC) No 2252/2004 have impacted several aspects of policy on biometrics. Firstly, the biometric data stored in the chip can only be used for identity verification. Secondly, the captured fingerprints have to be locally stored in an encrypted way and must be sent to the central production system through a Virtual Private Network (VPN) for digital signatures. Fingerprints are not stored in a database. Just like Germany, quality scores are centrally stored for monitoring and improvement purposes only. Facial images, stored in a central register, can't be used for 1:n identification and are stored for administrative purposes only.

---

[47] BSI TR-03104 Technische Richtlinie zur Produktionsdatenerfassung, -qualitätsprüfung und -übermittlung für PässeAnnex 1+2,

https://www.bsi.bund.de/ContentBSI/EN/Publications/Techguidelines/TR03104/BSITR03104.html;jsessionid=E91C7D06EAB603C995141C1DA223BD30.2_cid286

Current quality scores for Italy are as follows (dated 30/01/2012)[48]:

NFIQ 1 - 52%

NFIQ 2 - 22%

NFIQ 3 - 24%

NFIQ4/5 – 2%

This means that 74% of the fingerprints is of excellent or good quality. Biometric verification based on fingerprints is done when the citizen receives his or her passport. In case of problems, when the verification does not succeed, a new passport is issued free of charge. However, as it is not mandatory, this verification doesn't always take place. The facial image is taken from a scanned photo, instead of a live picture.

Capabilities

The operators that take the fingerprints are not certified, but there are some training activities.

4.3.5 The Netherlands

Policy and legislation[49]

The Ministry of the Interior is responsible for the production and issuance of passports, as well the administration of travel documents and overall public administration. Passport production is contracted to a private company. Since 2001 the passport has been centrally produced and personalized, so no blank passports are distributed. This has substantially reduced fraudulent personalization and criminal trade in blank passports.

In addition to the regulatory requirements of (EC) No 2252/2004, the Dutch government also decided in 2004 that a central biometric database including facial images and fingerprints needed to be installed for detection and prosecution purposes. It was also decided to store two extra fingerprint scans in the database. These two extra scans can be used to verify a person's identity in case the passport is unreliable or if there is no passport at all. The national ID-card (NID-card) applies under the same law, meaning that the NID-card is also equipped with an ICAO compliant chip with biometric data.

In 2009 the final amendments to the passport act were accepted by parliament and senate (Stb. 2009, 253). Regarding implementation costs, the government aimed at a minimal increase in the overall costs of passport applications, production and issuance. Based on preliminary studies and pilots the government felt that a reject rate of below 3% (e.g. meaning that meaning that less than 30.000 of 1 million verifications should be reported as a non-match) should be achievable and acceptable. It is unclear which considerations led to this requirement, as it was not specified if these are false or true rejections.

Privacy

In 2007 the Dutch Data Protection Authority (CBP) provided its opinion on the proposed passport act, stating it was violating the privacy of Dutch citizens (CBP 2007). Other experts criticized the decision to establish a central biometric database at an early stage. Nevertheless, the proposed legislation was approved by parliament, leaving the proposed act unchanged.

---

[48] Source: DIGIT PA: National Agency for the Digitalisation of the Italian Public Administration

[49] See also: FIDIS, D3.14 The Privacy Legal framework for Biometrics, Chapter 6: The Netherlands

In November 2010 two reports from the Dutch Scientific Council for Government Policy (WRR) on the Dutch Passport Act were published (Böhre 2010; Snijder 2010). These had a strong impact on parliament, the media and public opinion. In April 2011 there was a public hearing about the biometric passport, as a majority of parliamentarians no longer felt comfortable with the new passport legislation. High reject rates had been reported (one test revealed a rejection rate for the fingerprint verification of 21%)[50] and there were potential privacy implications for the fingerprint database and consequences for citizens due to technical imperfections. Following this hearing the minister decided to withdraw the central fingerprint database and delete all the prints that had been stored so far. Fingerprints would now only be stored until the passport was issued (usually 3-5 days). Storing fingerprints for the NID-card would be optional. Yet so far (June 2012), the fingerprints of issued passports have not yet been deleted and citizens still need to submit their fingerprints for the NID-card.

As most parliamentarians still had many questions regarding the decision making process related to the making of the current law, they requested an independent study on its history. In February 2011 the study was finalized (Bekker 2012). It concluded that the technical and practical implications of introducing biometrics at a nationwide scale had been strongly underestimated during the decision making process. This matter wasn't just at national level, but extended to the European level as well. The study shows that no clear criteria regarding the performance of the biometric verification process exist. In addition, the study indicates a significant gap between policy makers and experts. The international political climate had an impact. The terrorist events of 9/11 and those that followed in Europe had exerted a strong pressure on the decision making process. This resulted in the implementation of the ePassport being speeded up, while disregarding privacy matters. The study concludes that the Data Protection Authority's opinion on the upcoming passport act was ignored by policy makers and politicians (CBP 2007). This opinion explicitly stated that the provision for a central biometric database had not been sufficiently tested or studied and questioned the motivation for its development. Alternatives had not seriously been considered or evaluated.

The study on the history of law making was well received by government and parliament. In the meantime, and partly based on the Dutch studies for the Dutch Scientific Council for Government Policy (WRR), the European Commission had started an investigation regarding the potential violation of Article 8 of the UCHR and the issue of the high rejection rate at the request of the European Parliament. Questions for written answers were submitted by Members of the European Parliament (MEP) S. in 't Veld regarding the Dutch law on passports[51] and together with MEP Baroness S. Ludford, regarding the quality and verifiability of fingerprints[52] and third-country access to the biometric data of EU citizens[53].

Implementation

There are more than 600 municipalities where one can apply for a passport. The instructions to operators are to only verify the fingerprints if there are doubts about the person collecting the passport. In practice,

---

[50] Some municipalities requested the government to perform tests in order to see how well the biometric verification performs. The results of these tests could then be used to improve aspects of the biometric capturing process. When the government rejected this request, the community of Roermond executed their own test. This test revealed a rejection rate of 21%. Details on the causes of these rejections are not available.

[51] S. in 't Veld (MEP), Questions for written answer to the Commission regarding the Dutch law on passports, E-9264/2010

[52] S. in 't Veld (MEP), Baroness S. Ludford (MEP), Question for written answer to the Commission regarding the quality and verifiability of fingerprints, E-001306/2012

[53] S. in 't Veld (MEP), Baroness S. Ludford (MEP), Question for written answer to the Commission regarding third-country access to biometric data of EU citizens, E-001307/2012

no verification takes place (Snijder 2010). The facial image is scanned from a picture provided by the applicant according to strict guidelines.

Capabilities

Training of operating personnel is mainly provided through a digital course. There is no verification as to whether or not an operator actually followed the course and if so, if the operator has sufficiently understood the instructions. No instructions on how to detect fake fingerprints are provided.

Future plans, European cooperation

On 12th April 2012 the Minister of the Interior reaffirmed the Dutch commitment to the use of biometrics in a letter to parliament (Tweede Kamer 2012). The Netherlands believes that cooperating at a European level, e.g. by exchanging experiences and by developing common views, is relevant. It will invest to ensure higher standards in the application and issuance process and the government will increase its efforts in monitoring, analyzing and improving the quality of these processes in order to reduce the negative consequences of false rejects. Where possible, experiences from other member states will be taken into account.

4.3.6 Norway

While not a member of the European Union, other forms of contact enable Norway to maintain a very high level of economic integration, and political co-operation, with the EU and its Member States. Norway has signed up to the Schengen Agreement, and is thus participating in co-operation on common passport and border control, as well as several other issues within the EU policy area of Freedom, Security and Justice. Norway has also adopted the (EC) No 2252/2004 Regulation.

Policy, legislation

The Norwegian Passport Act contains provisions for the capture of biometric and storing them in a passport, together with rules for transparency and privacy. There are no additional uses as regards to the use of biometrics in passports, apart from verification of the passport holder for border control purposes. Regarding immigration (visa, asylum seekers etc.) Norway has other rules on the use of biometrics. The use of biometrics for investigation of criminal cases and recording of criminals are regulated in The Penal Proceeding Act.

Privacy

In 2005, when the amendments in the passport legislation were implemented, the Norwegian Data Protection Authority stated that the introduction of biometrics in passports was premature and needed more explanation and deliberation before it could be enacted[54]. The Norwegian Data Protection Authority argued that the use of biometrics for border control purposes was premature and lacked acceptable standards. This opinion did not prevent the new legislation from being approved and implemented. After this unsuccessful intervention, the Norwegian Data Protection Authority asked for investments in passport readers at the issuance and application points (e.g. the police stations) that could be used for all passport holders to verify whether the information stored in the chip is correct. The Norwegian DPA also instructed the Norway Police Directorate to conduct a risk analysis regarding the management of the passport data, which was carried out.

[54] Interview with Norwegian Data Protection Authority conducted by Max Snijder

Implementation

A passport lasts for 10 years. The application process, which takes place at police stations, includes taking a live facial image. The facial image is stored in the passport database but without on-line matching capacities. In order to obtain good quality fingerprints as much time is taken as needed. No biometric verification takes place when the passport is issued.

From June 2012, the facial image of the ePassport will be used for verification purposes at border control. The biometric information of the ePassport is not used in field operations (e.g. by the police). No additional services enabled by the biometrics of the ePassport are currently being envisaged.

Capabilities

Operators receive specific training on the capturing of fingerprints, although no certification of the personnel takes place. Only trained personnel are allowed to capture the biometric data. Personnel are not trained to recognize fake fingerprints. Competences have primarily been set up in the application centers (police stations) and border control stations. In addition, an infrastructure for logistics support has been set up in the Police Computer Service. Norway has recently opened its National Identity and Documentation Centre (NID Senter for ID Kunnskap). In cooperation with the University of Gjøvik a center of excellence on biometrics has been established containing international experts. Conformance to standards and performance requirements have been partly based on tests carried out in other countries.

