EUROPEAN PARLIAMENT

Security of eGovernment Systems

Final Report

Science and Technology
Options Assessment

STOA

Security of eGovernment Systems

Final 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 for 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, 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.

Reproduction and translation for non-commercial purposes are authorised, provided the source is acknowledged and the publisher is given prior notice and sent a copy.

Manuscript completed in July 2013.
Brussels, © European Union, 2013.

ISBN 978-92-823-4618-1
DOI 10.2861/29262
CAT BA-01-13-378-EN-C

Abstract

The project 'Security of eGovernment systems' aimed at assisting policymakers in discerning policy options for meeting future challenges in securing eGovernment systems. The project focused on upcoming challenges of eGovernment security in delivering public services across borders. Through identifying key security barriers and enablers, the project points to promising avenues of policy development in an environment of rapidly changing ICTs and changing socio-economic concerns in the EU.

The most important contribution of the project is the development and assessment of 11 policy options.

Policy Option 1: Develop a policy strategy for improving the security of IT-systems used in Europe

Policy Option 2: Stimulate development and use of security checklists (short-term)

Policy Option 3: Policy Option 3: Encourage the development and use of highly secure components (mid-term)

Policy Option 4: Encourage the development and use of highly secure systems (long-term)

Policy option 5: Create stronger institutional supervision and oversight of security

Policy option 6: Build a 'Privacy by Design' knowledge base

Policy option 7: Substantiate the data minimization principle by using anonymization techniques in all European eGovernment systems

Policy option 8: Stimulate technical and legal solutions that avoid or limit privacy risks caused by re-identification of previously anonymized data

Policy option 9: Make Privacy Impact Assessments of eGovernment systems mandatory and public

Policy option 10: Use gateways to achieve interoperability of different national eGovernment security tools, but aim at Europe-wide availability and usability of tools

Policy option 11: Ensure open and transparent evaluations of the trade-offs between privacy, security, usability, interoperability and costs of an eGovernment system.

Table of Contents

Executive summary

In April, 2011, the project 'Security of eGovernment Systems' was initiated by the STOA Panel of the European Parliament.

The aim of the project is to assist policymakers in discerning policy options for meeting future challenges to securing eGovernment systems. The project has focused on upcoming challenges to eGovernment security in delivering public services across borders. By identifying key security barriers and enablers, the project points to promising avenues of policy development in an environment of rapidly changing Information and Communication Technologies and changing socio-economic concerns in the EU.

The project has analysed and discussed the security of eGovernment systems and services, paying special attention to the possibilities of future EU eGovernment services, by:

- Gathering typical examples of existing national and international eGovernment services in Europe
- Analysing the most relevant security issues and possible responses/solutions to these issues
- Debating policy options for advancing EU eGovernment services
- Assessing and delivering specific policy options

This final report presents the main results of the project. It contains an introductory chapter outlining the scope of the project (Chapter 2), followed by the results of three case studies of eGovernment applications (eProcurement, eHealth and ePassport) and some specific policy options (Chapter 3). Chapter four presents the main results of the conference regarding policy challenges for secure eGovernment systems. The concluding chapter (Chapter 5) contains the policy options assessment, specifying detailed overarching policy options.

Overarching policy options

In addition to the detailed case studies of three different applications of eGovernment, the most important outcome of the project is the development and assessment of 11 overarching policy options. The policy options are grouped by four overall objectives:

1. Improving the resilience of European eGovernment systems
2. Increasing privacy protection
3. Achieving interoperability
4. Matching political ambitions with technological possibilities and benefits

Below, descriptions of the aims and associated policy options are summarised. An overview of all policy options can be found in Box 1.

Overview of policy options

Aim 1: Improving the resilience of European eGovernment systems

Policy Option 1: Develop a policy strategy for improving the security of IT systems used in Europe

Policy Option 2: Stimulate development and use of security checklists (short term)

Policy Option 3: Encourage the development and use of highly secure components (medium term)

Policy Option 4: Encourage the development and use of highly secure systems (long term)

Policy option 5: Create stronger institutional supervision and oversight of security implementations at the EU and Member State levels

Aim 2: Increasing privacy protection

Policy option 6: Build a 'Privacy by Design' knowledge base

Policy option 7: Substantiate the data minimization principle by using anonymization techniques in all European eGovernment systems

Policy option 8: Stimulate technical and legal solutions that avoid or limit privacy risks caused by re-identification of previously anonymized data

Policy option 9: Make Privacy Impact Assessments of eGovernment systems mandatory and public

Aim 3: Achieving interoperability

Policy option 10: Use gateways to achieve interoperability of different national eGovernment security tools, but strive for Europe-wide availability and usability of tools

Aim 4: Matching political ambitions, technological possibilities and benefits

Policy option 11: Ensure open and transparent evaluations of the trade-offs between privacy, security, usability, interoperability and costs of an eGovernment system

Box 1 Overview of Policy Options

Aim 1: Improving the resilience of European eGovernment systems

The objective of a common European security baseline is to raise the general level of security in European eGovernment services and systems. The development of such a baseline starts by outlining a security strategy on a political level that presents a roadmap of security measures for Europe. Implementing a security check list could be the short-term measure to start improving the level of security of eGovernment services. In the medium-term perspective, it would be relevant to start looking at policy options that can achieve security by design of crucial components. In the long term, policy measures that push for highly secure entire IT systems become relevant.

Policy Option 1: Develop a policy strategy for improving the security of the IT systems used in Europe

The objectives of this comprehensive security strategy are to address all the uses of IT systems in Europe and to develop policy measures to be taken in the short run (e.g. the use of security checklists), in the medium term (including directions for future legislation, for example, to make the certification of

software development processes mandatory) and in the long term by describing more 'radical' new ways of ensuring security, such as a "clean slate" design such as pushed by the US DARPA.

Policy Option 2: Stimulate development and use of security checklists (short term)
There are various checklists available to improve the security of running servers. Such lists should be followed more comprehensively by more organisations, including government institutions. The use of such lists should be evaluated, the development of tools for the automation of the procedures may need to be encouraged, and finally one or more lists could be recommended for use in eGovernment, or even be made mandatory.

Policy Option 3: Encourage the development and use of highly secure components (medium term)
Depending on the threats, the aim should be the production of more secure components, be it operating systems, application software or tamper-resistant components. The use of certified product evaluations or certified development processes could be made mandatory, but this will be very hard to enforce if components are produced outside the EU. Also, the discussion and implementation of product liabilities could help to create demand for better software.

Policy Option 4: Encourage the development and use of highly secure systems (long term)
In the long run, it would be feasible to use computer systems with a much higher resilience to malware. A classical approach is to use isolation for separating sensitive applications from insecure ones. Industry is pursuing such approaches, ranging from using isolation with existing systems to developing proven isolation. The US DARPA (2013) is attempting to design such systems in its "Crash" project. This process could be pushed by various means, starting with creating awareness, producing communications (by the Commission, Parliament, or e.g. trans-Atlantic working groups), supporting research and ending with legislating rules on the liability of the producers of IT systems and the quality of systems and components (e.g. certified or proven). Such more secure computing environments would also be beneficial if digital signature solutions were attacked. A system with secure user input and output would be an upgrade of a "qualified signature" card being used in an off-the-shelf computer.

Policy option 5: Create stronger institutional supervision and oversight of security implementations at the EU and Member State levels
Various problems justify strong and fast supervision of IT-security processes. For example, industrial software has been hacked, IT-security companies have been attacked successfully, and certification authorities have been intruded. Foreign-made components will lead to new risks, and countermeasures will need to be updated. Different institutional arrangements of such supervision are possible and need to be evaluated.

Aim 2: Increasing privacy protection
This report shows that eGovernment systems pose significant privacy risks for citizens with regard to the collection, storage, processing and exchange of personal or confidential data. It is clear that there is a need for improved privacy protection, such as giving citizens and other players a better technical and legal position enabling them to exercise control over their data. The European Parliament and the Council are currently discussing a new proposal for a General Data Protection Regulation (EC, 2012) to replace the current Directive 95/46/EC. The following policy options build on the measures proposed in the draft regulation and propose additional measures to increase privacy protection in Europe.

Policy option 6: Build a 'Privacy by Design' knowledge base
Privacy by Design (PbD) is currently included in the revised draft regulation for data protection in the EU (EC 2012), referred to as 'Data Protection by Design'. This will increase the incentives both for suppliers of IT systems that process personal data and for (government) organisations that procure such systems to implement privacy by design. To further stimulate the adoption of PbD, it is necessary for a

public knowledge base to be developed that includes reference architectures, design patterns, anonymisation and pseudonymisation techniques. This would specify what Privacy by Design entails, showcase practical experiences and improve the level of general knowledge in the EU about Privacy by Design. The availability of such a knowledge base, and possibly its mandatory use, would strengthen the skills and capabilities of IT suppliers, IT professionals and programmers to implement privacy-enhancing features in their systems.

Policy option 7: Substantiate the data minimization principle by using anonymization techniques in all European eGovernment systems

An important element of the data protection framework in Europe is the principle of data minimization, limiting the collection of personal information by data controllers to what is directly relevant and necessary to accomplish a specified purpose. A strong way to implement this principle is to limit the amount of personal data that is collected, stored, processed and exchanged by governments. This can be achieved by privacy-enhancing techniques such as attribute-based credentials, encryption, decentralised data storage, anonymization and pseudonymization. These techniques have matured and are deemed ready for commercial use. This would enable government organisations that procure IT systems to mandate the use of such techniques in their systems.

Policy option 8: Stimulate technical and legal solutions that avoid or limit privacy risks caused by the re-identification of previously anonymized data

Large datasets from governments and organisations – and their combination – can contain or may reveal the personal data of citizens. Even anonymised datasets pose privacy risks as the technical means to fully anonymise personal data is very difficult. Anonymised data can be recombined with other datasets, and individuals can subsequently be 're-identified'. Funding is needed for the research and development of technical solutions that hinder de-identification and improve the full anonymisation of datasets. Also data protection regulation could restrict the use of anonymised data to healthcare and research purposes with a 'high public interest' (Brown et al 2011), or it could ensure a minimum level of transparency by notifying data subjects and offer them a means to opt out, or by asking for their consent (opt in).

Policy option 9: Make Privacy Impact Assessments of eGovernment systems mandatory and public

Privacy Impact Assessments refer to standardized and systematic procedures to identify the privacy risks posed by systems that process personal data, and to identify ways to prevent or mitigate them. PIA's or 'data protection impact assessments' are now included in the new EU draft data protection regulation. To maximize the benefits of conducting PIA's, an additional policy option is to make PIA's publicly available (redacted if necessary) to promote public scrutiny and trust in eGovernment systems. This might heighten evaluation of the purpose and eligibility regarding data usage and storage.

Aim 3: Achieving interoperability

Interoperability poses another big challenge to cross-European eGovernment systems. Interoperability between systems and/or between countries is difficult to achieve and may constitute one of the most important barriers for European eGovernment services. With regard to security this is very much a question of the exchange of data, e.g. between different national eGovernment systems. Using 'gateways' is a pragmatic way to address interoperability for cross-border eGovernment systems in Europe. Gateway servers would check whether requirements, e.g. with regard to user identification, are met by a certain 'foreign' procedure (e.g. a procedure from another eGovernment system). The gateway provides an automatic response to the party which has made the initial request.

Policy option 10: Use gateways to achieve interoperability of different national eGovernment security tools, but strive for Europe-wide availability and usability of tools

Considering the EU's unique situation (of 27 Member States, each with its own legislation, systems and organisations), gateway computers can be used to achieve interoperability of national security tools, such as ID or smartcards. However, using such an infrastructure may lead to significant transaction costs, as it involves various national entities producing statements about the validity of a signature, using relevant auxiliary services, such as servers knowledgeable about national requirements and lost keys. Therefore it would be desirable for any security tool to be usable across Europe. Competition between a variety of tools might be good, but each tool, e.g. an advanced signature, should be available in all the countries and usable abroad. This may require far-reaching changes in the European legal setup, but would be very beneficial to achieve a real common market.

Aim 4: Matching political ambitions, technological possibilities and benefits

The decision regarding the development and subsequently the design of an eGovernment system inherently involves political choices regarding safeguarding privacy, security levels, interoperability and costs. Different requirements may be at odds with each other. For example, interoperability between systems and across borders may enable function creep and privacy risks; high levels of security and privacy typically require higher financial investments. The project results show that current policy discussions often lack a clear and explicit decision regarding these trade-offs.

Policy option 11: Ensure open and transparent evaluations of the trade-offs between privacy, security, usability, interoperability and costs of an eGovernment system

Insight into the different architectural and organisational designs of a particular system and into the consequences of those designs in terms of privacy, security, interoperability and costs can be provided to policy makers via independent feasibility studies. Such feasibility studies would be based on rough functionality and design outlines of a new eGovernment system. The studies should focus on the purpose and scope of the system and on its impact on security and privacy, interoperability and usability. The studies should include a cost–benefit analysis and an assessment of the extent to which the system can actually meet the challenge for which it is designed. Mandatory public feasibility studies ensure an open and transparent political evaluation and public scrutiny of an eGovernment system, particularly concerning the purpose of an eGovernment system and its trade-offs.

Case-specific policy options

The above-mentioned overarching policy options are a major outcome of the project. They apply to eGoverment in general as well as to the three case studies. Furthermore a number of case-specific recommendations have been developed. These recommendations can be found in Chapter 3 and are summarized as follows.

eProcurement recommendations:

- Address user reluctance: There is a reluctance to use eProcurement even by government procurement agencies, as a Commission survey has shown (European Commission 2010f). This issue should be explored in detail, with in-depth interviews and case studies, focusing on the reasons, such a national laws which need to be applied, perceived lack of financial efficiency, etc.
- Efficiency should be ascertained ahead of making a procedure mandatory (as currently planned according § 19 of the Draft Procurement Directive). The Parliament may wish to make mandatory use of technologies (also § 19) subject to parliamentary approval.
- Consider that bidders control decryption: Procurement systems are set up in a way that the buyer opens the tenders after the deadline. However, there is a certain risk that hackers or insiders could manage to read information in the bid at an earlier time. It could therefore be investigated if it were preferable that the bidder supplies the information which is necessary for decryption only after the deadline has passed.
- Enhance control of certification authorities, as the case of Diginotar showed (Prince 2011).

eHealth recommendations:

- There is need for agreement on a common baseline for security of eHealth data, a minimum set of requirements for eIdentification of professionals and a framework for the cross-national acceptance of a national ID for patients/citizens (as is the objective of STORK 2), a minimum set of standards for access control to Electronic Health Records (EHR) data and a set of common standards for 'secondary use' – i.e. de-identification standards allowing EHR data to be used for research. In light of the new privacy regulation, the standards for patient consent and a patient's right to his own data, among others, also need harmonization.
- Separate the decision on establishing a national identity system from the eHealth system. Ensure the general applicability of this eID system across domains and applications in order to ensure its popular acceptance.
- Any progress towards a standardized, controllable eHealth environment needs to be incremental and coordinated by key stakeholders who define the basic principles and basic standards.
- Ensure proportionality between the security level and the perceived threat and selection of principles for de-identification of patient records.
- Health records for individual patients should not be destructed, but migrated to follow-on systems in a secure way.
- Standards for a pan-European system should be clearly defined and documented.
- In the design phase it must be clear how a national control point could be established that would serve as a gateway to other EU countries and ensure compliance with accepted standards.
- In the operational phase of transnational eHealth projects a body should be established to ensure audit, oversight control and the resolution of differences between the participating nations.
- Decommissioning of transnational eHealth solutions needs to be planned and accepted by the participating countries.

ePassport recommendations:

- 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 improve the quality of the biometric images it must be established as a European standard that facial images are taken "live" at issuance.
- Improve the interoperability and security measures of the chip in the passport. This includes the Basic Access Control protecting identity information and facial image, which is deemed insufficient. It also involves the security of the fingerprints (currently the Extended Access Control), for which there must be a successful exchange mechanism in order for them to be used in all Member States and to add to border security in Europe.
- Improve procedures for redress with regard to errors and mistakes that may occur during the border control process. The ways in which citizens can correct errors need to be clearly addressed in legislation when using biometric systems for border control purposes. The legislative frameworks regarding privacy, data protection and civil rights in Europe vary. This adds to the difficulties citizens face when trying to attain justice, and they need to be harmonized.