Future plans, European cooperation

Norway is not currently participating in any concerted activity at European level in order to develop a common approach on the implementation of the ePassport. Norway would welcome such activities and intends to participate in them as soon they take place.

Future plans regarding the improvement of the quality of the biometric data of the ePassport include better equipment, better training of front end personnel, the establishment of central biometric repositories and the establishment of online access to certificates.

4.3.7 Slovenia

Policy and legislation

Slovenia follows (EC) No 2252/2004 and has published the new passport act in the Official Gazette of Slovenia Nr.29/2011. The passport act was coordinated by several ministries and the information commissioner. In contrast to the other selected countries, the data protection officer of Slovenia did not express an opinion on the passport act.

Implementation

During the application process there is no duplicate check based on biometric data, nor does a background check takes place. That means that during the application process no criminal databases are searched based on the biometric data only. When the passport is issued, no biometric verification takes place. At border control check points both the facial images as well as the fingerprints are being used for passport control. Apart from border control, no other applications or services are being envisaged for the biometric passport.

The passport has a validity of 10 years for citizens of 18 years and older. For citizens between 3 and 18 years the validity is 5 years and for children under 3 years it is 3 years. Slovenia has no electronic national ID-card.

The facial image is scanned from an existing photo provided by the applicant. Facial images are also permanently stored in a central repository, while fingerprints are stored until the passport has been issued. The biometric equipment is being tested and certified by a national testing institute. Capturing the fingerprints may take as long as needed to get the highest possible quality scores. No quality scores have been provided.

Capabilities

Personnel that capture biometric data during the application process have been trained and certified. Only certified personnel may capture biometric data. Personnel are not trained in recognizing fake fingerprints. There are no roadmaps or plans to improve the quality of the biometric data.

4.3.8 A short analysis of the country studies

A comparison of the country descriptions leads to the following observations.

- All countries comply to the EU regulation (EC) No 2252/2004;
- No clear criteria for the quality and security of the biometric images are available at EU level, resulting in different national implementations and biometric data that varies in quality. Some countries take a more proactive approach on mastering and improving biometric technology, while others are following developments. Out of these selected countries Germany seems to be the most proactive in this respect, and also in their cooperation with other countries. Germany and Italy provided quality scores of fingerprint data for this study. The scores of Germany are substantially higher than those from Italy. Germany has 20% more images of the highest quality, while having 16% less of the lowest quality. It seems that Germany's quality approach does pay off;
- Countries show different levels of engagement when it comes to taking the full life cycle of the biometric passport into account. Some have significantly invested in the quality of the biometric registration through testing, studies and standards. Others took a more reactive approach by following what others did and what the industry offered;
- Operating personnel are being trained for capturing biometric data, but some countries certify their personnel and others don't. This means that not all countries are able to provide the same level of quality and integrity of the biometric data;
- Fingerprints are not being used for verification at border check points on a structural basis, nor does biometric verification take place at issuance;
- Only the Czech Republic and Norway are taking the facial images 'live' during the application process. In Italy and Norway biometric data is captured at a police station, where personnel have experience with biometrics. The other countries keep the capturing process at the municipalities;
- In some countries the opinion of the national Data Protection Authority has directly impacted the legislative process (Italy, Germany) while in others the opinions of the DPAs have been ignored;
- Countries keep repositories, but they differ in the kind of data, the purpose of its use and the place and duration of storage. France and The Netherlands initially intended to use central

biometric repositories for detection and prosecution purposes. Norway intends to do so in the future. The two countries that installed a centralized biometric database for law enforcement purposes (France and The Netherlands) have both withdrawn them. The other countries are explicitly preventing databases from being searched for establishing identity based on biometric features;

- Acquiring information about the implementation of the biometric passport is not easy as not all countries wish to provide data officially. This is a key issue if common European goals need to be achieved.

4.4 Addressing the research questions

4.4.1 Security

Within the biometric framework, the term security refers to two aspects: making the biometric data available for authorized users while being protected from non-authorized users; establishing a more reliable link between the passport and its genuine holder in order to improve the security of European borders. There have been very few studies looking into the security of the ePassport at a European level. The most recent, and also the most comprehensive study, was done by Frontex (formerly known as the European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union in 2011 (Frontex 2011a). Rather than solely focusing on the passport itself, the study takes the full life cycle of a passport or ID-card into account, from application to its actual use for border control purposes. The Frontex study shows that the ePassport can only be a trustworthy tool for border control if the registration, production and distribution processes are also taken into account. The main elements that determine the level of security of the passport are described in more detail below.

Document Security

Since the early 2000s, passports have become increasingly secure thanks to more sophisticated document security features and a move towards central production for personalization when the personal data of a citizen is added to a blank passport. Fraud typically takes place at the weakest link but the technical security of the ePassport itself is higher than ever. Therefore it can be assumed that the weakest link is shifting from document fraud to fraud in the issuance process. This includes the possibility of obtaining a genuine passport based on false breeder documents, such as fake birth certificates, and in lookalike fraud when a passport is illicitly used by someone with similar physical features to enter a country, for example. European legislation regarding a minimum security standard for identity documents is currently lacking and there are no figures available about the actual size of these two types of fraud. This makes it difficult to assess the effects of EC Regulation No 2252/2004 (which aimed to combat fraud by establishing a stronger link between the passport document and its legitimate holder) or provide a judgement on the proportionality of such a regulation.

Chip-security

Although the Basic Access Control and the Extended Access Control elements were designed to improve the protection of the personal information stored in the chip of the ePassport, experts stated in 2005 and 2006 that BAC is not sufficient to protect the data stored on the chip, it only prevents simple skimming

attacks (WP29 2004; FIDIS 2006a).[55] This was confirmed by the more recent Frontex study (2011). To improve security the new Supplemental Access Control (SAC) standardwill replace BAC in the long term. There is no official standard which specifies SAC yet, only preliminary technical reports by the ICAO Technical Advisory Group on Machine Readable Travel Document (TAG-MRTD).[56]

Fingerprints are securely stored through Extended Access Control. However, the EAC keys are not being adequately distributed, which significantly limits their operational use. None of the selected European member states (except Slovenia) are using the fingerprints contained in the ePassport in their border control processes. In practice, the fingerprints are not adding security to the ePassport. To improve the exchange of keys the ICAO established the Public Key Directory (see paragraph *2.2.4*). Only a limited number of countries have subscribed to the PKD. Fingerprints will only be able to add security to the ePassport when a proper key exchanging mechanism is in place. The success of this mechanism will largely depend on its technical and operational security. Confidence in the system is only achieved if sufficient trust exists between the exchanging countries regarding each other's security and integrity standards.

Spoofing of biometric features

Spoofing of biometric features such as fingerprints is a risk for the security of the biometric passport and the security of the border control process (Frontex 2011a, p. 118). Fingerprint sensors are not capable of detecting all possible spoofing attacks yet (BSI 2004; Schumacher 2012b). That means the only countermeasure against spoofing is direct supervision by qualified personnel. This supervision should take place at any stage in the identity chain where fingerprint data is captured, starting with the application process. As of today, fake prints can be applied almost invisibly, so special training is needed to make operating personnel capable of detecting such fakes (Grefrath and Tekampe 2010). The country studies show that no specific training takes place for operators to detect fake fingerprints. So the risk of storing fake fingerprints in the passport (and potentially also in local/central databases) is realistic. Fingerprints that are stored in the passport system might be associated with the wrong person, while the real person will not be identified. It goes without saying that this will impose significant risks to the security of the passport system as a whole, as well as the security of the processes that rely on the passport.

To prevent spoofing with facial images, pictures for the ePassport should be taken 'live' during the passport application process. From the case studies, only the Czech Republic and Norway take 'live' images. Currently ABC-gates, which are based on the use of face recognition, have extensive human supervision, thus reducing the risk of spoofing and look-alike fraud (Schumacher 2010).

Application and issuance process

The (EC) No 2225/2004 Regulation doesn't cover the full process of application, biometric capturing, production, personalization and issuance of the biometric passport. The report by Frontex (2011a) concluded that there are no European security regulations regarding the issuance process of the ePassport. Although work has been done to standardize the application process in Europe, no such standard yet exists.

---

[55] Fidis, Budapest Declaration on Machine Readable Travel Documents (2006), available at http://www.fidis.net/press-events/pressreleases/budapest-declaration/#c1307

[56] Additional information from ICAO, including reports of the Technical Advisory Group on Machine Readable Travel Document (TAG-MRTD), is available online at http://www2.icao.int/en/mrtd/.

Regarding the capturing of the facial image and fingerprints, the integrity of these data largely depend on the skills and reliability of the operating personnel and the security of the equipment being used. From the countries described in the previous chapter, only Slovenia has certified personnel taking the biometric data. There is a risk that fake or wrong fingerprints can being taken, that a 'look alike' picture is being scanned or that a 'look alike' receives the new passport particularly if the facial image is not taken 'live' during the application process and an existing picture is scanned compromising the quality of the image. In addition there are no EU quality requirements (yet) for the biometric images, meaning that low quality images could be stored in the passport chip. Low quality means more mistakes, more use of back up procedures (to handle exceptions), a higher tolerance to quality thresholds in order to prevent too many rejections and overall, less efficiency. This threatens the security level of the passport verification process and subsequently the security of the border control process.