1. Introduction

In April 2011 the project "Security of eGovernment 'systems' was initiated by the STOA Panel of the European Parliament.
The aim of the project was to analyse and discuss security of eGovernment systems and services with special attention to the possibilities of future EU eGovernment services by:

- Gathering typical examples of existing national and international eGovernment services in Europe
- Analysing the most relevant security issues and possible response/solutions to these issues
- Debating policy options for advancing of EU eGovernment services
- Assessing and delivering specific policy options

The project was carried out in four phases:

- **Phase 1: Pre-phase**
  Scoping the project in cooperation with a group of experts and identifying the key issues to be worked with in the project
- **Phase 2: Knowledge building**
  Building the knowledge base of security of eGovernment systems through three case studies of applications of eGovernment
- **Phase 3: Expert/stakeholder debate on the perspectives of EU eGovernment services**
  Debating the policy options for advancing EU eGovernment services at an open conference about security challenges for eGovernment systems and a small expert workshop on possible policy options
- **Phase 4: Policy options assessment**
  Assessing the future policy options for promoting EU eGovernment services

1.1 Background and motivation

The background and motivation for the project was the trend of digitalization in today's society, the changes in the way we communicate with the public sector and the way the public sector is governed and public services are delivered. The digitalization of the public sectors and services across Europe is increasing. This development is going to continue and is seen by many as part of the answer to the challenges of increasing demands for public service combined with an ageing society with a decreasing workforce. But to get the best out of the digitalization of public service there are a number of challenges to be met. Problems with user-friendliness, discrimination of people with poor IT-competences, transparency, efficiency and reliability are just some of the challenges.

A more specific set of challenges is found in the technical area. Especially the development and increased use of digital public services or eGovernment poses a number of major challenges. The security of eGovernment is a crucial issue, and a basic level of confidence and security must be established in order for people to be able to trust and use future digital public services.

Nevertheless internet-based communications and digital public services are moving further and faster and becoming increasingly crucial to the economies and to the fabric of our modern society. Therefore this STOA project was initiated to focus on the specific challenges connected to security of eGovernment systems.

1.2 Final report

This report is the final report of the "Security of eGovernment". In this report the results of the four phases of the project will be presented. First the results of the pre-phase (phase 1) followed by the results of the case studies as well as the more general conclusions and syntheses based on them (phase 2). Subsequently the results of the conference will be presented (phase 3) and finally we will focus on the policy option assessment and present a number of specific policy options (phase 4).

The purpose of this report is to give an overview of the project and specifically the most significant results of the project work.

It is our hope that the work of the project, this report and especially the policy options presented will support the Members of the European Parliament in general and the members of the STOA panel in particular in promoting future secure European eGovernment systems.

1.3 Thanks to

The consortium would like to thank a number of people who has provided significant contributions to the project.

In phase 2 the following people were essential to the results of the case studies: Christian Henrich und Maik Herfurth, Forschungszentrum Informatik, Karlsruhe, Germany (eProcurement), Soeren Duus Oestergaard and Kristian Duus Oestergaard, Duus Communication (eHealth), Max Snijder, European Biometrics Group (ePassport).

Furthermore the consortium would like to thank the members of the expert group for sharing their knowledge and insights and thereby improving the case studies, the conference and the policy option assessments. The expert group consists of: Juliet Lodge, Chris Dalton, Antonio Lioy, Barbara Ubaldi and Michael Waidner.

We would also like to thank the speakers of the conference for their insights and contributions. Some of them have already been mentioned above, but in addition Gernot Heiser, Peter Hustinx, Florent Kirchner, Antonio Lioy and David Wright gave presentations.

Linda Kool
Geert Munichs
Arnd Weber
Mikkel Lund Jensen
Anders Jacobi

June 2013

2. Scoping the project

Electronic Government or eGovernment is at the forefront of current public sector reform policies across Europe and the rest of the world, where the use of computer-based information and communication technologies (e.g. telecom networks, computers and mobile phones) to deliver public services in the public sector is seen as a major leverage of public sector innovation. eGovernment is usually presented as using Information and Communication Technologies (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) provide citizens with the opportunities to participate in different kinds of democratic processes (Silcock 2001, Bhatnager 2004, Lambrinoudakis et al. 2003, Layne and Lee 2001). However, eGovernment is also a powerful guiding vision for the transformation of public governance (Lenk and Traunmüller 2000). It is about enhancing democratic processes and using new ideas to make lives easier for citizens, enabling economic development and renewing the role of government in society. The implementation of eGovernment services involves a transformation in the way the government interacts with the governed but also the reinvention of its internal processes and organization (Meijer and Zouridis 2004). This transformational role of eGovernment is 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). In the EU, the current eGovernment Action Plan 2011-2015[1] 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 provision of eGovernment services and products across Member State borders serves as a key example of a transformational government ambition. In the 'Security of eGovernment' project the starting point is the development and roll-out of EU cross-border public services in the domains of procurement, border control and health. The intention to deliver public services across the 27 Member States is strongly emphasized in the eGovernment Action Plan 2011-2015 where the reinforcement of mobility in the single digital market supports Action 84 of the Digital Agenda 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. Thus, as governments across the globe strive toward providing ICT enabled public services to citizens and businesses, 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 Digital Agenda pillar three: Trust and Security.[2]

The project 'Security of eGovernment Systems' aims at assisting policymakers in discerning policy options for meeting future challenges in securing eGovernment systems. The project will focus on upcoming challenges of eGovernment security in delivering public services across borders. Through 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

[1]Communication from the Commission COM (2010) 743, December 2010, The European eGovernment Action Plan 2011-2015: Harnessing ICT to promote smart, sustainable & innovative Government.

[2] For an overview of EU policies on Network and Information Security, see http://ec.europa.eu/information_society/policy/nis/index_en.htm.

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 will provide an in-depth case study of three application areas of cross-border eGovernment: eProcurement, biometric passports and eHealth records and transactions. The aim of the case studies will be to analyse identified threats and challenges related to security of eGovernment. The project consortium will identify relevant security challenges and corresponding policy solutions for addressing these challenges (the work of phase 2).

2.1 Identifying key security challenges and selecting the cases

In order to identify the most pressing security challenges facing European governments and enterprises the project consortium consulted the latest eGovernment benchmarking reports including:

- the UN eGovernment Surveys (2012 forthcoming, 2010, 2008, 2005, 2004, 2003)[3]
- the coming EU 2011 – 2015 benchmarking framework[4] replacing the current i2010 benchmarking framework[5]
- and the latest EU eGovernment Benchmarking Report (2010)[6]

Based on the above mentioned desk research supplied with interviews and informal discussions with security experts, industry stakeholders and MEPs interested in the development of eGovernment systems the project consortium identified a set of interrelated security challenges facing the roll-out and operation of cross-border eGovernment systems. They included network security, interoperability, identification, usability, privacy, access control and function creep. These cross-cutting security challenges were examined in the context of our three case studies, each exemplifying different aspects of the security issue at hand. Selecting the cases we tried to strike a balance between similarity and diversity. If cases were performed on very similar eGovernment applications, it was easier to compare them, while a diversity of cases allowed us to draw more general conclusions on other eGovernment application. For the goal of this project, we opted therefore for case studies which resemble each other in complexity and scale of use, while they differ in terms of user groups, societal sectors and technologies used. All case studies should dealed with eGovernment systems which are applied throughout the majority of EU Member States. This allowed us to compare different member states and / or variations between national and European legislations. Also, the cases 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 concern a Business to Government (B2G) relation, a second involves a Government to Citizen (G2C) relation and a third involve governments, citizens and businesses. Also, a measure of diversity in technologies in use was needed: 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: identification, payment, personal data storage, etc. Taking these factors into account, we opted for the following three case studies: eProcurement, biometric passport and eHealth records and transactions.

[3]For full details, see http://www.unpan.org/egovkb/global_reports/08report.htm and for the UN interactive e-Government Development Database (UNeGovDD), see http://www2.unpan.org/egovkb/

[4]Http://ec.europa.eu/information_society/eeurope/i2010/docs/benchmarking/benchmarking_digital_europe_2011-2015.pdf

[5] For full details, consult http://ec.europa.eu/information_society/eeurope/i2010/benchmarking/index_en.htm

[6] Digitizing Public Services in Europe: Putting ambition into action - 9th Benchmark Measurement - December 2010. Full information at http://ec.europa.eu/information_society/newsroom/cf/item-detail-dae.cfm?item_id=6537

Table 1: Case study selection criteria

	Criteria	1. eProcurement	2.Biometric passport	3. eHealth records
Similarity	Use	EU + Member States	EU + Member States	EU + Member States
	Scale	Many companies and most governments	All EU citizens and governments	Some governments and some citizens
	Complexity of security issues	Many incompatible systems	Differences between EU Directive and national implementations. Risk of function creep	Many incompatible systems with a strong incentive for harmonization. Many privacy issues.
Diversity	Relation provider-user	G2B	G2C and G2G	G2B, G2G, G2C
	Technologies used	eSignatures, databases	RFID, biometrics, facial recognition, databases	Tokens, smart cards, eCards, ID numbers, databases

2.2 Setting the EU eGovernment policy context

Following the implementation of the first European eGovernment Action Plan 2006[7] large-scale pilot projects are developing solutions for rolling out cross-border eGovernment services. Building on the experiences of the first action plan, the second eGovernment Action Plan 2011-2015 aims to realize the ambitions of the Malmö Declaration[8] made at the 5th Ministerial eGovernment Conference in 2009. The Action Plan supports and complements the Digital Agenda for Europe[9]- as one of seven flagship initiatives under the Europe 2020 Strategy[10]. One of the key challenges facing eGovernment systems is aligning national and EU legal frameworks. As cross-border eGovernment initiatives operate between national and EU laws and regulation, the roll-out of cross-border services may potentially conflict with national legal frameworks. In eHealth, for instance, policies on health, employment, social affairs, regional development, research, innovation, industry and internal market intersect. Securing cross-

[7] Http://ec.europa.eu/information_society/activities/egovernment/docs/action_plan/comm_pdf_com_2006_0173_f_en_acte.pdf

[8] This conference was preceeded by bi-annual Ministerial meeetings of Brussels in 2001, Como in 2003, Manchester in 2005 and Lisbon in 2007. For full information, see http://ec.europa.eu/information_society/activities/egovernment/library/index_en.htm.

[9] See http://ec.europa.eu/information_society/digital-agenda/index_en.htm for full background

[10] See http://ec.europa.eu/eu2020/pdf/COMPLET%20EN%20BARROSO%20%20%20007%20-%20Europe%202020%20-%20EN%20version.pdf.

border eGovernment services may additionally challenge existing regulations at national and EU level. The project has put a specific emphasis on discussing lines of intersection and conflict where the imperative to secure ICT systems impedes legal protection of civil rights, privacy etc. In order to expose the intricacies of existing and upcoming EU and national regulation, the project consortium included legal experts in our scheduled interviews. In the presentation of the project's case studies we addressed the regulative framework in closer detail.

2.3 Key security challenges

In the following, the key security challenges facing operation of cross-border eGovernment systems are described.

2.3.1 Network security

With eGovernment the need for security in communication networks is increasing and resilience against network attacks (access, modification, denial of service) is of pivotal importance. Threats to network security (cyber terrorism, cyber espionage, Advanced Persistent Threats, blended threats etc.) are continually changing as vulnerabilities in both established and newly introduced systems are discovered, and solutions to counter those threats are needed. Measures to ensure network security comprise firewalls and proxy to keep unwanted people out, antivirus software and Internet Security Software suites, anti-malware, encryption, security fencing, as well as improved computer architectures etc. (Grawrock 2006, Heiser 2010).

2.3.2 Interoperability

Effective communication between and among consumers and providers, whether governments, citizens or businesses, requires that the products they use are able to share and exchange data. Thus, interoperability – the ability of products, systems, or business processes to work together to accomplish a common task - has remained a longstanding EU goal. The European Interoperability Framework (EIF) - a priority component of pan-European eGovernment strategy - identifies three distinct elements of interoperability: (1) "technical" interoperability, involving the linking up of computer systems via agreed standards for the exchange of data; (2) "semantic" interoperability, focused on ensuring that exchanged data shares the same meaning between linked systems as well as analyzing different European national digital XML-standards; and (3) "organisational" interoperability, involving the organisation of business processes and infrastructures to enhance data exchange (i.e. the cross-border process itself)[11]. The provision of seamless cross-border and cross sectorial public services – for which interoperability is a prerequisite – is considered to have a potential high impact on businesses and citizens. Just as it is essential, interoperability in the eGovernment context is also complex. An eGovernment system must address communication needs at many levels, including government's ability to communicate with citizens (individuals), with the private sector, and within the public sector itself. There are a range of diverse software and hardware systems and various types of data implicated in these transactions as well as different users (citizens and businesses); portals (Government, local authorities, the private sector); infrastructure, multiple access channels and competing government systems.

2.3.3 Identification

The issue of identification raises several important questions related to our cases. In eProcurement the issue of verifying the identity of a business is important, not only for making sure that the business is who the business purports to be when making a deal, but also in the long-term. Will businesses be able

[11] Http://ec.europa.eu/isa/strategy/index_en.htm.

to be held liable in the future by the digital signatures they've used when closing deals? Is there a risk that this ID-information might be lost, stolen, deleted, or become insecure, and does this also entail a risk that agreements will not be upheld because there might be doubts about the correctness of the identification of the business? With regard to biometric passports doubts have been aired as to if biometric data will be reliable and if it will be protected against criminals who would want to forge the data and biometric passports. As such the efficacy of biometric data will be a matter that will be addressed. In eHealth the problem of how patients, doctors and other health professionals will identify themselves is an issue. Will a pin code be used? Or a smart card? Which means of identification is needed to create patients' data, modify them and get access to them and who is responsible for the correctness of a record?

2.3.4 Usability

Usability focuses on making applications and services easy for people to use. The issue of usability is linked to security concerns since attempts to increase data security may decrease their usability. In terms of this project, usability also addresses how data is going to be used and who is using the data. As such usability entails a strong focus on issues of trust in eGovernment invoked by the interaction among actors that control, deliver, or benefit from the service. In eProcurement, usability problems emerge from national requirements demanding company dossiers, or from eSignature schemes. In eHealth different health systems have different record holding systems, and even within these systems there might also be different record holding systems. Even more there is the problem of making the record holding systems fully digital and making sure that staff and patients know how to use a digital system.