The country studies show differing approaches to the development of biometric technology. Germany and the Czech Republic have invested significantly to improve quality (and integrity), while other countries take a minimal approach. The country studies also show that not all countries perform biometric verification at issuance, thus creating a gap in the feedback loop on quality and integrity. Mistakes may not be detected (or corrected) and the passport holder may only discover a problem exists at border control. Or it might never be found out. Not performing biometric verification means that there are no possibilities to monitor and evaluate the quality and integrity of the process.

The security of the application process needs attention as it is the start of the passport life cycle. The skill and reliability of operating personnel is important for the overall quality and integrity of the application process. Without proper screening, temporary staff should be considered a major security threat (Frontex 2011a). Although the ICAO has developed a detailed guide for the security of handling and issuance of travel documents (ICAO 2010), no European policy has yet been formalized to address the issues of the ePassport life cycle not regulated through (EC) No 2252/2004. As shown by the case studies, countries have different approaches to the design and implementation of the application process. If a common European level of quality and security of the full ePassport life cycle is to be achieved, the quality and integrity of the application and issuance process of the biometric passport need to be harmonized.

Border security

Biometric passports are intended to be used for border control purposes but no requirements, functional specifications or standards for inspection systems have been identified (see also paragraph *2.2.3* and Frontex 2011a). This could be considered a serious threat to border security and interoperability. Apart from ABC gates that mostly use a facial image for automated verification of the passport holder, biometric checks are not currently being deployed in regular passport checks. So the biometric data stored in the passport chip do not yet provide a significant contribution to the security of inspection process of the ePassport.

4.4.2 Interoperability

Technical interoperability of the ePassport chip

The Basic Access Control and Extended Access Control technologies are supported by clear and accepted standards. Work done by the Brussels Interoperability Group (BIG), a former technical working group from the Article 6 Committee of the Schengen Agreement, has improved the interoperability of ePassports in Europe. Nevertheless, the Frontex study reports that there are regular failures in reading the BAC protected information due to quality and interoperability issues, such as shiny laminates that prevent the MRZ being properly scanned, incorrect signatures, low level technical problems with the RFID chip, authentications failure because the CSCA certificate is not available and various other issues. As a result, border guards might not be able to use ePassport data.

Interoperability of the EAC access key exchange mechanism

The fingerprint is stored behind the Extended Access Control mechanism. Theoretically, technical interoperability exists thanks to the work of the BIG and the German BSI[57]. But a solution needs to be found to make the fingerprint operational in practice. EAC interoperability is currently hindered by problems with the current key distribution mechanism. The ICAO PKD system (see also paragraph 2.2.4) does not provide an overall solution for that yet, as a limited number of countries have subscribed to the PKD. As a result there is non-interoperability in practice and fingerprints that are stored in the ePassport can't be generally used for border control purposes.

Interoperability of biometric products and components

The interoperability of biometric products is still an issue at the level of image quality and template design. Member States are supplied by a variety of vendors, so problems of interoperability between countries exist. There are still no independent criteria or independently validated test databases available in Europe for assessing the quality of biometric images. The most commonly used quality criteria currently available are the NIST Fingerprint Image Quality scores (NFIQ scores). However, systems containing biometric components from a single vendor (i.e. both hardware and software) still provide the best performance (NIST 2004) as the implementation of the NFIQ criteria are still vendor dependent. As a consequence, single vendor systems are preferable to achieve the highest performance and lowest error rates. The risk of this is a vendor lock in; changing to another vendor might involve high costs and several practical problems because a complete redesign of the software application and re-enrolment of all biometric data might be needed.

4.4.3 Identification

The purpose of EC 2252/2004 is to increase the reliability and efficiency of the identification process for border control purposes by making use of the ePassport. Adding biometric data strengthens the link between the passport and its holder. The improvements on document security and the centralization of production and personalization processes have already improved the reliability of passport based identity claims. As mentioned in the previous paragraphs, issues regarding quality, security and interoperability prevent the particular features (i.e. the chip and biometrics) of the biometric passport from being used at a supranational scale. So it can be concluded that EC 2252/2004 has not yet achieved its full potential in improving the identification capabilities of the biometric passport.

A side effect of the EU regulation is that countries like France and the Netherlands have introduced central biometric repositories. A central biometric database enables additional functionality but also brings new challenges. The main reason for installing a national biometric database is to perform identification. It can be used to filter out multiple identities by de-duplication and can also be useful in checking a person's identity once a passport is unreliable or lost. Moreover, central biometric databases can also be used for establishing identity for law enforcement purposes, such as detection and prosecution. This capability can be extended to the identification of citizens without their knowledge or consent as faces, irises and fingerprints can be captured covertly. Once a biometric database is available, this identification capability can easily be activated. Since people can be identified at any place and time, governments or private parties would be able to achieve identity dominance. Transparency regarding the purpose of this capability and the right to anonymity is putting pressure on this potential usage.

---

[57] BSI TR-03110, Technical Guideline Advanced Security Mechanisms for Machine Readable Travel Documents, German Federal Office for Information Security

4.4.4 Function creep

Although the passport itself is used for identification, the function of the biometrics stored in the ePassport chip is for verification purposes only. So far (EC) No 2252/2004 is clear and restrictive regarding the purpose for using the biometric data, as Art. 4.3 says:

"For the purpose of this Regulation, the biometric features in passports and travel documents shall only be used for verifying: (a) the authenticity of the document; (b) the identity of the holder by means of directly available comparable features when the passport or other travel documents are required to be produced by law."

However, the amendment No 444/2009 from 28 May 2009 on EC 2252/2004 preamble sub 5) states that:

"Regulation (EC) No 2252/2004 requires biometric data to be collected and stored in the storage medium of passports and travel documents with a view to issuing such documents. This is without prejudice to any other use or storage of these data in accordance with national legislation of Member States. Regulation (EC) No 2252/2004 does not provide a legal base for setting up or maintaining databases for storage of those data in Member States, which is strictly a matter of national law."

Storing the biometric data of citizens in a central database was not the purpose of (EC) No 2252/2004, but the 2009 amendment explicitly leaves open that possibility via national laws. This raises the question that if the function of central biometric repositories that were set up for the implementation of EC2252/2004 were extended at a later stage, it could be considered a case of function creep (Kindt 2012, p. 564).

Central storage of facial images will get another dimension as soon as governments make these images available for surveillance purposes. With the increase of video surveillance cameras in public and private spaces, camera images can be matched against these repositories. Police units can also use mobile scanning devices to identify people on the streets. Biometric modalities such as face and iris are typically well suited for such usage, as they can be captured on relative large distance and without a person's knowledge.

As demonstrated by the country studies of France and The Netherlands, the unregulated area within the regulation has been used to establish such databases and so extend the primary biometric function from verification to identification. But not all the installed databases have the same function: the Czech Republic stores facial images centrally, but these images are not searchable. The same goes for Norway and Italy. Germany decided otherwise. It only stores the quality data of the biometric images (not the images themselves), which is aligned to its objectives of monitoring, maintaining and improving the quality of the biometric data.

Extending the use of the biometric data taken for ePassports to law enforcement purposes has an impact on the quality requirements of the biometric data. The implementation of (EC) No 2252/2004 only requires two fingers to be scanned and stored in the passport. If 1:n searches need to take place through tens of millions of records, there are several system performance issues. Firstly, two fingers are not discriminative enough when used for searching in large scale databases causing large numbers of failures. More fingers will be needed to be stored in order to reduce the risk of failures. Secondly, the quality of the biometric data will become more critical if 1:n searches at such a scale are performed. Getting the proper quality for 1:1 verification has proven to be rather challenging (see reject rates in The Netherlands). For 1:n searches it is even more difficult. Taking high quality fingerprints that are suitable for law enforcement purposes is time consuming in the citizen domain. Current processes for application and issuance of the biometric passport are generally not sufficient for 1:n searches. Thirdly, there are no provisions on how to handle false matches, which can potentially put innocent citizens into the position

of being wrongly accused (Ashbourn 2005, p.8). This means that the biometric data taken for the ePassport therefore don't seem suitable for law enforcement purposes.

4.4.5 Privacy

General

In the context of biometrics, there are specific issues related to privacy. Biometric characteristics (face, voice, iris, fingerprints, etc.) are exposed and cannot be considered a secret like a password or pin-code. Technology is available to capture biometric features covertly, though with different degrees of difficulty. This could lead to identity theft, or linking a person to various events, actions or behaviour, causing potential privacy risks. Moreover, biometric features cannot be revoked, cancelled, or reissued if compromised, since they are the user's intrinsic characteristics and they are in limited number. In this context privacy means something more than just keeping biometric data secret or safe through data protection measures. It is relevant to consider the purpose of a biometric system and the limitations on the use of shared biometric information in relation to the original purpose determined for collecting the data.

A specific privacy related issue is that the European data protection framework is implemented differently in various countries (de Hert and Sprokkereef 2010; Lodge 2010). This can lead to different engagement in different Member States. The data protection framework may also overlap or interact with other relevant European or international legislation, such as the treaty of Prüm[58] (FIDIS 2007).

Biometric passport

Privacy issues regarding the biometric passport occur at four levels: the ePassport itself; the management and handling of the personal data (including biometrics) at border control checkpoints and other passport control situations; potential additional uses of centrally stored biometric data in conjunction with emerging commercial biometric databases; interaction with other European legislation, such as the Treaty of Prüm.

Biometrics can identify a person at any time and location, with or without their knowledge or consent. Some biometric data can reveal sensitive personal data, such as race or health related information. Biometrics can also link people to specific information, services, events and behaviour. Mandating the biometric passport means that most European individuals will be enrolled in a biometric system. This creates privacy and data protection risks for citizens with potentially far reaching consequences for the individual involved, especially when things go wrong such as a data security breach or biometric identity theft. And citizens have only limited legal power to correct mistakes.

It is mostly for these reasons that the data protection authorities (DPAs) in France, Germany, Norway and The Netherlands have criticized the introduction of biometrics to the passport, particularly with regard to a central repository of biometric data. In all these cases the DPAs were not convinced about the necessity and therefore the proportionality of the measure of (EC) No 2252/2004 in general and of a central biometrics repository in some specific cases (see also Article 29 Working Party, 2005). The Biometrics European Stakeholder (BEST) network concluded that European regulations should address the possible errors and technical failures inherent to any biometric recognition system, that the errors should be made available to the data subjects. BEST also recommended that compliance with privacy and data protection regulation needs to be enforced more strongly and that function (or mission) creep

[58] The Prüm treaty is an international police-cooperation agreement that was initiated by Belgium, Germany, Spain, France, Luxembourg, the Netherlands and Austria in May 2005 (informally also called 'Schengen III')

needs to be combated via the principle of proportionality. The network further recommended that European Regulations need to specify the rights of data subjects in case of failure (Lodge 2010; de Hert and Sprokkereef 2010; Venier and Mordini 2011). Within the EU, the data protection directive is implemented differently, which adds to the difficulties citizens face when trying to attain justice.

Moreover, the use of biometrics carries the risk of excluding or failing to detect certain groups of citizens. The performance of biometric recognition is dependent on physical aspects like age, social origin (e.g. workers performing heavy manual labour will have lower quality fingerprints) and race and is associated with the detection of specific health information, which can be sensitive to certain people or groups. In order to avoid exclusion, alternative methods will be needed for these groups. If no alternative methods are available or too expensive, certain people or groups might be excluded from services or rights. To address these issues Frontex has conducted an additional study addressing ethical aspects on machine assisted border control (Frontex, 2011b).

The country studies on The Netherlands and France show that (EC) No 2252/2004 has been used as a springboard for governments to go beyond the main objective of the regulation by creating a central biometric repository for detection and prosecution purposes. Norway also has this ambition. Germany, Italy and the Czech Republic have demonstrated their intention to restrict functionalities. The Article 29 Working Party concluded that the use of biometrics in passports "has to be technically restricted for verification purposes comparing the data in the document with the data provided by the holder when presenting the document" (WP 29 2004, p. 11).

Additional privacy risks are emerging with the addition of parallel European legislation such as the Treaty of Prüm and the tendency to centralize public administrations. This is another way in which the biometric passport could be part of a framework of centrally stored biometric data for law enforcement purposes, with international exchange through the Schengen Information System-II or the Treaty of Prüm. This would extend th original purpose of EC 2252/2004 and citizens might not know this when applying for a biometric passport.

Automated Border Control (ABC) systems

When used as part of border control systems, the biometric passport might contribute to the proliferation of citizen surveillance technologies. Personal data (including biometrics) captured by the ABC-gates can be stored and exchanged with other systems, such as CCTV and Departure Control. It should be clear and transparent to the traveler what information is being captured, stored and shared. Data collected following interaction of ABC systems with other external databases is not yet safeguarded. From a European perspective it is not clear where the captured information will be stored (if at all), whether it will be stored with other data or data sets and who has access to it and for what purpose.

With regard to the privacy and data protection aspects of ABC systems, experts from BEST Network concluded that the existing guidelines are poor. The lack of focus on this major issue was regarded as concerning. Frontex (2011b) conducted a study regarding ethical aspects on machine assisted border control. It concluded that there are significant gaps between national and EU codes of conduct and that existing codes of conduct are often not written specifically for border guards, thereby not addressing many of the ethically difficult tasks they perform.

4.4.6 Usability

The usability of the biometric passport, i.e. the extent that the biometric passport can be used for specific purposes, can be assessed in relation to the data subject, the user-friendliness of the biometric equipment and the usability of the biometric passport for border control.

There will always be a percentage of people whose biometric features can't be properly captured (e.g. because their fingers are damaged by labour or skin disease), which might lead to low quality images or no images at all. This group might never be able to use a biometric system. In order not to exclude these people from certain rights or services, alternative procedures and methods will need to be put in place. Another aspect of usability is the user-friendliness of the biometric process and equipment during the application and issuance process, and at border control checkpoints. The ergonomics of an installation is important for the acceptance and behaviour of the data subject and for a smooth and convenient process. Bad ergonomics might lead to mistakes and lengthy procedures. On the other hand, increasing the user-friendliness can also be achieved by lowering the thresholds in order to reduce the rejection rates. Both mistakes and lower thresholds can lead to a lower level of security and impact negatively on the usability of the biometric passport for border control.

In Norway the capturing of the biometric data during the application process takes as long as is required to obtain good quality images. This is exceptional, as most countries consider the capturing process should be as short as possible (preferably not exceeding a few minutes) for the convenience of the citizen and the operator. It is probably for the same reason that biometric verification at passport issuance is not performed. False rejections will be difficult to judge and to handle, as well as true rejections that are claimed to be false. Operators currently don't have the possibilities of making a judgment on that. If a passport is not to be issued due to a rejection, the applicant might get seriously annoyed as they will have to go through the application process again.

At ABC gates, this balance between security and convenience also counts: raising the security level of an ABC-gate (e.g. by setting the threshold for biometric matching at a higher level) might lead to higher rejection rates. This will reduce the usability of the ABC-gates.

4.4.7 Access Control

For this case study the issue of access control in relation to the biometric passport will be limited to the access to biometric and other personal data stored in the ePassport. Access to the conventional data (i.e. the data being printed on the identity page) will not be discussed here. The data that are stored in the chips of the ePassport include the personal data and facial image as well as the fingerprint images.

The personal data and the facial image, protected by the BAC mechanism (see also paragraph 2.2.3), can only be accessed when the owner of a passport opens it or when they pass it to a passport control officer to open. That implies that the passport owner can control to a certain extent who is reviewing the information and for what reason. The passport owner starts losing control as soon as digital information is stored in a digital device, such as an electronic passport reader or an ABC-gate. From that moment it will be harder for the passport owner to understand which systems and organizations will have access to this data. Security specialists claim that the wireless chip can also be read by unauthorized people and systems, and the BAC is not able to protect the information from all attacks (see also paragraph 4.2). In that case the passport owner might worry about unauthorized access to his/her personal data and facial image.

Another aspect is access to the biometric information by citizens. Article 4.1 of EC2252/2004 says that: "…. persons to whom a passport or travel document is issued shall have the right to verify the personal data contained in the passport or travel document and, where appropriate, to ask for rectification or erasure." Regarding stored fingerprints it seems that citizens are not always provided with that right, as verification at issuance in most cases does not take place.

4.4.8 Current policy discussions in Europe

Over the last few years, several discussions regarding the biometric passport have taken place at the Brussels Interoperability Group (BIG, see also 4.2), although the requirements and specifications of biometric images were not given a high priority on the agenda. In April 2010 the chairman of the BIG submitted a discussion paper on fingerprint images to the BIG meeting.[59] In order to discourage low quality images being stored in the passport chip, it was suggested that only fingerprint images with a high NFIQ score (1 or 2) should be stored because "….with today's matching algorithms an NFIQ score of 3 or less is not likely to be verified." It was also suggested that applicants with a low NFIQ score (3 or less) should not use automated finger validation locations. However, neither suggestion has been followed.

During one of the last BIG meetings on 25 May 2010, it was acknowledged that the quality of the biometric images will become important in the near future and that the BIG should be supportive of activities which aim to improve image quality. Unfortunately the BIG was dissolved shortly afterwards and no replacement body has been established. The issues regarding biometric image quality have been acknowledged, but no binding quality requirements or performance criteria have been established.

The latest decision on the EC2252/2004 regulation, from 4 August 2011 (C(2011)5499 F), does specify a minimum quality score for fingerprint images, but at the same time states that if this minimum score is not met, the images with the highest score should be taken. The C(2011)5499 decision also mentions the replacement of the Basic Access Control (BAC) by the Supplemental Access Control (SAC), thus introducing the 3rd generation of epassports. According to the timeline, the BAC should be replaced by 2025. SAC will improve the security of the non-EAC protected data (name, face). The development of the technical specifications is done by the ICAO.[60]

In paragraph 4.1 a comprehensive – and rather critical – report by Frontex on the security of the epassport was discussed. The study was commissioned by the Frontex Research and Development Unit. However, as far is could be investigated within the scope of this study, it was never formally sent to the European Parliament, nor was it ever presented to the LIBE administrator responsible for Frontex.

Based on questions from Member of European Parliament Sophie In 't Veld, the European Commission started an investigation on the implementation of the biometric passport in the Netherlands. The questions were primarily targeted to the aspects of privacy and human rights, but later questions were added regarding the quality and performance of the biometric data.[61] On 29 March 2012 the European Commissioner for Home Affairs Migration Ms Malmström stated that national accredited test labs are currently performing compliance tests[62]. In addition, she stated that the EC's joint Research Centre (JRC) has performed and reported on additional testing on the chips of electronic passports provided on a voluntary basis by some Member States to the Commission.[63] However, the quality of the facial image and fingerprint images stored in the chip, and the application, registration and issuance processes, were out of scope of these tests.