2.3.5 Privacy

With privacy we refer to the relationship between collection, minimisation, dissemination and protection of personal data through the use of technology. Privacy in eGovernment refers to the credible government protection of the personal information of citizens. We believe that concern among citizens about how their personal data will be stored, processed and transmitted in an eGovernment context will be among the top eGovernment barriers in the future. Citizens and businesses must be assured that they interact with public administrations in an environment of trust and in full compliance with the relevant regulations, e.g. on privacy and data protection. This means that public administrations must guarantee that the privacy of citizens and the confidentiality of information provided by businesses are respected. Within the necessary security constrains, citizens and businesses should have the right to verify the information which administrations have collected about them and to decide whether this information may be used for purposes other than those for which it was originally supplied. In all case studies, the information to be handled is often of highly sensitive nature. Gathered data may include information about income, tax, bank accounts, but also very personal information about previous diseases or medical treatments etc. Security breaches and privacy issues might therefore turn out to affect a citizen more than in usual information systems usage - even more so, taking into consideration that many eGovernment solutions intend to store data centralised. As eGovernment systems are established it thus becomes necessary to address the fact that this exposes the privacy of citizens and organisations to new threats. The more data on citizens is available in databases, the more risk for this to be exposed by third parties, or for the government to use this data in doubtful ways. For organisations it also entails the threat of having its data more easily exposed.

2.3.6 Access control

All electronic systems that contain sensitive information will be of interest to people who might want to use this information for nefarious purposes. As a result access control to these systems is needed in order to prevent unwanted use of the information stored. Access control in general has a very wide definition, since it can be anything from your car lock to the pin code to your credit card. But the basic function is to deny unwanted access. In the area of eGovernment these means of access control will mainly be electronic or physical (walls, cards, tamper resistant devices), and the systems can be anything from databases of citizen information, health records, bank accounts and contracts to control of infrastructure such as electricity, roads and airports etc. Access controls can be compromised. This means that there is a risk of fraud or of someone hacking an entire country by getting access to a government database with information on citizens. Likewise, even data that requires biometric information to be accessed can be forged. For businesses using eProcurement this could have the implication that their ID is forged and used for fraud, and for citizens using eID the risk of someone "hacking a country" or forging biometric data is a very real concern. Subsequently the digitalisation of health systems and utilization of eHealth and ePrescription are vulnerable to the same threats to access control; IDs might be used for fraud, passwords stolen and smart cards lost. As such, all electronic systems risk being compromised and having data stolen. And while very safe and elaborate systems of access control can be constructed, the more elaborate the access control system is, the more you might compromise the usability of the system or service. For example, from the viewpoint of usability a single sign-on system may be preferred, allowing users to remember just one access code for multiple data files. From a security point of view, multiple accounts might be preferred, preventing too much data loss in case of ID theft.

2.3.7 Function creep

Function creep is what occurs when an object or a procedure designed for one purpose ends up serving another purpose for which it was not originally intended. This can happen if the area of the function has not been sufficiently defined or delineated. For example a law can be put into effect which gives the police certain powers, and if these powers have not been defined well enough, the police might use them for other purposes than what the law was originally intended for. In relation to eGovernment this is a very important issue since large amounts of highly sensitive data on citizens will be broadly available to government agencies, and perhaps even private organisations. Therefore it needs to be considered thoroughly which implications the storage of citizen data might have, how one intends for it to be used and which legal and political initiatives need to be taken to protect citizen and company data. Still, once the biometrics of all citizens is gathered and stored in a searchable way, it can also be used for other purposes such as identification in criminal investigation. Also, an eHealth system could face the risk of health information of citizens being used by insurance companies unless clear limitations for the use of this information are put into place. A different type of function creep might occur if one type of eSignature is made mandatory in one field of applications and is subsequently made mandatory in another area. In the first field, a cheaper type might be enough, while in the second a more secure one could be appropriate, while in reality regulations might impose something different.

In order to illustrate the intersection of security challenges and case studies we have devised a security matrix model (table 2). Each security theme entails specific actions and policy options that the project will address in phases 2, 3 and 4.

Table 2: Security matrix model

	1. eProcurement	2. Biometric Passport	3. eHealth Records
Network Security	Lack of availability of Internet, denial of service attacks, malware	Centralised or decentralised storage, attacks from the network	Centralised, decentralised or host-based systems, attacks from the network, gaps between e.g. closed loop medication systems and web based data bases
Interoperability	Systems may not be interoperable	Different phases of implementations	Semantics regarding 20 languages and three alphabets in pan-European situations, different systems of classification of diseases and drugs
Identification	Parties may not be identified properly	Fault margins on biometrics	Unique identification of citizens/patients, healthcare professionals, pharmacies, locations and devices/hardware
Usability	Systems may be complex	Skills level of civil servants	Skill levels of citizens/patients, informal carers and health care professionals
Privacy	Confidentiality of information	Storage of all citizens biometrics	Patient consent, confidentiality
Access control	Access of outsiders	Security of the chip and databases	Opt-in/opt-out modalities in databases, re-use of individual patient health data
Function creep	Use of signatures	Biometrics for police investigation	Misuse of information by insurance companies

The seven security challenges we defined here are related. For example, weak access control or elaborate function creep may lead to privacy issues. Or, identification is one of the techniques for access control, etc. In Deliverable 2, we will elaborate on the interrelation among the seven challenges.

Taking the strategic objectives of this project into consideration, the project consortium decided to employ a multiple case study approach (Yin 2002). The case study approach consists of gathering enough information about a particular object of inquiry – in our case security challenges in the adoption/implementation of specific eGovernment systems – to permit the researcher to understand the system, processes and context involved and the dynamics present (Benbasat 1987, Eisenhardt 1989). A case study approach is also appropriate because of its ability to encompass multiple research methods. The project will draw on the following combination of case-focused methods:

- Semi-structured interviews with key case study stakeholders and technical experts relying on open questions guided by an emergent conceptual map of the research domain.
- Document analysis of policy documents, consultancy reports, reports from international bodies etc.

This was the starting point of carrying out the three case studies in phase 2 of the project. The three application areas to be studied were eProcurement, eHealth and ePassport.

3. Case studies of eGovernment applications

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 where the reinforcement of mobility in the single digital market supports Action 84 of the Digital Agenda 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.

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.

The second deliverable of the project 'Security of eGovernment Systems' is a report that 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 previous chapter 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.

3.1 Case study 1: eProcurement

3.1.1 Overview

In this section the most important issues and conclusions regarding eProcurement are presented. The rating of importance is based on how issues were discussed at the project conference and with the invited experts, as well as on own judgment based on the evidence obtained. Furthermore, the importance is based on whether an issue is of over-arching relevance for eGovernment in general. For a full overview of issues in public eProcurement see "Intermediate Report 2: Case Study Report".

The value of all public procurement spending in the EU amounts to around 19% of the GDP (European Commission 2011g). Procurement is an area prone to bid rigging and corruption (Thai 2009, OECD

2007). Attacks on the systems of buyers or bidders must be anticipated to take place in order to figure out details of offers such as prices.

With some exceptions, public eProcurement in Europe is conducted rarely. In some countries, such as Portugal, electronic procurement is mandatory. The Commission estimates that in the EU as a whole only about 5% of all public procurements above thresholds are done electronically. Trans-border 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 high-value transaction per year. However, already more than 300 procurement platforms have been set-up (Ampe 2012).

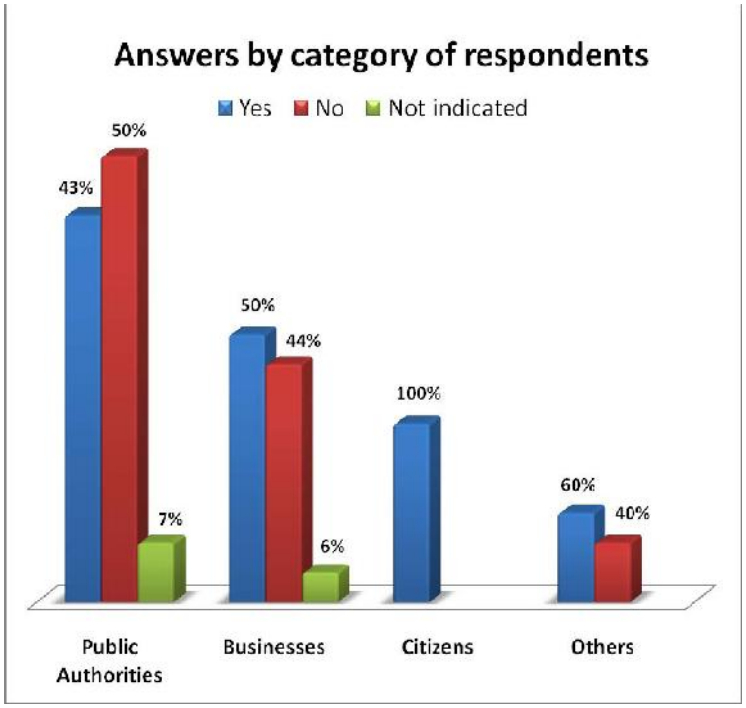


Figure 1: Answers to the question "Should EU law impose eProcurement?" (from: Summary of responses to the Green Paper on expanding the use of eProcurement in the EU, European Commission, 2010f).

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.

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. 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), cf. Figure 1. The reasons for this resistance are not clear. Anecdotal evidence suggests that among the reasons are the need to comply with foreign legislation, the costs of setting up software for various bidding platforms and the ease of using paper documents. Furthermore, there are issues such as the lack of interoperability that might arise if any special security tools are used, such as specific types of encryption, PKI-based authentication or digital signatures. However, the reasons for the resistance are not clear and should be explored in in-depth analysis ahead of making any new legislation.

3.1.2 Three country studies

The small case-studies below are supposed to shed some light on how eProcurement progresses, depending on the national setup. 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.
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. Still, large discrepancies are visible.

Table 3: 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)

Advanced signatures: Signing keys can be stored on any media (in an encrypted form) and are processed as normal.
Qualified signatures: Use a tamper-resistance module for storage and processing.

[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 table.
[xx] Even below EU thresholds.

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 Certification Authorities in 2001. For banking and stock trading, the use of certificates has been mandatory since 2005. Users have been provided a secure environment (Hardware Security Module - 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 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 certification authorities. The Korean Information Security Agency represents the electronic signature authentication management centre and issues certificates for accredited certification authorities (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).

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 issued smart cards. The former, called the Citizen's Card (Cartão de Cidadão), offers eSignatures. The Portuguese e-Procurement Program (PNCE) is built around components such as a portal (was www.Compras.gov.pt, now Vortal https://www.vortal.biz/), a registry of suppliers, eAuction platforms and a central Catalogue Management Tool (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 noted: "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).

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 3.

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 certification services (T7 & TeleTrust 2009).
The new eProcurement website (http://www.xvergabe.org) claims that the current eProcurement situation is problematic, as there are "many solution providers, different technologies, incompatible bid-clients (browser- or software based), 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-repudiation 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.

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 could be used. It would mean that any services such as registration or PKI services, should be available for any bidder or contracting authority, e.g. with a user interface in the national languages and in English.

3.1.3 Security and efficiency

Confidentiality
The confidentiality of bidding prices as well as of the content of bids is a particularly sensitive field of eProcurement. If the contracting authority has the capability of decrypting bids using means under their control, criminal insiders could possibly learn prices ahead of the tender deadline. This could take place if bidders use encryption keys provided by the contracting authority. No matter how securely the contracting authority may store the keys, e.g. in a so-called electronic tender box, they are accessible by their employees. Bidders would have to trust that insiders won't collude for accessing keys (manipulating logs, etc.). Bidders might claim that a procedure used by the contracting authority was not secure. In order to avoid any such risks, the bidders could encrypt their bids using keys generated by themselves.

One way to handle this would be to use a cryptographic commitment service. 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.

When deploying cross-border bid encryption, the risks of the parties should be taken into account when deciding on the selection of a procedure. Keys generated by the bidders would have some costs, but also benefits. Such procedures would make it useless for competitors to bribe insiders with the contracting authority, or to start an attack on the central system.

Non-repudiation
In eProcurement, some degree of non-repudiation is needed for achieving legal certainty in any later disputes. A large variety of approaches can be seen. The most noteworthy are:

1. Use digital signatures. There are different varieties of digital signatures, some using tamper resistant modules for storage ("qualified"), others not. For trans-border commerce this requires well working standards.
2. Use files which are digitally signed in combination with a paper contract. This requires trans-border interoperability, but reduces any issues with the verification of digital signatures in the long run (validation, time-stamping, re-signing).

3. Use files which are not digitally signed in combination with a paper document. This does not pose interoperability problems.
4. Use simple procedures, such as log-in via passwords (shared secrets), encrypted with SSL.

Regarding option 1, 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, such as the PEPPOL project. Furthermore, standardisation activities are supported, in particular a CEN-workshop, also aiming at compatibility with UN/CEFACT. At a Commission event, Rannenberg reminded the audience of the issue of missing secure signing environments (Rannenberg 2011). It was not possible to clarify, during the course of the project, whether the benefits of digital signatures would justify their costs, as there is a lack of related studies.

Regarding option 2, this option has been observed in Portugal.

Regarding option 3, handling can be made easier by signing only a coversheet, on paper. This procedure is used in Germany and called a Mantelbogen. 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). Also the PWC's Golden Book explicitly mentions the option of a manual signature (2011).
Regarding option 4, according to Siemens-time.lex, "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) So this is another valid option.

The various approaches obviously come with different costs and benefits. Given the estimate of costs of a paper document of about €15 (Posch 2011, referring to British estimates), using paper 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. It has not been possible to identify any studies providing estimates of the costs and risks. Such studies would need to be undertaken. Alternatively, the choice could be left to the market players. 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 handwritten signatures should not be ruled out. Also the use of certain tools for European eProcurement only, such as a Procurement Card, might be given consideration in order to achieve rapid progress.

Secure environment
For keeping the content of bids confidential, as well as for keeping keys and passwords confidential, computers would be needed which cannot be hacked.

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 an 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).

One must also expect that hidden functionality be put into hardware. This has been discussed at the project's conference and was also mentioned in a report by Reuters on spyware in Chinese hardware (Bilby 2012). Basing hardware on European designs such as ARM processors are an important option.

For existing systems, in the short run, professional management can help against attacks, e.g. based on following the advice in the SANS list of 20 measures (SANS 2012). Following such advice can be made mandatory. In the medium run, well-tested systems, certified ones or proven ones could be used. The European Union could support the development of proven operating systems kernels and ultimately computers much like US DARPA does (see DARPA 2012 and Heiser 2013). A proven kernel would be able to separate secure, isolated applications from others, such as untrusted email-attachments or websites, as Heiser presented at the project conference.

Efficiency
As indicated, it has not been possible to identify studies on the costs of using the various security instruments in procurement. Also other researchers have found it difficult to identify changes in process costs (Croom, Brandon-Jones 2009, p. 456). Misuraca et al. (2012) pointed out that it is important to involve stakeholders and beneficiaries very early in the design of eGovernment systems, and to evaluate each step regarding economic benefit. As an example, it would need to be evaluated what, e.g. the transactions costs of using the PEPPOL Validation Service Architecture are. No estimate for this can be made, as no transactions have been made during the empirical phase of this STOA-project. An alternative might be to use a single technology system with, e.g. a European Procurement Card or with shared secrets (password) in combination with handwritten signatures on contracts.