---

[59] Bob Carter, April 2010, "Issues with acquiring and recording of finger images: discussion paper for BIG"

[60] ICAO, 2011c, Technical Report Supplemental Access Control (TR-SAC)

[61] Questions for written answer E-001306/2012 to the Commission

[62] www.europarl.europa.eu/sides/getAllAnswers.do?reference=E-2012-001306&language=ES#def1

[63] EC/JRC ISPRA - JRC TEMPEST Testing Laboratory, Conformance Testing of 2nd Generation e-Passports

4.5 Concluding remarks and policy challenges

Biometrics can potentially significantly improve the link between the passport and its rightful owner. But policy makers at EU level have strongly underestimated the technical and practical implications of introducing biometrics to combat passport fraud and to raise the security level of border control. This has led to inadequate legislation at EU level with no clear criteria regarding the performance of biometric verification or uniform and verifiable criteria for the quality and integrity of biometric images. Taking facial images 'live' at issuance is not mandatory throughout the EU. In addition, security measures to protect the data on the chip of the passport itself seem to be insufficient (Basic Access Control, BAC) or non-interoperable in practice (Extended Access Control, EAC). Furthermore, the lack of available statistics regarding the actual size of different types of passport fraud, makes it difficult, if not impossible, to assess the effects and proportionality of EC Regulation No 2252/2004.

The lack of quality and integrity standards has created substantial differences in national implementations of the ePassport in European Member States. These differences include quality requirements for biometric data and the application and issuance process of the passport. They have resulted in various levels of performance between Member States. The lack of quality and integrity standards for biometric data seriously compromises the EU ambition to develop secure and interoperable biometric systems for border control purposes. Low quality images increase the chance of mistakes and induce a higher tolerance to quality thresholds in order to prevent too many rejections. This results in lower thresholds throughout the EU which threatens the overall security level of the ePassport verification process. Fingerprints are still not being used for border control, despite the fact that they were added specifically to provide a higher level of security. Border control in Europe still relies on facial images, whilst these data are more vulnerable to mistakes than fingerprints. Paradoxically, increased security for the fingerprints (Extended Access Control) seems to have created de facto non-interoperability between the Member States and non-use of the fingerprints. Technical complexity and seemingly lack of trust between countries hinder exchange of the digital keys that are necessary for using the fingerprints for border control.

The case study on the biometric passport also shows tension between a high level of security and high usability. High quality levels of biometric data and high security require careful procedures, certified personnel, take (considerable) time and may cause temporal inconvenience for citizens and government officials. It seems that most European countries considered convenience for citizens and government officials to be more important than demanding high quality requirements.

Another issue raised by the case study on the ePassport is that of function creep. The political climate after 9/11 combined with a general lack of biometrics knowledge led some countries to think that biometric data taken for the ePassport could easily be used for law enforcement purposes. There was insufficient distinction between the use of biometrics used for verification and for identification in the political discourse. Several countries created central repositories of biometric data to extend the function of the biometric data to law enforcement, even though biometric data taken for the ePassport does not seem suitable for that purpose. The creation of centralized biometric databases containing fingerprints and facial images has a wide range of technical, societal, legal and practical consequences. These have not been adequately anticipated. The amendment on Council Regulation (EC) No 2252/2004, enabling the possibility to use the biometric data for other purposes than originally intended via national laws, should have been considered more carefully at EU level.

A related issue is that policy makers, both at EU level and national level, have paid little attention to the legal position of the citizen and to implement redress procedures. Citizens currently have only limited legal power to correct mistakes made. Legislative frameworks regarding privacy, data protection and civil rights in general vary within the EU, which add to the difficulties citizens face when trying to attain justice.

Based on these observations, the following policy challenges for Europe can be formulated:

The first and main policy challenge is to develop uniform and clear standards with regard to four aspects that are currently not addressed by the EC 2225/2004 Regulation: 1) the required quality of biometric images; 2) the performance of biometric verification; 3) the application and issuance process; and 4) testing and certification schemes to make sure that standards are applied properly and that performance claims from vendors can be verified and compared. To improve the quality of the biometric images, facial images should be taken 'live' at issuance.

A second policy challenge for European policy makers that complicates the development of high quality standards is that different requirements, such as security, usability and convenience, may be at odds with each other and need to be carefully weighed against each other. Individual Member States may weigh security, usability and other requirements differently.

A third policy challenge is to improve the interoperability and security measures of the chip in the passport. The Basic Access Control (BAC) seems not sufficient and only prevents simple skimming attacks. The Supplemental Access Control will not replace BAC until 2025. The Extended Access Control (protecting the fingerprints) is more secure, but requires a successful exchange mechanism, which in turn, requires trust between Member States regarding each other's security and integrity standards.

The fourth policy challenge is to improve procedures for redress. The ways in which citizens can correct errors need to be clearly addressed when using biometric systems for border control purposes. Legislative frameworks regarding privacy, data protection and civil rights in Europe vary, which add to the difficulties citizens face when trying to attain justice.

4.6 References

- Article 29 Working Party (2004) *Opinion 3/2005 on Implementing the Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States*. WP 112 04/09/12, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp112_en.pdf

- Ashbourn, J. (2005) *The Social Implications of the Wide Scale Implementation of Biometric and Related Technologies*, for the European Commission Joint Research Center IPTS, Seville

- Bekker, R. (2012) *Onderzoek naar besluitvorming biometrie op reisdocumenten*, Report prepared for the Dutch Ministry of Internal Affairs

- Böhre, V. (2010) Happy Landings. Het biometrisch paspoort als een zwarte doos. Nr. 46. Rapport van de Wetenschappelijke Raad voor de Regering (WRR). Online available at

- http://www.wrr.nl/publicaties/publicatie/article/happy-landings-het-biometrische-paspoort-als-zwarte-doos-46/

- Breitenstein, M. Sanchez-Reillo, R. Peirce, M. et al. (2012) *D6.2 - Mapping Selected Applications Scenarios to their Respective Standards and Evaluation Schemes*. BEST Network

- Brauer, E. (2011) German Federal Ministry of the Interior, at the 7th EBF Biometrics Research Seminar, Brussels June 15th, 2011

- BSI (2004) *Evaluation of Fingerprint Technologies – BioFinger*. Report of Bundesamt für Sicherheit in der Informationstechnik. Available online at

https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Studies/BioFinger/BioFinger_pdf.pdf?__blob=publicationFile

- CBP (2007) *Adviesaanvraag wijziging Paspoortwet i.v.m de herinrichting van de reisdocumentenadministratie* ref.z2007/00010 College Bescherming Persoonsgegevens
- CNIL (2007) Decision No.2007-365. Commission nationale de l'informatique et des libertés
- Coetzee, L. and Botha, E.C (1993). Fingerprint recognition in low quality images. In *Pattern Recognition*, Vol. 26 (10), pp 1441-1460
- Conseil-constitutionnel (2012) Décision n° 2012-652 DC du 22 mars 2012. Loi relative à la protection de l'identité. Online available at:
- http://www.conseil-constitutionnel.fr/conseil-constitutionnel/english/case-law/decision/decision-no-2012-652-dc-of-22-march-2012.105428.html
- Council of the European Union (2010) Toledo Joint Statement: Joint Statement of the US Department of Homeland Security and Council of the European Union, (6261/10), adopted 21st January 2010.
- de Hert, P. (2005) *Biometrics: legal issues and implications.* Background paper for the Institute of Prospective Technological Studies.
- de Hert, P. and Sprokkereef, A. (2010) *D7.2 - Biometrics in Europe: Inventory on Biometric Data and Privacy Legislation* BEST Network
- Drahansky et al (2008) *Technické hodnocení biometrických systémů*, Brno, CZ, NBU, Czech National Security Agency
- European Commission (2000) No 2725/2000 concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of the Dublin Convention (11 December 2000)
- European Commission (2004) No 512/2004 establishing the Visa Information System (VIS) (8 June 2004)
- European Commission (2004) No 2252/2004 on standards for security features and biometrics in passports and travel documents issued by Member States (13 December 2004)
- European Commission C(2006) 3699 laying down the technical specifications on the standards for biometric features related to the development of the Visa Information System (22 September 2006)
- European Commission (2007) Council Document 5733/07 Need for systematic use of biometrics in checks at external borders (2007)
- European Commission Regulation (2009) No 444/2009 amending Council Regulation (EC) No 2252/2004
- http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:142:0001:0004:EN:PDF
- FIDIS (2006a) Budapest Declaration on Machine Readable Travel Documents (2006)

- http://www.fidis.net/press-events/pressreleases/budapest-declaration/#c1307
- FIDIS (2006b) *D3.14 The Privacy Legal framework for Biometrics*
- FIDIS (2007) *D3.10 Biometrics in Identity Management*, Chapter 3, Facts and Findings on Biometric Systems
- Frontex (2011a) *Operational and Technical security of Electronic Passports*. Online available at www.frontex.europa.eu
- Frontex (2011b) *Ethics of Border Security*
- Graham-Rowe, D. (2012) Aging Eyes Hinder Biometric Scans. In: *Scientific American*, May, 2012. Available online at: http://www.scientificamerican.com/article.cfm?id=aging-eyes-hinder-biometric-scans
- Grefrath, F. and Tekampe, N. (2010) Biometric Spoof Detection in the Context of Common Criteria. Presentation delivered at the 11th ICCC, Turkey
- http://www.11iccc.org.tr/4%20-20ID%20157%20Frank%20Grefrath%20-%20Biometric%20Spoof%20Detection%20in%20the%20Context%20of%20Common%20Criteria.pdf
- ICAO (2010) *Guide for Assessing Security of Handling and Issuance of Travel Documents*
- ICAO (2011a) *Recent developments of the public key directory*. Technical Advisory Group on Machine Readable Travel Documents (TAG/MRTD/20-IP/2), Montreal
- ICAO (2011b) *Towards better practice in national identity management* (TAG/MRTD/20-WP/5, 17/08/11) Technical Advisory Group on Machine Readable Travel Documents
- ICAO (2011c) Technical Report Supplemental Access Control (TR-SAC)
- Lodge, J. (2010) *D7.1 - Biometrics in Europe: Inventory on politico-legal priorities in EU27* BEST Network
- Kindt, E. (2012). The Processing of Biometric Data: a Comparative Legal Analysis with a focus on the Proportionality Principle and Recommendations for a Legal Framework, doctoral thesis, Leuven, KU Leuven Law Library (will be published with Springer (see www.springerlink.com), in the Law, Governance and Technology Series)
- NIST (2004) *Fingerprint Vendor Technology Evaluation 2003 - Summary of Results and Analysis Report*. NISTIR 7123, National Institute of Standards and Technology Available online at: http://www.nist.gov/customcf/get_pdf.cfm?pub_id=905710
- Sanchez-Reillo, R. (2012) presentation at European Biometrics Symposium, 17 February 2012 www.eab.org
- Schneider, J.K. (2010) *Quantifying the Dermatoglyphic Growth Patterns in Children through Adolescence*. Report prepared for US Department of Justice. Doc nr 232746. Online available at https://www.ncjrs.gov/pdffiles1/nij/grants/232746.pdf
- Seidel, U. (2009) Forensic Science Institute of the German Federal Criminal Police Office, Director Identity Documents Department. In *Keesing Journal of Documents and Identity*, Issue 29