In other words, trans-border processes need to be implemented, tested, their cost-efficiency be estimated, then rolled-out, and evaluated again.

3.1.4 Pending legislation

Several legislative acts have been pending during the course of the project. Most important is the 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". As it has the potential to make the use of digital signatures mandatory, we first review some clauses of the pending eSignature regulation "on electronic identification and trusted services for electronic transactions in the internal market" (European Commission 2012f).

Signature regulation
The European Commission has published a proposal for an eSignature regulation. It is meant to replace the signature directive (1999/93/EC). Some clauses are of particular relevance for e-Procurement:

- 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 ("qualified signature", cf. Annex II).

- 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 1999 directive.

The variety of means implies various ways 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. It does not appear to be clear whether an upgrade path for digital signature environments would be hindered by § 20.

Another issue is the surveillance of certification authorities certifying the applicability of cryptographic keys to identify an entity, e.g. for encrypting a message to it. It appears that Diginotar, a CA used by the Dutch government, was hacked in 2011 and did not take immediate action, nor publish the attacks in time (Prince 2011). Similarly, there have been reports about a hack into the Verisign systems (Reuters 2012). It might be necessary to control such certification authorities more intensively. 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.

Procurement directive
Several legislative acts have been pending:

- As mentioned, the Proposal for a Directive on public procurement, replacing Directive 2004/18. Brussels, 20.12.2011, COM(2011) 896 final.
- 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

The Draft Directive COM(2011)896 addresses classical public procurement and will be regarded below. Not taken into account here are COM(2011)895 and COM(2011)897, which address the utilities sector and concessions, are these are substantially similar, according to the European Commission (2012d). Details of Draft Directive 896 have been discussed in Intermediate Report 2; key issues concern the following.

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..."

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

That means that eSubmission above thresholds would become mandatory and that central purchasing bodies would have to use electronic means. Authorities would no longer be allowed to request bids using paper. As there currently are not enough trans-border interoperable solutions for achieving non-repudiation and confidentiality, it has been suggested that first such solutions should be developed and tested, before eProcurement can be made mandatory (BDI 2012).

Article 19(3) says: "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."

The Commission would then be able to impose standards for formats and authentication of submissions. Contracting authorities would 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 can 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 shared secrets or PDFs sufficient. According to a 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 transaction costs in Portugal or 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 technologies subject to parliament approval.

3.1.5 Main conclusions specific to procurement

The remainder of this section on eProcurement provides a summary of the conclusions. First, the conclusions are presented which are somewhat specific to eProcurement. Later, those are presented which apply to any type of eGovernment.

User reluctance
There is reluctance to use eProcurement even by government procurement agencies. This should be explored in detail, with in-depth interviews and case studies, focusing on the reasons, such a national laws which need to be applied, perceived lack of economic efficiency, etc.

Cross-border solutions should be cost-effective
Cross-border eProcurement solutions should be implemented and tested, as well as checked for efficiency. This includes the issue of how bidders can submit bids to contracting agencies in different countries. Efficiency should be ascertained ahead of making a procedure mandatory (as currently planned according § 19 of Draft Directive 896). Parliament may wish is to make mandatory use of technologies (also § 19) subject to parliamentary approval.

Consider that bidders control decryption
Procurement systems are set up in a way that the buyer opens the tenders after the deadline. However, there is a certain risk that hackers or insiders could manage to read information in the bid earlier (e.g. the price). It could therefore be investigated if it were preferable that the bidder supplies the information which is necessary for decryption only after the deadline has passed. This places some additional costs on the bidder, but would have the advantage that no bidder can claim that competitors knew prices beforehand. This is an issue to be addressed in further research. A proposal for a commitment service has been presented above.

3.1.6 Main overarching conclusions

Address business case for security instruments
Ahead of making any security tool mandatory, it should be addressed whether there is a business case for specific instruments. We are not saying that eProcurement is not efficient. We are also not saying that transborder procurement would not be efficient. We are stating, however, that it should be verified whether a certain transborder eProcurement procedure is the most efficient one. This implies that it should be studied whether a Peppol-like infrastructure with validation servers in various countries is the most efficient. At the other extreme, a single solution such as with a European procurement approach, possibly including a single card, might be more efficient. On the other hand, authentication based on shared secrets or even handwritten signatures might be efficient.

Explore steps towards a secure computer
In eProcurement there are various secrets, such as prices or passwords. On an open network such as the Internet, there might always be attacks. One way to keep confidential information away from eavesdroppers is to isolate it. There are various ways to isolate data. The most promising method would be to have a "container" in a provably secure computer. Isolated containers could then communicate with other isolated containers using a usual secure channel. A key component would therefore be a proven security kernel (Heiser 2013). The US DARPA is going in a similar direction (2012). Hardware free of Trojan horse functionality would be another requirement, with production in Asia being a problem, while ARM processor concepts are an important option. The European Union could push for such solutions, e.g. by supporting their production, by requiring the use of proven isolation, by investigating liabilities for producers of faulty systems, and even by leading a related discussion.

More secure environments would also be beneficial if digital signature solutions were attacked. A system with secure user input and output would be an upgrade of a "qualified signature" card being used in an off-the-shelf computer.

Use security engineering and comprehensive procedures for controlling systems
As long as no provably secure systems exist, comprehensive professional management of IT systems is needed, as specified for example in SANS (2013), possibly amended with penetration testing. Such management could be made mandatory, but does not completely protect against crafted attacks. Also, governments could make the use of best-practice security engineering mandatory.

Enhance control of certification authorities
Certification authorities may need to be controlled more tightly, if not even run by the government.

3.2 Case study 2: eHealth

3.2.1 Overview

Two national EHR projects and two International projects were studied in order to extract lessons learned and form a set of recommendations for policy enhancements and guidelines for future development. The UK National Programme for IT (NPfIT) from 2002 aimed at establishing a National Health system based on a single, centrally mandated electronic health care record ran into a number of challenges and parts of the project were cancelled in 2011 after massive critics, while the Estonian project from 2008 succeeded in implementing a nationwide, generally accepted eHealth solution.

The two international projects have different scopes, yet focused on some of the very central issues in establishing and operating cross-border eHealth services: The older project, the Baltic eHealth project (from 2005-2007) that aimed at improving access to eHealth professionals, particularly benefitting

patients in rural areas, and concentrated on exchange of radiology and ultrasound images to be analysed by specialists in other countries. The larger project, the epSOS project (Smart Open Services for European Patients) runs from 2008 until YE 2013. The aim of this project is to enable patients to receive medications using ePrescriptions while abroad and to permit health professionals to receive summary patient records stored in patients' home countries. Both international projects seem to have achieved their goals, but the epSOS pilot phase is still ongoing and more lessons and recommendations are expected.

3.2.2 Background

This study 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".[12]

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. Other dangers include financial risks (unmet expectations of cost

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

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.

3.2.3 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.

3.2.4 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 e-Health 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 e-Health Action plan for 2012-2020 (envisioned for release in 2012). In the public consultation on the second e-Health 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.[13]

It should be noted that eHealth as described above is more than Electronic Health Records and 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.

3.2.5 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.

[13] 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.

3.2.6 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.[14] 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[15] 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.[16]

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.

[14] See http://csrc.nist.gov/groups/SMA/fisma/index.html.
[15] Http://www.eurosfaire.prd.fr/7pc/bibliotheque/consulter.php?id=1507.
[16] 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 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.[17]

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

[17] 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[18], 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[19], and in particular the follow-up project ABC4Trust[20] (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[21]). One example of other types of privacy-enhancing technologies could be the so-called Hippocratic Database project[22] 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.

3.2.7 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 (eHealth 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 e-Health Action Plan (European Commission 2004) and the one forthcoming in 2012, Member States are committed to develop and issue national e-Health strategies and implementation roadmaps and plans for the deployment of e-Health 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

[18] Http://www.spiegel.de/wirtschaft/soziales/elektronische-gesundheitskarte-mega-flop-im-massentest-a-755464.html
[19] Http://primelife.ercim.eu/
[20] https://abc4trust.eu/
[21] Http://ojs.ubvu.vu.nl/alf/article/view/93/167
[22] 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 e-Health 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.

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.

3.2.8 Key findings - National EHR Projects

The UK NPfIT project launched by the National Health Service was at its launch the largest civil ICT project in UK so far - covering more than 30 hospitals, 30.000 professionals with a budget of > 15 Bn €. The purpose was to ensure use of standardised solutions across private and public actors, regions and local, existing solutions. The objective was to develop several sub-systems, among them the summary care record - SCR - and the detailed care record in accordance with NPfIT standards. The project ran into a number of delays and shortfalls, critics against lack of usability, lack of patient confidentiality and overall reliability. In 2010 an opt-out option was establishing for patients, and in 2011 the centralised approach had to be abandoned based on a critical audit. Some of the key reasons for the limited success were 1) the lack of an overall IT architecture, 2) the lack of buy-in by professional that had to abandon existing solutions, 3) the lack of trust in the centralised approach by the general population and 4) the lack of basic IT principles for security, trust and privacy from the outset. Further, a number of potential security breaches were identified, such as an old, perimeter defence approach to avoid intruders, a lack

of encryption and – compared to Estonia - a lack of an accepted national strategy for citizen identification.

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.
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.

3.2.9 Key Findings - International Projects

The Baltic eHealth project was faced with the problem of connecting the national or regional networks across the participating countries. To do this, an agreement system was created, ensuring the owner of each local eHealth IT system the possibility to control who should have access to his system and under which conditions. This agreement system supplemented the first level security consisting of secure VPN-tunnels between participants. The agreement system ensured that the connection could be established via a central hub. The 3rd level of security consisted of end user identification and password. As the participating end users are all health professionals, and as the data exchanged between countries are well-defined, the project demonstrated that cross border exchange of data was possible using the internet platform. The existence of well-defined standards from the Danish MEDCOM organisation was a prerequisite for the success. The project was continued as the R-Bay project running from 2007 through 2009 under eTen.
The epSOS project had a wider application focus and started by defining a Common Framework Agreement to establish a trusted domain between the National Contact Points. The agreement defined the baseline for security following the ISO 27002 standard. This includes rules for audit in each country. epSOS allows sending of patient summary records across borders, so that the healthcare professional in the requesting country will get a read-only access to the summary record in the patients home country as part of the patient treatment, and only via patient consent will the record in his home country be updated. Similar for ePrescriptions. So as the epSOS system does not allow local storing of data, the risk of data theft is minimised. Again, the participants in the project are health care professionals. One of the major barriers for this project was the lack of semantic interoperability from the outset, including different classification systems in each country. This led to the creation of Clinical Document Architectures - A Master Value Set Catalogue and a Master Translation/Transcoding Catalogue, using a specially developed epSOS ontology, a linguistic reference of terms used in the project to assist new participants to fill out their respective copies of the Master Value Set Catalogue.

Overall 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

3.2.10 General conclusions

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 the 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 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, the necessity of which is a consequence of greater mobility of both citizens and professionals and the emerging use of doctors and specialists operating from other countries. This requires at least that European countries adopt an acceptable and commonly agreed security baseline and that it becomes a common policy issue.

From a security perspective, the main differences between the European cases are found in the methods for establishing 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 a 'baseline' - not only for the aspects of practical interoperability 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 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 for developing a central security policy baseline, how to stimulate the implementation of this and the means necessary to support such endeavours, for instance by inspection, certification or some other means. A related observation is the necessity of embedding privacy and security concerns in the early design phase of any EHR system, which, as seen in the Estonian example, is 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 the different degrees of compliance with EU policy recommendations - both in regard to interoperability and to data protection - represent major barriers to the deployment of cross-border health services and the exchange of EHR. Although there is a commonly accepted belief in the benefits of an easy exchange of health data, the privacy and security risks must be addressed properly to ensure the trust of citizens and hence their 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 ensuring that all aspects of the proposed system are taken into account, from the overall architectural design and alignment with well-defined objectives and purposes to the design of applications and user interfaces to the design of the 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 - and from Australia, where a new national health reform was launched recently. In the Australian case, for instance, the privacy impact assessment took place before the system was opened, 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 the EU level. As noted by the recently released eHealth Task Force report, market fragmentation in eHealth is aggravated by the lack of common approaches (eHealth Task Force Report 2012). It may be comforting to observe that almost all countries now have based their EHR on standard HL7, but a lot of translation work still needs to be done, and the epSOS efforts, however 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 adopting 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.

Also of relevance for policy development is the need to address policies and procedures for harnessing the multiple functionalities of EHRs such as the 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 the pharmaceutical 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 the anonymization of such usage should be implemented as part of 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 being discussed by almost every data protection agency in Europe, minimum guidelines for the use of cloud computing in the health care environment should be developed. Seen from a technical point of view, this area is hardly mature but, as mentioned, some basic rules could be defined, such as use of private clouds or the possible use of hybrid clouds as a step forward.

Thus, the eHealth cases clearly demonstrate the need for us to address security and privacy during all phases of the life cycle of any eHealth system:

From the formulation of need and purpose (describing outcome and risks) across the political/administrative decision-making 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 the data generated.

3.2.11 Overall Conclusions and Recommendations: Way ahead for eHealth in Europe

In accordance with the life cycle approach as described in the ETAG report, the following recommendations should be made for the future development of eHealth systems in Europe.

3.2.11.1 General principles for eHealth systems

The differences between nations in their implementation of security suggest the need for an agreement on a common baseline for the security of eHealth data; a minimum set of requirements for the eIdentification of professionals and a framework for cross-national acceptance of national IDs for patients/citizens (as is the objective of STORK 2), a minimum set of standards for controlling access to EHR data and a set of common standards for 'secondary use', that is, de-identification standards allowing EHR data to be used for research. In light of the new privacy regulations, the standards for patient consent, right to own data etc. also need harmonisation.

3.2.11.2 National eHealth Systems

During the decision phase for new national eHealth systems two lessons seem to be of particular importance. The first is that it seems to be vital to separate decisions establishing a national identity system from the eHealth system and to ensure the general applicability of this eID system across domains and applications in order to gain popular acceptance. The second lesson is that most countries already have a number of eHealth applications installed with numerous historical data and with wide variations in quality, access control systems. Consequently, any progress towards a standardised, controllable eHealth environment needs to be incremental and coordinated by the key stakeholders, who from the outset must define their basic principles and basic standards. One of the key principles should be the observance of key international standards like HL7, which will also ensure there are future possibilities for international cooperation.

PBD - Privacy by Design - should be observed in particular during the design phase, ensuring proportionality between the security level, the perceived threat and the selection of principles for the de-identification of patient records. The principles for role-based access control are likewise important for the design of network security, in particular design of a doable, practical single sign-on system at the hospital or GP level preventing the unintended sharing of access by several professionals as is unfortunately a common practice.

During the operational phase in the life cycle, the constant trimming of the security level in accordance with new technology (use of mobile, cloud computing and telemedicine etc.) should be observed and documented. The need to update skills among staff - both IT and clinical - is important and should be audited along with an audit of compliance with accepted national (and international) security standards.

For the decommissioning of eHealth systems, in particular the migration of data is a key point of concern: health records for individual patients should not be destructed, but migrated to follow-on systems in a secure way.

3.2.11.3 International, cross-border eHealth Systems

As international studies have clearly shown, the major challenges are the different security levels in the different countries, a difference which hopefully can be reduced by agreement on a common minimum baseline and by the acceptance of the new regulation on privacy. But more challenges should be addressed during the development of a gradually more and more integrated network of eHealth services, which would benefit not only the citizens residing in or travelling to other countries, but likewise increase the general level of professionalism in the health sector and potentially also increase the quality of research for companies and universities working in the health sector.

During the decision-making phase, the baseline for the standards should be clearly defined and documented for the medical field for which the pan-European system in question will be decided. Most importantly, it is mandatory to define how these standards will be maintained and documented as the viability of an ill-defined system will be extremely short.

The design phase of new, pan-European services must address three vital questions. First, how could a national control point be established that acts as a gateway to other EU countries and ensures compliance with accepted standards on security, quality, completeness, and access control? Secondly, how could interoperability between users of each particular subdomain of eHealth be ensured? The key question here is to ensure patient safety. The steps taken in the epSOS project may well serve as a model. Thirdly, how could network security be well-defined and based on the highest level of secure VPN technology between professionals or secure encryption in communicating with patients?

During the operational phase of transnational eHealth projects a body should be established to ensure the audit and oversight control of the participating nations and to resolve differences between them. This may be a part of the new, pan-European Data Protection Board or similar high level organisation, but it needs to be supplemented by health professionals. Since ethical standards and pressure may arise because of new breakthroughs in treatments (genetics, for instance), a common set of ethical standards probably needs to be continuously updated. The decommissioning of transnational eHealth solutions - like the pass-over from Baltic eHealth to R-bay - need to be planned and accepted by the participating countries, likewise ensuring that migration of vital patient data to new systems is made in a secure way.

3.2.12 Short summary of recommendations

- There is a need for agreement on a common baseline for the security of eHealth data, on a minimum set of requirements for the eIdentification of professionals and a framework for the cross-national acceptance of national IDs for patients/citizens (as is the objective of STORK 2), on a minimum set of standards for controlling access to EHR data and on a set of common standards for 'secondary use' - that is, the de-identification standards allowing EHR data to be used for research. In light of the new privacy regulation, the standards for patient consent, right to one's own data etc. also need harmonisation.

- The decision establishing a national identity system must be separated from the eHealth system. The general applicability of this eID system across domains and applications must be ensured in order to gain popular acceptance.
- Any progress towards a standardised, controllable eHealth environment needs to be incremental and coordinated by key stakeholders that define the basic principles and basic standards.

- The proportionality between security level, perceived threat and selection of principles for de-identification of patient records must be ensured.

- Health records for individual patients should not be destructed, but migrated to follow-on systems in a secure way.

- Standards for a pan-European system should be clearly defined and documented.

- In the design phase, it must be clear how a national control point could be established to act as a gateway to other EU countries and ensure compliance with accepted standards.

- In the operational phase of transnational eHealth projects, a body should be established to ensure the audit, oversight control and resolution of differences between the participating nations.

- The decommissioning of transnational eHealth solutions needs to be planned and accepted by the participating countries.

3.3 Case study 3: ePassport

3.3.1 Scope of the study and objective

Since August 2006, Council Regulation EC No 2252/2004 has required the 27 Member States of the EU to issue e-Passports that contain a digital facial image. Since June 2009 the Regulation requires Member States to issue second generation e-Passports that include two fingerprints (Council Regulation (EC) No 444/2009). All European Member States are obliged to integrate biometric data into passports and travel documents: a digital facial image and two fingerprints (Council Regulation (EC) No 444/2009). After the adoption this regulation, EU Member States have made significant investments in order to include biometrics into their new passports. But the way in which the biometric data is gathered, stored and used differs among Member States. This case study examines the implementation of Council Regulation EC No 2252/2004 in several individual Member States and addresses the consequences for the main research issues of this project: network security, interoperability, identification, usability, privacy, access control and function creep. 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 have been desk research, questionnaires and interviews. The second interim report of this project describes the full details of the case study, including the country findings. In this final report, we will present the highlights and main findings of the case study.

3.3.2 European framework

Since August 2006, Council Regulation EC No 2252/2004 has required the 27 Member States of the EU to issue e-Passports that contain a digital facial image. Since June 2009 the Regulation requires Member States to issue second generation e-Passports that also include two fingerprints (Council Regulation (EC) No 444/2009). The policy objective of the Regulation is '…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 e-Passport chip should make it easier to verify the authenticity of the passport and strengthen the link between the passport and the legitimate holder of the passport.

3.3.2.1 European context and decision making

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. Europe was under pressure from the United States regarding the use of biometrics in border control. In policy making, the link between biometrics and the battle against terrorism was firmly set, although this still remains to be proven. It had become a common understanding that biometrics would play a strategic role in solving various issues regarding identity fraud, organized crime and terrorism, despite the many unknowns about the introduction of a biometric system on such an unprecedented scale and the lack of empirical data on the performance of such systems (de Hert 2005).

3.3.2.2 Biometrics: the technology

In order to better understand the impact of this Regulation and the challenges it creates, a short introduction to biometrics is needed. Biometric technology is used to identify a person based on his or her physical characteristics, such as a fingerprint or iris and are inherently based on probability. A digital image of a physical identifier (e.g. face or finger) is analysed using special software to extract its relevant characteristics. These are 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) or by 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 indicates the likelihood a match has been found. That means that there will always be a chance that the system fails to make a match or makes a mismatch. 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 human oversight. A high rate of mistakes will make a biometric system inefficient and unreliable. To prevent this, high demands on the quality of the biometric data are necessary.

The foundation of every biometric system is thus the biometric image: the picture that is taken of the face, finger, iris or other physical characteristic. The quality of this image has a major impact on the 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 e-Passport) 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).

3.3.2.3 History of biometrics: from law enforcement to civil domain

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. There are four main differences between the use of biometrics in passports and for law enforcement:

1. In law enforcement there is a closed group of data subjects. The 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 typically 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 low 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.

3.3.3 Challenges of the e-Passport

The EU regulation focuses on the passport document and its use at border control. No specifications or requirements are mentioned in the regulation regarding the application, production and issuance process of the e-Passport. Specifications of the quality requirements of the facial and biometric images are also missing. The next paragraphs show how this has impacted the implementation of the e-Passport in European Member States and address the resulting challenges regarding security, interoperability, privacy and usability. These findings are based on the country studies conducted for the Second Interim Report of this project.

3.3.3.1 Security of the e-Passport

Chip security

The personal data, the facial image and the fingerprints contained in the chip within the passport are protected by two security mechanisms: the Basic Access Control (BAC) and the Extended Access Control (EAC)[23]. BAC protects the personal data and the facial image on the passport via encryption. Experts have stated that BAC is not sufficient to protect the data stored on the chip, it only prevents simple skimming attacks (WP29 2004; FIDIS 2006a).[24] This was confirmed by the more recent Frontex study (2011). To improve security the new Supplemental Access Control (SAC) standard will replace BAC in the long term.

Fingerprints are securely stored through Extended Access Control (EAC) through a Public Key Infrastructure (PKI) system. The digital keys are generated and controlled by the government of the country where the passport is registered. Apart from the technical complexity of distributing and updating these keys, Member States seem reluctant to share the keys with certain other countries, due to a lack of trust caused by security, political or other issues. 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 thus still not 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). 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

[23] 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.

[24] Fidis, Budapest Declaration on Machine Readable Travel Documents (2006), available at http://www.fidis.net/press-events/pressreleases/budapest-declaration/#c1307

Key Directory[25]. However, currently 12 EU Member States (and 30 countries worldwide) use the Public Key Directory[26]. In practice, the fingerprints are not adding security to the e-Passport.

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. Regarding the capturing of the facial image and fingerprints, the integrity of these data largely depends on the skills and reliability of the operating personnel and the security of the equipment being used. Only a few countries have certified personnel for taking the biometric data. There is therefore a risk that fake or wrong fingerprints can be 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. 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 addition there are no EU quality requirements (yet) for the biometric images, meaning that low quality images could be stored in the passport chip. There are considerable differences in quality scores between European Member States. In Germany, 73% of the fingerprints have the highest quality score (NFIQ 1) and 17,6% has NFIQ 2. In Italy, only 52% is of the highest quality (NFIQ 1), 22% has NFIQ 2. Low quality means more mistakes and more use of back up procedures (to handle exceptions). In practice, this results in a higher tolerance to lower probability scores in order to prevent too many rejections. This threatens the security level of the passport verification process and subsequently the security of the border control process.

3.3.3.2 Interoperability

Technical interoperability exists for the Basic Access Control, protecting the facial image in the passport. Nevertheless, Frontex (2011) 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 Machine Readable Zone (MRZ, part of the passport identity page that contains a unique string of characters and can be read automatically) being properly scanned, incorrect signatures, low level technical problems with the RFID chip and various other issues. As a result, border guards might not be able to use e-Passport data.

Theoretically, technical interoperability also exists for the Extended Access Control, protecting the two fingerprints. But in practice, EAC interoperability is hindered by problems with the current key distribution mechanism. Only a limited number of countries subscribe to the alternative developed by the ICAO. As a result there is non-interoperability in practice and fingerprints that are stored in the e-Passport aren't generally used for border control purposes.

The interoperability of biometric products is also an issue at the level of image quality and template design. Member States are supplied by a variety of vendors, each using their own equipment, causing interoperability problems between countries. There are still no independent criteria or independently validated tests 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

[25] http://www.icao.int/Security/mrtd/Pages/icaoPKD.aspx

[26] 8 March 2012,
http://www.icao.int/Security/mrtd/Downloads/PKD%20Documents/ICAO%20PKD%20Participant%20Contact%20List.pdf

might involve high costs and practical problems because a complete redesign of the software application and re-enrolment of all biometric data might then be needed.

Furthermore, there are in Europe 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).

3.3.3.3 Privacy, function creep and identification

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 (i.e. without the person involved being aware of the capturing). 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 limited in number.

Privacy issues regarding the biometric passport occur at four levels: the e-Passport itself; the management and handling of the personal data (including biometrics) at border control checkpoints and other passport control situations; additional uses of centrally stored biometric data, potentially 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. Within the EU, the data protection directive is implemented differently, which adds to the difficulties citizens face when trying to attain justice. 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, errors should be made available to the data subjects, compliance with privacy and data protection regulation needs to be enforced more strongly and function creep needs to be combated via the principle of proportionality (Lodge 2010; de Hert and Sprokkereef 2010; Venier and Mordini 2011).

Function creep

So far (EC) No 2252/2004 is clear and restrictive regarding the purpose for using the biometric data, as Art. 4.3 says: "(…) 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 preamble sub 5) states that: "(…) 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.

Country studies conducted in the second interim report of this project 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 (Snijder et al, 2012). 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). 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).

A related issue is that biometric data taken for the e-Passport don't seem suitable for law enforcement purposes. The regulation (EC) No 2252/2004 only requires two fingers to be scanned and stored in the passport. If 'one-to-many' (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. Secondly, the quality of the biometric data is 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. For 1:n searches typical in law enforcement it is even more difficult. 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).

3.3.3.4 Usability

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.

3.3.4 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). In April 2010 BIG submitted a discussion paper on fingerprint images to the BIG meeting.[27] 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

[27] Bob Carter, April 2010, "Issues with acquiring and recording of finger images: discussion paper for BIG"

"….with today's matching algorithms an NFIQ score of 3 or less is not likely to be verified." However, the suggestion has not 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 BIG should be supportive of activities which aim to improve image quality. However, 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 so far.

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. This decision also mentions the timeline for the replacement of the Basic Access Control (BAC) by the Supplemental Access Control (SAC) by 2025.

In 2011 a comprehensive – and rather critical – report by Frontex was published. As far as 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.[28] On 29 March 2012 the European Commissioner for Home Affairs Migration Ms Malmström stated that national accredited test labs are currently performing compliance tests[29]. 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.[30] 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.

3.3.5 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) or non-interoperable in practice (Extended Access Control). 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 common EU quality and integrity standards has created substantial differences in national implementations of the e-Passport 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

[28] Questions for written answer E-001306/2012 to the Commission
[29] www.europarl.europa.eu/sides/getAllAnswers.do?reference=E-2012-001306&language=ES#def1
[30] EC/JRC ISPRA - JRC TEMPEST Testing Laboratory, Conformance Testing of 2nd Generation e-Passports

mistakes and induce a higher tolerance to lower probability scores in order to prevent too many rejections. This results in lower thresholds throughout the EU which threatens the overall security level of the e-Passport 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 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 this case study 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 e-Passport could easily be used for law enforcement purposes. There was insufficient distinction in the political discourse between the use of biometrics used for verification and for identification. 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 e-Passport 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:

- 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;
    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. The development of high quality standards is complicated by the fact 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 (see also Munnichs et al. 2012). Individual Member States may weigh security, usability and other requirements differently.

- Improve the interoperability and security measures of the chip in the passport. The Basic Access Control seems not sufficient and it successor will not replace BAC until 2025. The Extended Access Control (protecting the fingerprints) is more secure, but requires a successful exchange mechanism, which is currently lacking.

- 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 and need to be harmonized.

3.4 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).

3.5 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.

3.6 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.

3.7 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.

4. European conference on Security of eGovernment

4.1 Conference scope

The third phase of the project was focused on initiating a constructive debate between experts, stakeholders and policy-makers about the challenges to having secure eGovernment systems at a European level. It was held as a one-day conference in the European Parliament. The target group of participants was MEPs, ICT and security experts and all parties interested in the subject of secure eGovernment services. The conference consisted of presentations from experts and stakeholders and debate with MEPs/stakeholders/other experts about the challenges and policy options related to securing EU eGovernment systems.

The scope of the conference was structured around the life-cycle approach (developed in phase 2 of the project) to eGovernment services and systems. The life-cycle approach was presented, and policy-related challenges to each phase of the life-cycle were debated. Furthermore three cross-cutting security issues of high importance to security in eGovernment were presented and debated. Questions of a security baseline were taken up at the end of the conference.

Examples from the case studies were used to illustrate concrete challenges to different applications of eGovernment services. The overarching aim of the conference was to focus on and debate possible policy actions on the EU level.

4.2 Conclusions of the conference

The conference, at which around 60 participants engaged in the various debate sessions, was a success. The conference was opened by Malcolm Harbour, British MEP and member of the STOA panel. His opening remarks stressed the importance of cyber-security.

The first session featured the authors of the report from the second phase of the 'Security of eGovernment' STOA project, who presented the key findings from three case studies. Linda Kool from The Rathenau Institute, the Netherlands, pinpointed the challenges to biometric verification and the ePassport. These challenges were mainly connected to the lack of quality and integrity standards and to inadequate legislation at the EU level. There were no clear criteria regarding the performance of biometric verification and no uniform and verifiable criteria for the quality and integrity of biometric images and the application and issuance process.

Arnd Weber from KIT, Germany, talked about the main challenges to cross-border eProcurement in Europe. He pointed to the risk of confidential information being stolen in an attack, e.g. with an infected email attachment. There is a lack of interoperability among hundreds of seldom used platforms employing different security tools, such as shared secrets and various types of digital signatures and encryption procedures.