- Schumacher (2010) *D1.1 Inventory of biometrics enabled registration processes for immigration purposes.* BEST Network
- Schumacher (2012a) *D1.2 How EU Policy Requirements Shall Translate into Daily Business*, BEST Network
- Schumacher, G. (2012b) *D1.3 Biometrics for Border Control: a Roadmap for Europe*. BEST Network.
- Snijder, M. (2010). *Het biometrisch paspoort in Nederland: crash of zachte landing*, Rapport voor WRR. Online available at
- http://www.wrr.nl/publicaties/publicatie/article/het-biometrisch-paspoort-in-nederland-crash-of-zachte-landing-51/
- Staatsblad (2009) Besluit van 12 juni 2009 tot vaststelling van het tijdstip van inwerkingtreding van enkele onderdelen van de rijkswet van 11 juni 2009 tot wijziging van de Paspoortwet in verband met het herinrichten van de reisdocumentenadministratie. Stb. Nr. 253 2009
- Tweede Kamer der Staten-Generaal (Dutch Parliament) (2010) *Brief aan de Tweede Kamer over evaluatie van de invoering van de vingerafdrukken in de Nederlandse reisdocumenten*, Kamerstuk , 18th March 2010
- Tweede Kamer (2012) *Reactie op het onderzoek naar besluitvorming biometric op reisdocumenten*, 12th April 2012, Kamerstukken II, 2010/11, 25 764, nr. 45
- UK Biometrics Working Group (2002) Use of Biometrics for Identification and Authentication. Advice on Product Selection.
- Venier, S. and Mordini, E. (2011) *D7.3 - Overview of the ethical, social and policy implications of biometrics* BEST Network
- Wilson, C., Hicklin, R. A., Korves, H., Ulery, B., Zoepfl, M., Bone, M.,
- Grother, P., Micheals, R., Otto, S. and Watson, C. (2003) *Fingerprint Vendor*
- *Technology Evaluation 2003 Analysis Report.* Report prepared for NIST. Available online at: http://fpvte.nist.gov/report/ir_7123_summary.pdf

Technical guidelines

- BSI: Conformity Tests for Official Electronic ID Documents, Part 4: Test plan for ICAO compliant Proximity Coupling Device (PCD) on Layer 2-4,Version 2.2. [BSI03105-4] Technical Guideline TR-03105.
- http://www.bsi.bund.de/ContentBSI/EN/Publications/Techguidelines/TR03105/BSITR03105.html
- BSI: Conformity Tests for Official Electronic ID Documents, Part 5.1: Test plan for ICAO compliant Inspection Systems with EAC 1.11, Version 1.2. [BSI03105-51] Technical Guideline TR-03105.

- http://www.bsi.bund.de/ContentBSI/EN/Publications/Techguidelines/TR03105/BSITR03105.html
- BSI Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control (EAC), Version 1.11. [BSI03110] Technical Guideline TR-03110.
- http://www.bsi.bund.de/ContentBSI/EN/Publications/Techguidelines/TR03110/BSITR03110.html
- BSI: Biometrics for Public Sector Applications, Part 1: Framework, Version 2.1. [BSI03121-1] Technical Guideline TR-03121.
- http://www.bsi.bund.de/ContentBSI/EN/Publications/Techguidelines/TR03121/BSITR03121.html
- BSI: Biometrics for Public Sector Applications, Part 2: Software Architecture and Application Profiles, Version 2.1. [BSI03121-2] Technical Guideline TR-03121.
- http://www.bsi.bund.de/ContentBSI/EN/Publications/Techguidelines/TR03121/BSITR03121.html
- BSI: Biometrics for Public Sector Applications, Part 3: Function Modules, Version 2.1. [BSI03121-3] Technical Guideline TR-03121.
- http://www.bsi.bund.de/ContentBSI/EN/Publications/Techguidelines/TR03121/BSITR03121.html
- ICAO: Machine Readable Travel Documents, Part 1 Vol. 2 and Part 3 Vol. 2 (Doc9303) http://www2.icao.int/en/MRTD/Pages/Doc9393.aspx
- IEFF: Cryptographic Message Syntax (CMS), August 2002 [RFC3369] RFC 3369.
- http://www.ietf.org/rfc/rfc3369.txt
- ISO: Identification cards: Integrated circuit cards[ISO7816].
- ISO: Identification cards: Contactless integrated circuit cards. Proximity cards [ISO14443]
- ISO: Information technology: Biometric application programming interface Part 1: BioAPI specification [ISO19784-1] ISO/IEC 19784-1:2006.
- ISO: Information technology: Biometric data interchange formats Part 5: Face image data[ISO19794-5] ISO/IEC 19794-5:2005.

Further reading material

- Baker, S.E. et al. (2009) Empirical Evidence for Correct Iris Match Score Degradation with Increased Time-Lapse between Gallery and Probe Matches. In *Lecture Notes in Computer Science*, Vol. 5558/2009, pp 1170-1179
- Biometrics Institute Ltd. (2008) Biometric Vulnerability: A Principled Assessment Methodology. White Paper

- Ratha, N.K et al Enhancing security and privacy in biometrics-based authentication systems. *IBM Systems Journal*, Vol. 40, No. 3, pp 614-634 (2001)
- Rife, D.C. (1953) Finger Prints as Criteria of Ethnic Relationship. *Am J Hum Genet*. Vol. 5(4), pp 389-399
- Zoberts, C. (2007) Biometric Attack Vectors and Defence. In *Computers and Security*, Vol. 26, pp 14-25
- Salter, C (2011) Common Criteria Reform – Better Security Products through Increased Cooperation with Industry. NSA/CSS Commercial Solutions Center
- *Readings from the BEST Network. BEST Network was a thematic network funded under the FP7 ICT Policy Support Program. The project started in October 2009 and ended in March 2012. The mission of the BEST Network has been taken over by the European Association for Biometrics, founded in November 2011 with the purpose of sustaining and expanding the network in Europe. The BEST Network deliverables listed here are available from www.best-nw.eu*
- BEST Network B.Dorizzi et al. D2.1 Survey of existing and emerging commercial biometric applications (2010)
- BEST Network D2.2 Inventory of factors for failure and success (2011)
- BEST Network D2.3 Emerging applications for biometrics: analysis of multi disciplinary factors for failure and success (2011)
- BEST Network N.Onland, M. Snijder et al. D3.1 Inventory of best practices biometrics at airports (2010)
- BEST Network J.Cave, N.Robinson, et al. D4.1 State of Art: Biometrics in eID systems (2009)
- BEST Network N.Robinson et al. D4.2 Exploring the business case for biometrics in remote electronic services
- BEST Network H.Leitold et al. D4.3 Biometrics in eID and eServices final report
- BEST Network F.Deravi et al. D5.1 Inventory of Training & Skills Provision (2010)
- BEST Network F.Deravi et al. D5.2 Developing European T&E capabilities: addressing the requirements and needs (2012)
- BEST Network A.Nouak et al. D6.1 - Inventory of Testing & Certification Institutions in Europe (2010)

5 CONCLUSION

The overall findings of the three case studies will be presented in this concluding chapter. First there will be a short summary of the most important conclusions from each case study. Subsequently the most relevant overall challenges derived from the case studies will presented.

This will be followed by an outline of the further approach of developing policy options about security of eGovernment services leading to a description of the scope of the upcoming STOA conference about security of eGovernment services and systems.

5.1 Conclusions from the eProcurement case study

1. The interest of European contracting authorities in conducting cross border, fully electronic procurements does not appear to be sufficiently proven in the studies identified, so the obstacles could be explored in greater depth.

2. Country-specific regulations and requirements could be reduced.

3. Procurement systems run by local contracting authorities should not be discouraged by putting too much emphasis on central systems. Having a large number of local systems will provide more robustness against attacks from the Internet such as crafted attacks via Trojan horses on data such as prices, as well as against distributed denial of service attacks. However, bidders will wish to inform themselves about new bids and participate easily, so the issue of interoperability of any signing and encryption tool emerges.

4. Unhackable compartmentalisation of computers would help fight malware, and would provide a secure environment for any kind of authentication and encryption, including any client code. Therefore moves towards such compartmentalisation could be supported by the European governments.

5. Tools for authentication and encryption should be available at a European scale, not only in a single country, with suitable registration procedures, i.e. a European trust framework. Encryption must make sure that bids remain encrypted until the submission deadline, even if insiders collude.

6. The economic case for digital signatures needs to be clarified, e.g. by collecting data in countries with long experience (including costs for validation, time-stamping or re-signing), by interviewing experts and by performing projections. European legislation should remain open for various means of authentication until the case of digital signatures is better proven. Weak forms of authentication could be used if the parties intend to sign a paper contract anyway.

7. Certification authorities may need to be controlled more tightly, if not even government-run.

5.2 Conclusions from the eHealth case study

1. Personal health data is sensitive information and its theft, loss, or unauthorised use or disclosure entail serious consequences for the individuals involved. The introduction of full-scale eHealth solutions raises a number of important questions. What are the social and economic costs and are they acceptable? What safeguards are and should be in place to promote privacy and security? This discussion becomes more complicated when we consider cross-national health

care applications. This requires at least an acceptable and commonly agreed security baseline to be obtained by the European countries, and it becomes a common policy issue to ensure alignment among Member States in obtaining common security standards.

2. The national projects from UK and Estonia illustrate the need for a precisely formulated strategy and purpose as well as well-defined and accepted security and privacy set of guidelines from the outset.

3. An important conclusion from the cross-European eHealth projects is that the establishment of binding security agreement between participating entities is vital.

4. A related observation is the necessity of embedding privacy and security concern in the early design phase of any EHR system, and as seen in the Estonian example, preferably based on a general ID infrastructure. Also epSOS is looking to the pan-European ID infrastructure as proposed and tested in STORK 2. It seems that a common identity structure will be much more acceptable than any ID-scheme developed domain by domain or sector by sector.

5. The diversity of Health systems in Europe with regard to privacy legislation, policies and local procedures and different level of compliance with EU policy recommendations - both in regard to interoperability and to data protection - represent major barriers for deployment of cross-border health services and exchange of EHR.

6. In both pan-European projects, the actual management of the security of the system is left with the individual members states. This evades the difficulty of handling differences in legal requirements and may potentially hamper the creation of mutual trust and confidence.

7. Technical and semantic interoperability among health information and communication systems and standards remains a challenge to both Member States and the EU level.

8. There is a need to address policies and procedures for harnessing multiple functionalities of EHRs such as secondary use of health data for research purposes, population health monitoring and quality monitoring. The threats not only come from insurance companies, employers or pharmacy industry, but also from the parallel drive to support 'Open Government Data', which poses a special risk when it comes to personal health data. Minimum standards for anonymisation of such use should be implemented as part as the overall concept of baseline security.

5.3 Conclusions from the ePassport case study

Potentially biometrics can improve the link between the passport and its rightful owner significantly. But policy makers at EU level have strongly underestimated the technical and practical implications of introducing biometrics to combat passport fraud and to raise the security level of border control. No clear criteria regarding the performance of biometric verification have been set, nor are there uniform and verifiable criteria for the quality and integrity of biometric images. The lack of standards has created substantial differences in national implementations of the ePassport and differing levels of performance. The lack of quality and integrity standards for biometric data seriously compromises the EU ambition to develop secure and interoperable biometric systems for border control. In addition, security measures to protect the data on the chip of the passport itself seem to be insufficient (Basic Access Control, BAC) or non-interoperable in practice (Extended Access Control, EAC). Furthermore, the lack of available

statistics regarding the actual size of different types of passport fraud, makes it difficult, if not impossible, to assess the effects and proportionality of EC Regulation No 2252/2004.

Based on the case study observations, the following policy challenges for Europe can be formulated:

1. The first and main policy challenge is to develop uniform and clear standards with regard to four aspects that are currently not addressed by the EC 2225/2004 Regulation: 1) the required quality of biometric images, 2) the performance of biometric verification 3) the application and issuance process and 4) testing and certification schemes to make sure that standards are applied properly and that performance claims from vendors can be verified and compared.

2. A second policy challenge, that complicates the development of high quality standards, is that different requirements, such as security, usability and convenience may be at odds with each other and need to be carefully weighed against each other. Individual Member States may weigh security, usability and other requirements differently.

3. A third policy challenge is to improve interoperability and security measures of the chip in the passport. The Basic Access Control seems not sufficient and only prevents simple skimming attacks. The Supplemental Access Control will not replace BAC until 2025. The Extended Access Control (protecting the fingerprints) is more secure, but requires a successful exchange mechanism, which in turn, requires trust between Member States regarding each other's security and integrity standards.

4. The fourth policy challenge is to improve procedures for redress. The possibilities for citizens to correct errors need to be clearly addressed when using biometric systems for border control purposes. Legislative frameworks regarding privacy, data protection and civil rights in Europe vary, which add to the difficulties citizens face when trying to attain justice.

5.4 Overall conclusions

Based on the policy challenges of the three case studies described above, this section will present the overarching conclusions regarding secure eGovernment systems. Firstly, we will highlight two main elements that can be derived from the case studies: the need for a common security baseline and the need to realize more control for citizens, businesses and employees over data. This is followed by a discussion of eight challenges that follow from these two main elements.

5.4.1 Common security baseline

The case studies show a need for a common security baseline for eGovernment systems in the European Union that protects citizens, businesses and employees from large damages. The baseline should be based on a minimum common standard, which should aim at a high security level where eGovernment systems and/or Member States need to 'lift' to. This high security level, however, may require radical and fundamentally different design choices that may not be feasible in terms of other requirements, such as interoperability, existing (legacy) systems, data subject control over data (or avoidance of personal data storage), financial investments etc. A high security level may for example require systems that do not make use of the Internet, refrain from Commercial-Off-the-Shelf (COTS) components, demand in-house manufacturing of hardware components, i.e. may require eGovernment systems to be technologically unique. The 'ideal' security solution may thus not be the 'ideal' solution in praxis. This would mean that some security risks have to be accepted. But what are acceptable risks and what does that mean for the design of eGovernment systems? Effectuating a common security baseline then brings the overall challenge of finding an adequate level of security, which can be combined with other

demands such as interoperability, privacy, usability, existing legislation etc. and that is responsive to technological advancements (in terms of malware and security threats as well as with regards to interoperability and privacy solutions).

5.4.2 Control over data

The case studies show, particularly in eHealth and the ePassport that significant privacy risks occur for citizens with eGovernment systems that collect, store, process and exchange personal or confidential data, while citizens have limited possibilities to address privacy infringements and correct errors. Different national implementations of the current data protection directive (95/46/EC) add to the difficulties citizens face when trying to attain justice. Therefore, it is necessary to focus on better control mechanisms for personal or confidential data and give citizens and other players a better technical and legal position to exercise control over their data.

5.4.3 Policy Challenges

From these two main observations, the following overall policy challenges can be formulated:

Purpose specification and level of interoperability

When deciding upon the establishment and design of an eGovernment system, the purpose of the system, its necessity and the proportionality regarding the data to be collected should be considered thoroughly. The case studies show that it is not always sufficiently clear what data actually needs to be exchanged and for what purpose. Therefore, the required level of interoperability as well as the feasible level of technical harmonization (and specification) between Member States has not been sufficiently defined. There is a need to clearly specify the overall purpose of the eGovernment system. The required level of interoperability should be based on the purpose specification.

Too high political ambitions and too little awareness of complexities

Defining the precise purpose of an eGovernment system requires sufficient awareness of policy makers of the technical possibilities and impossibilities of the system, organisational consequences and possible legislative conflicts. Too often this complexity is inadequately reflected in the policy making process regarding the establishment of eGovernment systems, resulting in too high policy ambitions with respect to what technology can actually deliver.

Safeguarding security and privacy

In order to meet a high(er) level of security, more investments in security measures are needed, i.e. with regard to verification and authentication procedures, training government officials, or protection against malware attacks. Alternative approaches for secure components, better isolation, and higher levels of certification should be considered. With regard to safeguarding privacy, technical measures that enhance data protection (attribute-based credential technologies, encryption, decentralised data storage, data pseudonymisation) and facilitate citizen's exercise of their legal rights to inspect and correct their own data should be considered (privacy by design).

Does one size fit all?

Another question raised by the case study findings is whether different eGovernment systems require different choices regarding the level of interoperability and harmonization. The ePassport case shows that a lack of technical harmonization compromises the overall security

level of border control in the EU. However, the eProcurement case shows that less technical harmonization (i.e. using a variety of security tools) might result in different degrees of resilience against malware attacks. Other approaches, such as STORK and epSOS, build on national systems and use national gateways that specify security levels to exchange data. With regard to a common security baseline, what lessons can be drawn from these approaches? Are they best practices for all eGovernment systems in Europe? Or is it possible to scale successful experiences in small countries like Estonia to a European level?

Interferences between requirements

The cases show that different requirements, such as security, interoperability, privacy and usability may be at odds with each other and need to be balanced in designing and implementing an eGovernment system. In the ePassport case, a high level of security decreases usability (for example regarding careful and timely procedures for taking fingerprints) and higher security in a subset of implementations resulted in non-interoperability. In addition, interoperability between systems and across borders may enable function creep and create (additional) privacy risks. Different requirements also have organisational consequences for (government) organizations that operate the system. For example, in the case of ePassport, municipality offers need sufficient training and certification in order to take high quality biometric data, to verify the quality of the biometric data and to recognize fake fingerprints. Lastly, high security solutions have financial impacts: higher levels of security typically require higher financial investments.

Full digitalisation?

Full digitalisation may not always be the optimal solution: as mentioned above, the case studies illustrate that policy makers often lack sufficient awareness regarding technical (im)possibilities of eGovernment systems, resulting in too high policy ambitions. For eProcurement, a combined solution of password-based eTendering and paper contracts may be an efficient and safe solution. This point relates to the difficulties in specifying the purpose of the system, and requires acknowledgement of the technical possibilities and organizational consequences as well as iterative dialogues between government officials and ICT experts.