Soeren Duus Oestergaard from Duus Communications, Denmark, showed the results from the study on the EpSOS Cross Border eHealth (2008 – 2013) and Baltic eHealth Project (2005 – 2007). It was possible to counter the challenges he noted by employing a common baseline for the security of eHealth Data. He pointed to the need for a framework for the cross-national acceptance of eID and talked about a baseline set of standards for access control. This included common standards for secondary use (like the de-identification for health data used in statistics, research etc.).

MEP Mr. Malcolm Harbour reflected on this first part of the conference by commenting on the critical balance between decentralisation and local customisation of eGovernment systems and (secure) interoperability of cross-border European systems.

The second session focused on security measures against attack. Chris Dalton from the Hewlett Packard Labs suggested distinguishing between security issues in (1) managed IT controlled by IT administrators and (2) unmanaged IT systems (smart phones, PCs at home etc.). There are two types of attacks: *malware attacks* and *ransomware*. Malware attacks compromise IT systems (for example by injecting code in a server) and are able to collect sensitive information. In *ransomware* attackers encrypt information and demand a ransom for returning the information or not disclosing it to the public. Dalton pointed out that both new hardware and operating systems are getting better and better in terms of security. Managed systems can benefit from these (new) hardware features. Although there will always be a risk of security breaches, there are several ways to minimize such breaches. Introducing security checklists, such as the "SANS 20 critical security controls", would significantly improve the security of eGovernment systems in Europe and could be recommended as a security baseline. With regard to unmanaged systems and mobile systems without the new features, however, Dalton recommended keeping them away from sensitive data.

Gernot Heiser from NICTA, Australia, argued for stronger security through the use of proven microkernels to iron out security breaches. He pointed out that eGovernment is an interaction between a government server and a terminal. Attacks can strike both or hit in between. These services include many errors in the millions of lines of code which create security vulnerabilities. Using virtualization decreases vulnerability, but even virtualization is still vulnerable to attacks. Gernot Heiser suggested using proven microkernel technology for the server side. Securing the terminal side, however, is more difficult, but new technical solutions are being developed. Gernot Heiser made it clear that the lack of business cases for secure systems hinders the improvement of security for (eGovernment) services. Heiser recommended that public institutions take the lead and create a market by investing in such systems or providing incentives by making the use of proven kernels mandatory.

Finally, Florent Kirchner from CEA LSL Labs, France, encouraged more fundamental research into formal methods in his forward-looking account and recommended striving for complete security rather than just making it as hard as possible to break into eGovernment systems. Florent Kirchner pointed out that layering different security measures is simply not sufficient. Rather, guarantees would be needed and should be required.

The ensuing debate in this session reached agreement that the lack of business cases for security investments is an important barrier to improving the security of eGovernment systems. The financial costs of the many attacks do not seem to hurt enough to prompt decisive action. Although security measures will never be absolute – it will always be a trade-off between the effort to protect and the value of what we are protecting – the current security standard is low in general and could be significantly improved by implementing for example check lists as suggested by Chris Dalton. Gernot Heiser pointed out that Australia has a 35 point check list. If only the top four measures from this list were implemented, the current threat level could be reduced by 85%. But the checklist would have to be implemented in a controlled and quality-oriented manner to be effective. It was argued that check lists are also of rather limited value because they merely shift the ground for attacks. When everybody has implemented the security baseline, attackers will just try harder. Therefore, the policy makers should consider requiring guaranteed components and systems.

The third session concerned privacy protection in eGovernment services. Peter Hustinx from the European Data Protection Supervisor underlined the importance of re-allocating the tasks and responsibilities of data controllers (e.g. the government organizations that operate eGovernment

services) and making them more accountable for privacy protection, which is currently proposed by the draft Data Protection Regulation (EC 2012). Peter Hustinx pointed out that a very high level of security is a must, but that good security is not necessarily equal to good privacy. Peter Hustinx indicated that the draft regulation aims to replace the current diversified legal framework of diverse national implementation of the EU Data Protection Directive (EC 1995). Furthermore, the draft regulation aims to improve privacy protection by requiring Data Protection by Design, Data Protection by Default and Data Protection Impact Assessments.

David Wright from Trilateral Research & Consulting spoke on Privacy Impact Assessments (PIAs) as being mandatory in Canada, the US and the UK. He reported that these assessments lend practical force to the right to know and can improve the adoption and uptake of eGovernment services. PIAs are an instrument to improve transparency of and citizen confidence in eGovernment services. Wright defined PIA as a process for assessing the impacts on privacy of eGovernment services and, in consultation with stakeholders, taking remedial action as necessary to avoid or minimise the negative impacts. The proposed Data Protection Regulation makes PIAs mandatory (EC 2012). However, David Wright recommended improving article 33 of the Regulation by (1) making these assessments "required for such processing operations even on a small scale" instead of only on a large scale, (2) using the term Privacy Impact Assessment rather than Data Protection Impact Assessment, 3) citing the benefits of PIA in the recitals of the draft regulation, 4) encouraging auditing and publication of the PIA report (if necessary, redacted) and 5) obliging organizations to keep a public registry of their PIA reports.

Michael Waidner from Fraunhofer SIT highlighted the challenges to technical privacy and their solutions, which include purpose violation, lack of data minimization, lack of control, lack of knowledge, incorrect data, unauthorized data, persistency, context violation, and the risks associated with anonymous aggregated data. Technical privacy protection for improving confidentiality is widely deployed. Recent techniques such as privacy-preserving attribute-based credentials have matured, can be implemented on smartcards and are now ready for commercial use. Techniques for privacy-preserving computations such as homomorphic encryption are prototyped. He gave four recommendations: (1) demonstrate the positive impact of privacy protection measures on innovation and prosperity (by keeping an inventory of business ideas and capabilities), (2) mandate and enable informed consent by using, e.g. privacy agents, (3) consider that the difference between personal and anonymized data have eroded, and (4) encourage privacy by design with concrete tools and architectures, e.g. by supporting anonymous credentials.

The fourth session was designed to discuss the challenges posed by interoperability of cross-border eGovernment systems in Europe. Linda Kool opened this segment by summarising certain findings from the case studies relating to different aspects of interoperability: (1) legal challenges to interoperability, e.g. the different national implementations of European Directives, (2) technical challenges to interoperability, e.g. different national tools that are not compatible, (3) semantic challenges to interoperability, e.g. information exchange problems due to different languages (even within the same national region). The case studies show that some services need more European harmonisation, while other services such as increased harmonisation and the use of a single European system increase security threats.

Walter Castelnovo from the University of Insubria, Italy, shed light on the aspects of interoperability with a recommendation to focus more strongly on services that create value for the user and allow European citizens to interact with public administrations in different Member States as if they were all members of a (virtually) integrated system of European public administrations, which again would contribute to strengthening the European citizens' perception of living and working in a single market.

Juliet Lodge (University of Leeds) opened by addressing the important factor of trust in the relationship between users and eGovernment services. She recommended enforcing and requiring ICT and application developers to have transparent ethical codes/mores regarding multipurpose use. She made it clear that it should be reasonable to require a certain moral behaviour from big market players. Ethical values and practice must inform and work with information collection, encourage correct handling etc., but they can only do so if human intervention is visible, identifiable and accountable. Transparency is vital. A secure eGovernment solution must uphold transparency and accountability to ensure trust when society is permanently online.

Antonio Lioy, Politecnico di Torino, Italy, reported findings from the STORK project, which has implemented interoperability gateways. He characterized security as a difficult and elusive target. He noticed that different countries use different eIDs of variable strength, which can be seen as an advantage, because it minimizes risks of choosing the wrong – i.e. insecure or uneconomic – solution for all. The interoperability solution chosen in STORK permits the use of all of these European ID systems, yet it does not compromise security, rather it supports adaptive security where each electronic service can request (and receive) the appropriate level of protection. Any country can adopt a new eID technology without breaking its interoperability with the other countries.

As the conference drew to a close, MEP Amelia Andersdotter commented on some of the questions from the audience and a constructive debate evolved, e.g. on the role of governments creating incentives for more secure IT systems. MEP Paul Rübig closed the conference by referring to the role of ethics, incentives, and enforcement.

5. Assessment of policy options

During the STOA project about the security of eGovernment systems a number of relevant questions have been raised, discussed and evaluated. The overall focus of the project and the analysis has been the most relevant security threats to eGovernment and the possible measures to counter them. One of the overall aims of the work has been to offer policy relevant advice on how to overcome the security-related barriers to a European Interoperability Framework for eGovernment services.

The following policy option assessment will recommend a number of initiatives for fostering eGovernment capacity building through more secure services. As part of the project three case studies have been carried out. The policy options presented in this chapter focus on the general challenges to security identified in these case studies. However, some case-specific policy options have been developed as part of the case study work. The case-specific policy options can be found at the end of each case study (Chapter 3).

The overall level of security of European eGovernment systems must be raised, as applications become more sensitive and as attacks become more sophisticated. The purpose of the policy options suggested below is to promote increased levels of security. The policy options assessment outlines an overall roadmap towards increased the security of European eGovernment systems and points out the necessary short-term, medium-term and long-term steps towards increased security.

- In the short term the level of security can be increased by establishing a European baseline of security for all European eGovernment systems, via the comprehensive use of security checklists.
- In the medium term, increasing security can be achieved by promoting security by design (e.g. isolated components, proven designs, certified software etc.).
- In the long term, it could be relevant to consider more "radical" ways of ensuring security, such as a "clean slate" design as is being pursued by the US DARPA (2012).

However, as explained in Chapter 2, measures to increase security cannot be considered in isolation. Security issues interrelate with cross-cutting themes such as privacy, interoperability and costs. Furthermore, the design and organization of eGovernment systems need to consider important issues such as acceptability and cost–benefit relations. These interrelations have been taken into account throughout the project and therefore the policy option assessment will be focusing on promoting four overall aims:

1. Improving the resilience of European eGovernment systems
2. Increasing privacy protection
3. Achieving interoperability
4. Matching political ambitions with technological possibilities and benefits

An overview of all policy options can be found in Box 2 below.

Overview of policy options:

Aim 1: Improving the resilience of European eGovernment systems

Policy Option 1: Develop a policy strategy for improving the security of IT systems used in Europe

Policy Option 2: Stimulate development and use of security checklists (short term)

Policy Option 3: Encourage the development and use of highly secure components (medium term)

Policy Option 4: Encourage the development and use of highly secure systems (long term)

Policy option 5: Create stronger institutional supervision and oversight of security implementation at the EU and Member State levels

Aim 2: Increasing privacy protection

Policy option 6: Build a 'Privacy by Design' knowledge base

Policy option 7: Substantiate the data minimization principle by using anonymization techniques in all European eGovernment systems

Policy option 8: Stimulate technical and legal solutions that avoid or limit privacy risks caused by the re-identification of previously anonymized data

Policy option 9: Make Privacy Impact Assessments of eGovernment systems mandatory and public

Aim 3: Achieving interoperability

Policy option 10: Use gateways to achieve interoperability of different national eGovernment security tools, but strive for Europe-wide availability and usability of tools

Aim 4: Matching political ambitions, technological possibilities and benefits

Policy option 11: Ensure the open and transparent evaluation of the trade-offs between privacy, security, usability, interoperability and costs of an eGovernment system

Box 2: Overview of Policy Options

5.1 Aim 1: Improving the resilience of European eGovernment systems

A common European security baseline aims to raise the general level of security in European eGovernment services and systems. The development of such a baseline starts by outlining a security strategy at a political level that presents a roadmap of security measures for Europe. Implementing a security check list could be the short-term measure to start improving the level of security of eGovernment services. In the medium term perspective it would be relevant to start looking at policy options that can achieve Security by Design of crucial components. In the long-term, policy measures that push for highly secure entire IT systems become relevant.

Policy Option 1: Develop a policy strategy for improving the security of IT-systems used in Europe

Currently, a coherent overall strategy regarding IT security in Europe is lacking. The Cybersecurity Strategy of the European Union[31] is a step in the right direction. The strategy is accompanied by a proposal for legislation to establish common requirements for network and information security at the national level which would oblige Member States to designate national competent authorities for network and information security and adopt a national strategy and a national security cooperation plan, among other things.[32]

A more comprehensive and long-term security strategy would cover all usage of IT systems in Europe, and thus also address systems used for eGovernment. The strategy would comprise items such as:

- Measures to be applied in the short run, such as encouraging government users to improve the security of their running systems by using security checklists, rules on the use of access with mobile devices, rules on the use of smartcard readers with display, recommendations for private users, etc.
- Key content of future legislation, covering e.g. issues as mentioned in the draft cyber security directive, paths towards more secure computers and networks, etc.
- Descriptions of means to reach comprehensive protection against attacks on networks and computers, even against "Advanced Persistent Threats" or "spear phishing" attacks, which may even include production of hardware in Europe.
- Concepts and plans for a comprehensive avoidance of processing personal data (e.g. plans for the avoidance of data up to moving towards unobservable communication).

Policy Option 2: Stimulate the development and use of security checklists (short term)

There are various checklists available to improve the security of running servers. A very comprehensive one is the SANS/CPNI-list (SANS 2012), and a more basic one is the baseline security standards produced by German BSI (BSI 2013). Such lists are to a certain degree known to IT professionals, but should be followed comprehensively by more institutions. The use of such lists should be evaluated, the development of tools for the automation of the procedures may need to be encouraged, and finally one or more lists could be recommended for use in eGovernment, or even made mandatory. Such lists may not be applicable to PCs, mobile devices and any computer used by citizens, as these are less thoroughly designed and used with a large variety of programs.