Standardization

All cases show a lack of technical and legal harmonization to enable interoperability between Member States. As a result of this lack of harmonization, interoperability and security can be compromised. Formulating the required standards of harmonization is a challenge in its own right, not least because the standardization should be flexible enough to be able to incorporate the continuous technological developments regarding (the protection against) malware threats, privacy solutions, etc.

On the basis of the three case studies the above security related challenges in the way eGovernment services are designed, implemented and operated at European level today have been identified. These security challenges are pivotal in order to have secure European eGovernment services in the future. In cooperation with the expert group of the project an approach for further debate and analysis of the possible solutions and policy options related to the challenges has been defined. The approach is a life-cycle approach and it is described further in the following. This life-cycle approach will also define the scope of the conference together with the challenges identified.

5.5 The life cycle approach

The identified challenges can be split into four groups which each relate to a phase in the life cycle of an eGovernment service, the four phases are:

1. The decision phase
2. The design phase
3. The operational phase
4. The decommissioning phase

The Life-Cycle Approach allows for defining and analysing the European level challenges in the light of the life-cycle of an EU-level eGovernment service. Talking about the life-cycle of an eGovernment service can easily be misunderstood as if there is an ideal approach, which can solve all challenges of making secure eGovernment services. This is not the case. The life-cycle approach highlights some important aspects – and related challenges - of making secure eGovernment services, but there are no easy solutions. What may sound straightforward becomes very complex when specified and related to concrete services – the devil is in the detail.

Furthermore it is important to stress that the life-cycle approach is exactly that – a cycle. It can never be seen as linear but is rather an iterative process in which the different phases constantly refer to and affect each other.

The life-cycle approach is foremost a frame that helps understanding and analysing the consequences of a number of choices that is made in relation to eGovernment systems. Decisions that affect the security of the system in ways that cannot easily be understood when looking at the details, but in the light of the life-cycle approach the interconnections and interdependencies of decisions are revealed. The life-cycle approach helps to get overview and to analyse challenges and possible solutions.

The four phases in the life-cycle approach and the related overall challenges are described in the following, but before describing the four phases there are three general principles.

General principles

The first general principle is that there should be a *European baseline of security* of eGovernment services. Such a baseline can potentially ensure a minimum level of security in all EU eGovernment services. This baseline must be defined at the political level and will be a guiding principle for the life-cycle of every eGovernment system. What it means in practical life depends upon the systems involved.

This leads to the next general principle that there must be a *connection between security baseline challenges and research priorities*. Research priorities should reflect the demands of securing eGovernment systems and possibly a road map of different scenarios of development could guide research in the field.

A third general principle concerns the procurement rules related to developing eGovernment systems. *The procurement rules must be more flexible* in order to allow for knowledge building in the development of a system and incorporating the newest technology as it becomes available and/or proves its security level.

Decisions phase

The first phase in the life of an eGovernment service is the decisions phase. This is where decisions are made about establishing an eGovernment service and the decisions taken at this stage will define and steer the further design, development and operation of the service and the system behind it. Therefore decisions taken in this phase are absolutely crucial for the security of the eGovernment system.

The three case studies have exemplified what challenges can occur in this phase and what the consequences of not meeting these challenges can be. The most important overall challenge is to decide on the very precise purpose of the eGovernment service. A precise definition of the purpose is absolutely crucial to the possibilities of ensuring security when it comes to the design and operation of the eGovernment system behind the service.

In short the most important challenges in the definition phase are:

- Insufficient knowledge base when political decisions are taken about establishing new EU level eGovernment services
- A mismatch between political ambitions and realistic possibilities (technical, organisational and legislative)
- The two above challenges leading to the overarching challenge of imprecise definition of the purpose of eGovernment services, which makes it very difficult to design, implement and operate secure eGovernment services and systems

Design phase

The second phase in an eGovernment life-cycle is the design phase. In this phase the system behind the service is designed and this includes a number of choices that in the end will define the level of security as well as other requirements, such as interoperability, privacy and usability. In the design phase decisions are taken about technological solutions, organisational and social requirements, level of security related to possible threats, consequences of security breaches and resilience measures.

In short, the basic challenges of the design phase are:

- Implementing security and privacy by design (control, data minimisation, transparency, resilience)
- Ensuring proportionality in security measures related to likely threats
- Finding technical solutions that can meet the EU level eGovernment security baseline
- Matching the technical solutions with the relevant organisational and social design solutions
- The above leading to the overarching challenge of setting the rules of a design phase that promotes secure eGovernment service systems complying with the requirements of privacy, proportionality, security and usability

Operational phase

The third phase of the life-cycle approach is the operational phase. The operational phase refers to the actual operation of the eGovernment service and system. In the operational phase the emphasis is on compliance and the effects on the security level of the eGovernment system. It is important that the system is operated in a way that does not reduce the security level that was implemented in the design phase. The case studies have clearly shown that the operation of the system can compromise security and it is challenging to meet the organisational requirements that can counteract security breaches.

In short the most important challenges of the operational phase are:

- Establishing transparency and democratic audit or control in the operation
- Ensuring a high level of competency among users to reduce risk of security breaches
- Maintaining the defined security level by being resistant towards security challenges from changes (technological, organisational, legislative etc.)
- The above challenges points to the need for increased focus on the operational challenges and the need for standardising and harmonizing the training and certification of personnel in the operation of eGovernment services

Decommissioning

The fourth phase of the life-cycle of an eGovernment service is the possible decommissioning of the service and the system. The challenges related to decommissioning are about what happens to the data in the system if it is shut down or if it is merged with another system. It must be considered what kind of data the system contains and what the ethical and privacy-related dilemmas of function/mission creep, data pooling and the risk of lowering the security level when merging systems are.

In short the most important challenges related to the decommissioning phase are:

- Deleting data when shutting down an eGovernment system
- Maintaining the level of security when merging systems

This life-cycle approach gives an opportunity life cycle gives an opportunity to have an overview of and discuss the many interconnected challenges that arise when securing eGovernment systems. The life-cycle approach and the overall challenges from the case studies are the frame of scoping the conference.

5.6 Conference scope

The conference will be a 1-day conference in the European Parliament. The target group of participants will be MEPs, ICT and security experts and all interested in the subject of secure eGovernment services. The aim is to have 50-100 participants. The venue will be the European Parliament and the conference will be designed within the frame of a STOA conference. The conference will build on presentations from experts and stakeholders and debate with MEPs/stakeholders/other experts about policy options related to securing EU eGovernment systems. It has been suggested to have the conference in February 2013 and the precise date will be decided in dialogue with the STOA secretariat and with the aim of ensuring participation of relevant MEPs.

The scope of the conference will be structured around the life-cycle approach to eGovernment services and systems. The life-cycle approach will be presented and policy related challenges for each phase of the life-cycle will be debated. Furthermore three cross-cutting security issues of high importance to security in eGovernment will be presented and debated. In the end of the conference the questions of a security baseline will be taken up.

Examples from the case studies will be used in all parts of the conference to illustrate concrete challenges related to different applications of eGovernment services. The overarching aim of the conference is to focus on and debate possible policy actions on EU level.

In order to clearly illustrate the outline of the STOA conference to be carried out we hereby describe a first draft of the programme of the conference. The draft does not deliver a complete programme and is not fixed in any way. It can be changed when planning the conference. The relevant changes will be discussed with the STOA secretariat and if requested and feasible with the STOA panel.

5.6.1 Draft Programme

1. **Setting the scene – Security of European eGovernment services in a life-cycle perspective**

Presentation of the findings from the three case studies focusing in the overall challenges derived from the cases. Explaining the life-cycle approach that will set the scene for the conference

2. **Life cycle phases and the connected challenges:**

    1. Decision phase:

a. Purpose; what data needs to be exchanged and why?
b. Proportionality

2. Design phase:
   a. Level of required interoperability
   b. Level of required digitalisation
   c. Organisational and social consequences; level of personnel training, EU certification etc.

3. Operational:
   a. Protecting against malware
   b. Enforcing privacy principles and control in practice
   c. Interferences between requirements (security, interoperability, usability)

4. Decommissioning:
   a. Best practices in how to delete data
   b. Security issues when merging systems

3. Cross-cutting issues

a. The challenges of protecting against malware and attacks from the internet

What are the security challenges about?

Solutions: What is state of the art in technology options? What are the future options? What are the policy options?

b. How to ensure privacy

What are the privacy challenges about?

Solutions: What is state of the art in technology options? What are the future options? What are the policy options?

c. Interference between security, interoperability, privacy and usability

To what extent does a high level of security interfere with other requirements regarding interoperability, privacy and usability?

Solutions: What is state of the art in technology options? What are the future options? What are the policy options?

4. **European security baseline for eGovernment systems – is that possible?**

Is there such a thing as 100% security? Which risks do we need to accept? What does that mean for the purpose, design and operational choices of eGovernment systems?
Why have a security baseline? How can it improve the level of security? What are the challenges related to defining a baseline? How could it be done? What are policy options?

This document is the Case Study report of the STOA final report 'Security of eGovernment Systems'.

The STOA studies can be found at:
http://www.europarl.europa.eu/stoa/cms/studies
or requested from the STOA Secretariat: STOA@ep.europa.eu

In addition a short Options Brief is also accessible through the STOA studies website via this QR code:

This is a publication of the
Directorate for Impact Assessment and European Added Value
Directorate General for Internal Policies, European Parliament

PE 513.510
CAT BA-02-13-353-EN-C
DOI 10.2861/34324
ISBN 978-92-823-4767-6