Figure 2 (overleaf): SANS/CPNI 20 critical security controls

[31] European Commission, High Representative of the European Union for Foreign Affairs and Security Policy, "*Joint Communication to the European Parliament, The Council, The European Economic and Social Committee and the Committee of the Regions. Cybersecurity Strategy of the European Union: An open, Safe and Secure Cyberspace.*" Brussels, 7. February 2013

[32] European Commission, "*Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union*" Brussels, 7. February 2013

1	Inventory of Authorized and Unauthorized Devices	**Reduce the ability of attackers to find and exploit unauthorized and unprotected systems:** Use active monitoring and configuration management to maintain an up-to-date inventory of devices connected to the enterprise network, including servers, workstations, laptops, and remote devices.
2	Inventory of Authorized and Unauthorized Software	**Identify vulnerable or malicious software to mitigate or root out attacks:** Devise a list of authorized software for each type of system, and deploy tools to track software installed (including type, version, and patches) and monitor for unauthorized or unnecessary software.
3	Secure Configurations for Hardware & Software on Laptops, Workstations, and Servers	**Prevent attackers from exploiting services and settings that allow easy access through networks and browsers:** Build a secure image that is used for all new systems deployed to the enterprise, host these standard images on secure storage servers, regularly validate and update these configurations, and track system images in a configuration management system.
4	Continuous Vulnerability Assessment and Remediation	**Proactively identify and repair software vulnerabilities reported by security researchers or vendors:** Regularly run automated vulnerability scanning tools against all systems and quickly remediate any vulnerabilities, with critical problems fixed within 48 hours.
5	Malware Defenses	**Block malicious code from tampering with system settings or contents, capturing sensitive data, or spreading:** Use automated anti-virus and anti-spyware software to continuously monitor and protect workstations, servers, and mobile devices. Automatically update such anti-malware tools on all machines on a daily basis. Prevent network devices from using auto-run programs to access removable media.
6	Application Software Security	**Neutralize vulnerabilities in web-based and other application software:** Carefully test internally developed and third-party application software for security flaws, including coding errors and malware. Deploy web application firewalls that inspect all traffic, and explicitly check for errors in all user input (including by size and data type).
7	Wireless Device Control	**Protect the security perimeter against unauthorized wireless access:** Allow wireless devices to connect to the network only if it matches an authorized configuration and security profile and has a documented owner and defined business need. Ensure that all wireless access points are manageable using enterprise management tools. Configure scanning tools to detect wireless access points.
8	Data Recovery Capability	**Minimize the damage from an attack:** Implement a trustworthy plan for removing all traces of an attack. Automatically back up all information required to fully restore each system, including the operating system, application software, and data. Back up all systems at least weekly; back up sensitive systems more often. Regularly test the restoration process.
9	Security Skills Assessment and Appropriate Training to Fill Gaps	**Find knowledge gaps, and fill them with exercises and training:** Develop a security skills assessment program, map training against the skills required for each job, and use the results to allocate resources effectively to improve security practices.
10	Secure Configurations for Network Devices such as Firewalls, Routers, and Switches	**Preclude electronic holes from forming at connection points with the Internet, other organizations, and internal network segments:** Compare firewall, router, and switch configurations against standards for each type of network device. Ensure that any deviations from the standard configurations are documented and approved and that any temporary deviations are undone when the business need abates.
11	Limitation and Control of Network Ports, Protocols, and Services	**Allow remote access only to legitimate users and services:** Apply host-based firewalls and port-filtering and -scanning tools to block traffic that is not explicitly allowed. Properly configure web servers, mail servers, file and print services, and domain name system (DNS) servers to limit remote access. Disable automatic installation of unnecessary software components. Move servers inside the firewall unless remote access is required for business purposes.
12	Controlled Use of Administrative Privileges	**Protect and validate administrative accounts on desktops, laptops, and servers to prevent two common types of attack:** (1) enticing users to open a malicious e-mail, attachment, or file, or to visit a malicious website; and (2) cracking an administrative password and thereby gaining access to a target machine. Use robust passwords that follow Federal Desktop Core Configuation (FDCC) standards.
13	Boundary Defense	**Control the flow of traffic through network borders, and police content by looking for attacks and evidence of compromised machines:** Establish multilayered boundary defenses by relying on firewalls, proxies, demilitarized zone (DMZ) perimeter networks, and other network-based tools. Filter inbound and outbound traffic, including through business partner networks ("extranets").
14	Maintenance, Monitoring, and Analysis of Security Audit Logs	**Use detailed logs to identify and uncover the details of an attack, including the location, malicious software deployed, and activity on victim machines:** Generate standardized logs for each hardware device and the software installed on it, including date, time stamp, source addresses, destination addresses, and other information about each packet and/or transaction. Store logs on dedicated servers, and run biweekly reports to identify and document anomalies.
15	Controlled Access Based on the Need to Know	Prevent attackers from gaining access to highly sensitive data: Carefully identify and separate critical data from information that is readily available to internal network users. Establish a multilevel data classification scheme based on the impact of any data exposure, and ensure that only authenticated users have access to nonpublic data and files.
16	Account Monitoring and Control	**Keep attackers from impersonating legitimate users:** Review all system accounts and disable any that are not associated with a business process and owner. Immediately revoke system access for terminated employees or contractors. Disable dormant accounts and encrypt and isolate any files associated with such accounts. Use robust passwords that conform to FDCC standards.
17	Data Loss Prevention	**Stop unauthorized transfer of sensitive data through network attacks and physical theft:** Scrutinize the movement of data across network boundaries, both electronically and physically, to minimize the exposure to attackers. Monitor people, processes, and systems, using a centralized management framework.
18	Incident Response Capability	**Protect the organization's reputation, as well as its information:** Develop an incident response plan with clearly delineated roles and responsibilities for quickly discovering an attack and then effectively containing the damage, eradicating the attacker's presence, and restoring the integrity of the network and systems.
19	Secure Network Engineering	**Keep poor network design from enabling attackers:** Use a robust, secure network engineering process to prevent security controls from being circumvented. Deploy a network architecture with at least three tiers: DMZ, middleware, private network. Allow rapid deployment of new access controls to quickly deflect attacks.
20	Penetration Tests and Red Team Exercises	**Use simulated attacks to improve organizational readiness:** Conduct regular internal and external penetration tests that mimic an attack to identify vulnerabilities and gauge the potential damage. Use periodic red team exercises—all-out attempts to gain access to critical data and systems— to test existing defenses and response capabilities.

Policy Option 3: Encourage the development and use of highly secure components (medium term)

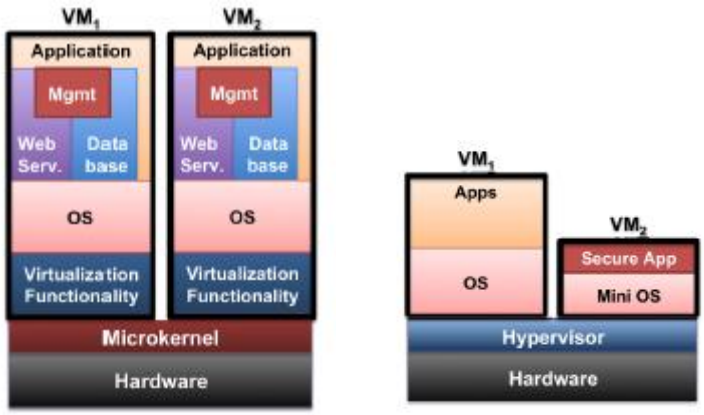
Depending on the threats, one goal should be the production of more secure components, be it operating systems, application software or tamper-resistant components. The use of certified product evaluations or certified development processes could be made mandatory, but will be very hard to enforce if components are produced outside the EU. Also, the discussion and implementation of product liabilities could help create demand for better software.

Policy Option 4: Encourage the development and use of highly secure systems (long term)

In the long run, it would be feasible to create computer systems with a much greater resilience to malware. For financial reasons, backwards compatibility with existing applications will be needed. A classical approach is to use isolation to separate sensitive applications from insecure ones (see Figure 3 for examples). Industry is pursuing such approaches, ranging from isolation with existing systems up to developing proven isolation (VMWare, LaGrande/TXT, SELinux, seL4). The US DARPA is attempting to design such systems in its "Crash" project (DARPA 2013). Even a well-specified system may, however, be implemented incorrectly, contain errors in proofs, have exploitable side-channels, rely on unproven mathematics, etc. Still, computer science has means to develop computers which are much more secure against even advanced attacks than those we use today. Designs for highly secure computers will have to address the hardware side, too, not only for obvious reasons, such as isolation in processors and memory, but also to make sure that hardware components do not contain Trojan horse functionalities (e.g. for eavesdropping or interrupting processes).

It would also be beneficial to have more secure environments should digital signature solutions be attacked. A system with secure user input and output would be an improvement over using a "qualified signature" card in an off-the-shelf computer.

Figure 3: Isolation based on a microkernel.



Examples of servers (left) and smartphones (right); VM = virtual machine, OS = operating system (Heiser 2013).

The process of migrating towards highly secure computers could be pushed with various means, ranging from creating awareness, producing communications (by the Commission, Parliament, or e.g. trans-Atlantic working groups), and supporting research to legislating rules on the liability of the producers of IT systems and the quality of systems and components (e.g. certified or proven). The rules could apply to the components used in eGovernment only, but for financial reasons (creating economics of scale with IT suppliers) they should ultimately cover all systems, even non-European ones.

Policy option 5: Create stronger institutional supervision and oversight of security implementations at the EU and Member State levels

Various problems justify strong and fast supervision of IT-security processes. Industrial software has been hacked, IT-security companies can be attacked successfully, and certification authorities have been intruded, for example. Foreign components will lead to new risks; countermeasures must be updated, etc. Different institutional set-ups of such supervision are possible and need to be evaluated.

5.2 Aim 2: Increasing privacy protection

The case studies from the intermediary report from phase 2 as well as the debates from the conference and expert meeting reflect the fact that eGovernment systems pose significant privacy risks to citizens with regard to the collection, storage, processing and exchange of personal or confidential data. They highlight the need for improved privacy protection, both in terms of a better technical and legal position for citizens and other players to exercise control over their data.

The European Parliament and the Council are currently discussing a new proposal for a General Data Protection Regulation (EC, 2012) to replace the current Directive 95/46/EC. The new regulation aims to update the old framework in light of rapid technological developments, to strengthen the current data protection framework in Europe and to apply data protection legislation consistently in all Member States (EC, 2010). The draft regulation provides enhanced responsibilities for organisations, including government bodies, that process or control personal data[33], such as the implementation of "data protection by default" and "by design", conducting "data protection impact assessments". The draft regulation also provides data protection authorities (DPA's) stronger supervisory powers, including the possibility to impose higher fines on organisations that do not comply with the measures in the regulation[34]. In addition, citizens' or data subjects' rights are strengthened by increasing the requirements for transparency in data processing and include new rights such as the "right to be forgotten" and the right to "data portability"[35]. Furthermore, the draft regulation aims to harmonize data protection legislation in Europe to be directly applicable in all Member States and replace current national laws. It also proposes to establish a European Data Protection Board that would replace the current Article 29 Working Party. The Board aims to prevent different responses from national DPA's and to address complicated and cross-border issues in a consistent manner.

The implementation of this regulation would be a clear step in the right direction. The following policy options build on the measures proposed in the draft regulation and propose additional measures to increase privacy protection in Europe.

Policy option 6: Build a 'Privacy by Design' knowledge base

Privacy by Design is currently included in the revised draft regulation for data protection in the EU (EC 2012), referred to as 'Data Protection by Design'. This will increase incentives to implement Pivacy by Design (PbD) for both suppliers of IT-systems that process personal data and for (government) organisations that procure such systems.

To further stimulate the adoption of PbD, the development of a public knowledge base is necessary. The knowledge base should include reference architectures, design patterns, anonymization and

[33] Data controller is the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data and that bears the responsibility for compliance with data protection regulation. The data processor is the natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller.

[34] See article 79, with fines up to 1 000 000 EUR or, in the case of an enterprise up to 2 % of its annual worldwide turnover for specific breaches in data protection.

[35] Respectively articles 17 and 18

pseudonymization techniques in order to specify what PbD entails, showcase practical experiences and improve the level of knowledge in the EU about Privacy by Design in general. The knowledge base, and possibly its mandatory use, strengthens the skills and capabilities of IT suppliers, IT professionals and programmers to implement privacy-enhancing features in their systems.

Several EU funded scientific projects, like PRIME, PRIMELIFE and ABC4Trust, provide the basis for this knowledge platform. The development of such a knowledge base requires funding and continuous maintenance and should be placed in the care of an independent organisation at the European level, for example the European Data Protection Board or a similar high-level organisation.

Policy option 7: Substantiate the data minimization principle by using anonymization techniques in all European eGovernment systems

An important element of the data protection framework in Europe is the principle of data minimization, meaning that data controllers (such as governments collecting and processing citizens' data) should limit the collection of personal information to what is directly relevant and necessary to accomplish a specific purpose. Data controllers should also retain the data only for as long as it is necessary to fulfil that purpose.

A strong way to implement this principle that significantly reduces the privacy risks for citizens is to limit the amount of personal data that is collected, stored, processed and exchanged by governments. This can be achieved by using currently mature privacy enhancing techniques. These techniques include attribute-based credentials, encryption, decentralised data storage, anonymisation and pseudonymisation (see Table 4 for a description of these terms). The techniques help avoid identifying users while allowing typical functionalities of eGovernment systems, such as checking statements with information on the status or rights of a citizen.

A promising example of these techniques are privacy-preserving attribute-based credential systems (as developed by the EU funded research project ABC4Trust https://abc4trust.eu/). These systems enable the authentication of users (e.g. verifying the status or citizens´ rights, such as receiving state benefits) without identifying all the information about that particular individual.

These techniques have matured and are deemed ready for commercial use. This would enable government organisations that procure IT systems to mandate the use of such techniques in their systems.

Table 4: From protection of personal data to unobservability

Protection of personal data	Legislative, technical and organisational means are used to preserve the confidentiality of personal information
Pseudonymity	A pseudonym is an identifier of a subject other than one of the subject's real names, thereby hiding the identity of the subject. Pseudonyms should be designed in a way that their use is untraceable. However, information such as IP addresses may in practice be used to de-anonymize pseudonymous data
Anonymity	Anonymity means that a subject can use a service without being identified, i.e. the subject is not identifiable within a set of subjects. De-anonymization may be possible.
Unlinkability	Unlinkability of two or more items of interest (data on a network) means that within the system, the attacker cannot sufficiently distinguish whether these items are related or not.
Undetectability	Undetectability of data (i.e. an item of interest) means that an attacker cannot sufficiently distinguish whether the item (data) exists or not.
Unobservability	Unobservability is defined in terms of undetectability (see description above) and anonymity (see description above). This means that third parties or attackers cannot trace a particular individual.

Source: adapted from Pfitzmann and Hansen, 2010

Policy option 8: Stimulate technical and legal solutions that avoid or limit privacy risks caused by re-identification of previously anonymized data

The increasing use of the Internet, mobile phones and cloud computing has resulted in a continuously increasing availability and use of large data sets. They provide new financial and social opportunities for citizens, businesses and governments. In recognition of the financial and societal potential, the European Commission and the national Member States stimulate the access to and re-use of (anonymised) Public Sector Information by third parties for the development of new products and services (EC 2013, EC 2003).

However, these large data sets, or their combination with other available datasets, can reveal personal data of citizens and consumers. Even anonymized datasets pose privacy risks as it is technically very difficult to fully anonymize personal data (see for example Sweeney 2002; Dalenius 1986 and Koot, 2012). Through the large availability of datasets, anonymized data can be recombined with other data sets and subsequently individuals can be 're-identified'. This results de facto in an erosion of the difference between personal and anonymized data. Currently, no (mature) technical or legal solution to this risk is available.

To address the aggravated risk of re-identifying previously anonymized data, funding is needed for research and development of technical solutions that hinder de-identification and improve full anonymization of data sets. Relevant examples include techniques like differential privacy (Dwork, 2009). In some Member States asking for consent is necessary in the current data protection legislation. The new draft data protection regulation (articles 81 and 83) allows for the processing of personal data for statistical, historical or research purposes, without requiring consent or notifying data subjects. This is relevant not only for medical data, but also for other public sector information.

To limit the risks of re-identification, the draft data protection regulation could restrict the use of anonymized data to healthcare and research purposes of "high public interest" (Brown et al 2011), or could ensure a minimum level of transparency by notifying data subjects and offer them means to opt-out or give their consent (opt-in).

Policy option 9: Make Privacy Impact Assessments of eGovernment systems mandatory and public

Privacy Impact Assessments (PIAs) refer to standardized and systematic procedures to identify privacy risks of systems that process personal data and ways to prevent or mitigate these risks (for example by using privacy-enhancing techniques). PIAs are therefore an important way to identify, reduce and manage privacy risks.

In countries, such as Canada, the US and the UK, conducting PIAs is already mandatory. PIA's (or 'data protection impact assessments') are now also included in the new EU draft data protection regulation. Data controllers will have the responsibility to perform a data protection impact assessment "where processing operations present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes" (EC, 2012, article 33).

To maximize the benefits of conducting PIAs, an additional policy option is to make PIAs publicly available (redacted if necessary) to promote public scrutiny and trust in eGovernment systems (Wright 2013). This could increase the evaluation of purpose and eligibility regarding data use and storage. Publishing PIAs would also make it possible for (government) organisations to learn from each others' ways to mitigate privacy risks. Furthermore, it increases transparency and can thereby strengthen the incentives of implementing Privacy by Design.

5.3 Aim 3: Achieving interoperability

Interoperability is another big challenge for cross-European eGovernment systems. This is not exclusively a security issue, but it has security aspects. Interoperability between systems and/or between countries is difficult to achieve and constitutes perhaps one of the most important barriers to European eGovernment services. In relation to security this is very much a question of the exchange of data, e.g. between different national eGovernment systems.

At the conference and at the expert meeting it was pointed out that it is important to accept that seamless interoperability is certainly desirable, but in many cases unrealistic given the sheer number of Member States and their resistance to change national rules and existing systems.

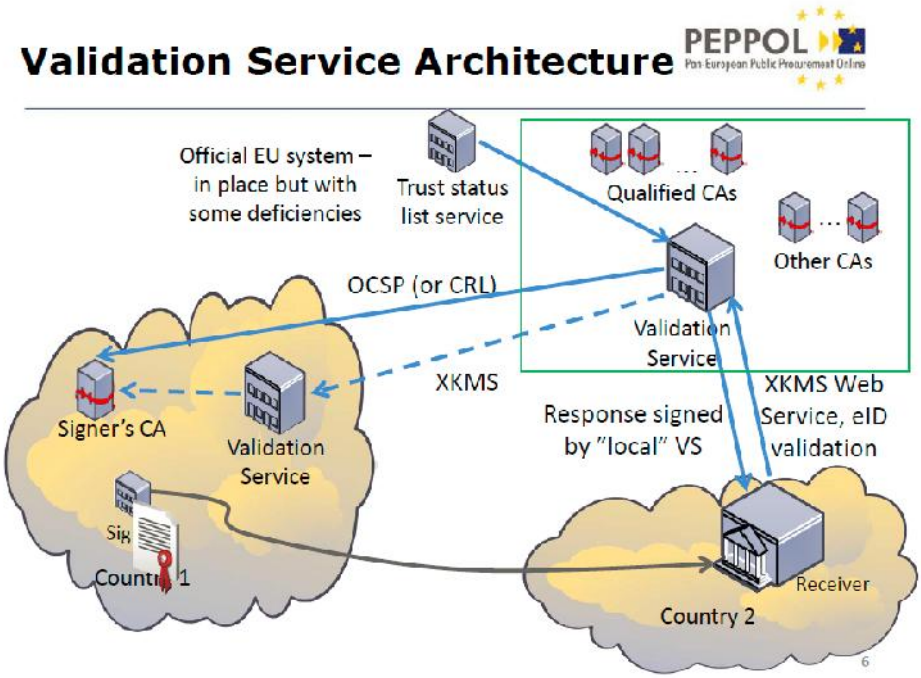
To handle the interoperability challenge it was argued that it is necessary to base every system on a minimum layer of interoperability meaning that only the absolutely necessary interoperability is implemented.

It was debated whether gateways are the way to reach interoperability to ensure the minimum layer of interoperability. Gateway servers would check whether requirements, e.g. with regard to the quality of the user identification, are met by a certain "foreign" procedure. This can be a procedure from another system, for example a particular cross-border eGovernment system. The gateway provides an automatic response to the party which has made the initial request. This approach was used in the EU project STORK (https://www.eid-stork.eu/), the architecture of which relies heavily on gateways to connect services rather than defining new standards and systems.

Policy option 10: Use gateways to achieve the interoperability of different national eGovernment security tools, but strive for Europe-wide availability and usability of tools

Today, considering the EU's unique situation (27 Member States, each with its own legislation, systems and organisations), gateway computers can be used to achieve interoperability of national security tools, such as ID or smartcards. Such a gateway could check, for instance whether a means of identification is sufficiently reliable for a foreign entity regarding the quality of a user registration process. However, such gateways come with costs, as envisioned by the pan-European procurement gateways, for example (Figure 4). Here, various national entities producing statements about the validity of a signature will be involved, using relevant auxiliary services, such as servers knowledgeable about national requirements, lost keys, etc. Such an infrastructure may lead to significant transaction costs. Therefore it would be desirable to have any security tool usable across Europe. Actually, competition between a variety of tools might be good, but each tool, e.g. an advanced signature, should be available in all countries and usable abroad. This may require far-reaching changes in the European legal setup, but would be very beneficial towards achieving a real common market.

Figure 4, PEPPOL Validation Service Architecture. Source: PEPPOL.



5.4 Aim 4: Matching political ambitions, technological possibilities and benefits

The decisions on the development and subsequently the design of eGovernment systems inherently involve political choices regarding safeguarding privacy, security, interoperability and costs. Different requirements may be at odds with each other. For example, interoperability between systems and across borders may lead to function creep and privacy risks, and high levels of security and privacy typically require higher financial investments. The case studies from phase 2 of the project show that current policy discussions often lack a clear and explicit decision regarding these trade-offs (see also Munnichs et al. 2012).

Policy option 11: Ensure open and transparent evaluations of the trade-offs between privacy, security, usability, interoperability and costs of an eGovernment system

Making political decisions on the purpose and design requirements of eGovernment systems requires policy makers, including Members of Parliament (both at the national and the European level), to have insight into the different architectural and organisational designs of a particular system, and into the consequences of those designs in terms of privacy, security, interoperability and costs.

This could be achieved through assessment processes with independent expertise. Such feasibility studies would be based on rough functionality and design outlines of a new eGovernment system. The feasibility studies should focus on aspects such as the purpose, scope, and impact on security and privacy, interoperability and usability. Furthermore, the studies should include a cost–benefit analysis and an assessment of the extent to which the system can actually meet the challenge for which it is designed.

Mandatory public feasibility studies ensure an open and transparent political evaluation and public scrutiny of an eGovernment system, particularly concerning the purpose of an eGovernment system and its trade-offs. The feasibility studies can significantly improve the design of a new eGovernment system and help prevent a mismatch between high political ambitions and what technology can actually deliver. Studies should be conducted from the design phase up to the roll-out of the eGovernment system.

An additional policy recommendation is to include mandatory upstream involvement of stakeholders to further improve the quality of the policy making in the design phase and, eventually, the quality of the resulting eGovernment systems (Misuraca et al. 2012). In order to design a system that will be adopted by businesses and citizens alike, stakeholders are required to be involved early in the design phase. Stakeholders must consider the usability and financial feasibility of the development of the system.

6. References

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

- Ampe, Floris: Golden Book 2012. http://de.slideshare.net/Nicolas_Loozen/golden-book-presentation-challenges-and-opportunities

- 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

- 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.
- Bilby, Ethan: EU report urges action against Chinese telecom firms. Brussels 2012. http://uk.reuters.com/article/2012/12/12/uk-eu-china-telecoms-idUKBRE8BB18420121212

- Benbasat, I., Goldstein, D.K. and Mead, M. (1987). The Case Research Strategy in Studies of Information Systems, MIS Quarterly (11:3), 369-386.

- Bhatnagar, S. (2004). E-Government: From Vision to implementation: A practical guide with case studies. Sage: New Delhi, Thousand Oaks, London.

- Bleyer 2011: Presentation at: Tag der IT-Sicherheit; Karlsruhe 2011

- 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

- Brown, I., Brown, L. and Korff, D. (2010), Using NHS Patient Data for Research Without Consent, aw, Innovation and Technology, Vol. 2, No. 2, pp. 219-258, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1753029

- BSI: IT-Grundschutz Catalogues. https://www.bsi.bund.de/EN/Topics/ITGrundschutz/itgrundschutz.html Access June, 6, 2013

- 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)

- 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.

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

- Dalenius, T. (1986) Finding a needle in a haystack – or identifying anonymous census record. Journal of Official Statistics, 2(3):329-336

- 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.

- DARPA (2013): Information Innovation Office. http://www.darpa.mil/Our_Work/I2O/Programs/Clean-slate_design_of_Resilient_Adaptive_Secure_Hosts_%28CRASH%29.aspx, access 17.3.2013

- DARPA: DARPA's UAS Cyber Defence $18M Project Goes Open Source. November 20, 2012. http://www.uasvision.com/2012/11/20/darpas-uas-cyber-defence-18m-project-goes-open-source/
- 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

- 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

- 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

- Dwork, C. (2009) *The Differential Privacy Frontier*, TCC 2009, LNCS 5444, pp. 496–502

- 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

- Eisenhardt, K. M. (1989). Building Theories From Case Study Research, Academy of Management. The Academy of Management Review.ENISA (2011). Who is Who-Directory, available at http://www.enisa.europa.eu/publications/studies/who-is-who-directory-2011

- 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: http://www.enisa.europa.eu/activities/identity-and-trust/privacy-and-trust/eid/xborderauth, retrieved June 6 2013

- European Commission (2003) Directive 2003/98/EC of the European Parliament and of the Council of of 17 November 2003 on the re-use of public sector information. Available online at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2003:345:0090:0096:EN:PDF

- 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 (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 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

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

- 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: 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: 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: 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 (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: eGovernment Factsheet - Portugal - National Infrastructure. 2012. http://www.epractice.eu/en/document/288346 (2012b)

- 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/eprocurement/strategy/COM_2012_en.pdf (2012d)

- 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 (2012) *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*, COM(2012) 11 final 2012/0011 (COD), 25.1.2012, http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

- European Council (2013) *Proposal for a Directive of the European Parliament and of the Council amending Directive 2003/98/EC on re-use of public sector information - Approval of the final compromise text*. 2011/0430. 15 April 2013
- http://register.consilium.europa.eu/pdf/en/13/st08/st08469-ad01.en13.pdf

- European Council (2013) Proposal for a Directive of the European Parliament and of the Council amending Directive 2003/98/EC on re-use of public sector information - Approval of the final compromise text. 2011/0430. 15 April 2013, http://register.consilium.europa.eu/pdf/en/13/st08/st08469-ad01.en13.pdf

- 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

- 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
- Frontex (2011) Operational and Technical security of Electronic Passports.
- 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, Hans; Lambert, Guy; Jossin, Brigitte; Meyvis, Eric: European eGovernment 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
- Grawrock, D.: The Intel Safer Computing Initiative. Intel Press, 2006.
- Hange, Michael: Presentation given at: Zukünftiges Internet, Berlin 2011
- Heiser, Gernot: White Paper: Protecting e-Government against attacks. Sydney 2013. In: Intermediate Report 3: Conference Report.
- Heiser, Gernot et al.: The Road to Trustworthy Systems. Communications of the ACM, 53(6), 107–115, June, 2010. http://ertos.nicta.com.au/publications/papers/Heiser_AEKKR_10.pdf.
- 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. 52no. 128, pp. 105 –117.
- 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)
- Kang, Hoin: The experience of the Republic of Korea. Presentation given at: Electronic Procurement – Challenges and Opportunities. 26 June 2012, Brussels.
- 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
- 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)

- Koot, M. (2012) Measuring and Predicting Anonymity. PhD Thesis, University of Amsterdam

- Lambrinoudakis, C., Gritzalis, S., Dridi, F., and Pernul, G. (2003). Security requirements for e-government services: a methodological approach for developing a common PKI-based security policy, Computer Communications 26 (16), 1873-83.
- Langner, Ralph: Stuxnet: Dissecting a Cyberwarfare Weapon, IEEE Security and Privacy Vol. 9 2011, http://doi.ieeecomputersociety.org/10.1109/MSP.2011.67

- Layne, K. and Lee, J. (2001). Developing fully functional e-government: A four stage model , Government Information Quarterly 18 (2), 122-136

- Lenk, K. and Traunmüller, R: (2000). A framework for electronic government, Proceedings of DEXA 2000, 340-345.

- Lodge, J. (2010) D7.1 - Biometrics in Europe: Inventory on politico-legal priorities in EU27 BEST Network

- Meijer, A.J. &Zouridis, S. (2004). E-government as Institutional Transformation, In: Innovations through Information Technology, M. Khosrow-Pour (ed.), Idea Group, Hershey PA, 2004, pp. 565 – 568.

- Misuraca, Gianluca; Savoldelli, Alberto; Codagnone, Cristiano (2012): Explaining the eGovernment Paradox: An analysis of two decades of evidence from scientific literature and practice on barriers to eGovernment. Presentation given at: ICEGOV 2012, Albany

- Munnichs, G., Schuijff, M. en Besters, M. (Eds) (2012) Databases: the promises of ICT, the hunger for information, and digital autonomy. Rathenau Institute

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

- 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

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

- OECD (2009). Rethinking e-Government Services - User-Centred Approaches: http://www.keepeek.com/Digital-Asset-Management/oecd/governance/rethinking-e-government-services_9789264059412-en

- 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

- Pfitzmann, A. and Hansen, M. (2010) *A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management*, v0.34, August 2010. http://dud.inf.tu-dresden.de/Anon_Terminology.shtml

- 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

- PWC: Golden Book of eProcurement Good Practice. 2011. http://ec.europa.eu/internal_market/publicprocurement/docs/eprocurement/conferences/121214_e-procurement-golden-book_en.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

- 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 eProcurement 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

- Sanchez-Reillo, R. (2012) presentation at European Biometrics Symposium, 17 February 2012 www.eab.org

- SANS: 20 Critical Security Controls. http://www.sans.org/critical-security-controls/. Access April 4, 2013

- 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)

- Silcock, R. (2001). What is eGovernment? Parliamentary Affairs, Vol.54, pp.88-101.

- 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

- Snijder, M., Kool, L., Munnichs, G. (2012) Case study e-Passport. In: Jacobi, A., Paldam

- Folker, M., Kool, L., Munnichs, G., Weber, A. (Eds) Security of e-Government Systems. Intermediate report 2: Case study Report – Phase II. Report prepared for STOA.

- 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

- 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

- Sweeney, L.: k-anonymity: a model for protecting privacy. International Journal on Uncertainty, Fuzziness and Knowledge-based Systems, 10 (5), 2002; 557-570;

- 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

- 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

- Venier, S. and Mordini, E. (2011) D7.3 - Overview of the ethical, social and policy implications of biometrics BEST Network

- Waidner, Michael: Presentation given at: Zukünftiges Internet. Berlin 2011

- 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

- Wright, D. (2013) Privacy impact assessment: an instrument for transparency and building trust in e-government services. Presentation given for STOA Workshop Security of e-Government systems, February 19 2013, Brussels, http://www.europarl.europa.eu/stoa/cms/cache/offonce/home/events/workshops/egovernment;jsessionid=CBFB072EC797E00C73B4FB610080B046

- 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

- Yin, R. K. (2002). *Case Study Research, Design and Methods*, 3rd ed. Newbury Park, Sage Publications.

This document is the final report of the STOA study: 'Security of eGovernment Systems'. A 'Conference Report' and a 'Case Study Report' are also available.

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-01-13-378-EN-C
DOI 10.2861/29262
ISBN 978-92-823-4618-1