ETAG
European Technology Assessment Group
ITAS · DBT · FCRI·ISI·IST·ITA ·TC ·Rathenau

Security of eGovernment Systems

Intermediate report 1: Elaborated Scope Description - Phase I

Deliverable No.1 of the STOA Project
“Security of eGovernment Systems”

Commissioned by STOA and carried out by ETAG
Order Form No. IP/A/STOA/FWC/2008-096/LOT4/C1/SC5
Ref.: Framework Contract No. IP/A/STOA/FWC/2008-096/LOT4

Paper prepared by

Marie Paldam Folker (DBT)
Anders Jacobi (DBT)
Jacob Kjærsgård Lester (DBT)
Christian van 't Hof (Rathenau Institute)
Geert Munnichs (Rathenau Institute)
Arnd Weber (ITAS)
Leonhard Hennen (ITAS)

August 2011

European Technology Assessment Group

- Institute for Technology Assessment and Systems Analysis (ITAS), Karlsruhe
- Danish Board of Technology (DBT), Copenhagen
- Catalan Foundation for Research and Innovation (FCRI), Barcelona
- Fraunhofer Institute for Systems and Innovation Research (ISI), Karlsruhe
- Institute Society Technology (IST), Brussels
- Institute of Technology Assessment (ITA), Vienna
- Rathenau Institute, The Hague
- Technology CentreAS CR, Prague

Contact:
Dr Leonhard Hennen (Co-ordinator)
Institute for Technology Assessment and Systems Analysis; Karlsruhe Institute of Technology
c/o Helmholtz-Gemeinschaft
Ahrstr. 45, D-53175 Bonn
Leonhard.Hennen@kit.edu

Project Description

Contract number IP/A/STOA/FWC/2008-96/LOT4/C1/SC5

The project is being carried out by the
The Danish Board of Technology (DBT), DK (project co-ordinator);
together with the Rathenau Institute (RI), NL and Institute for Technology Assessment and Systems Analysis (ITAS), DE, as members of ETAG.

Project Leaders: *Anders Jacobi and Marie Paldam Folker, The Danish Board of Technology, DBT*

Authors:

Marie Paldam Folker (DBT)
Anders Jacobi (DBT)
Jacob Kjærsgård Lester (DBT)
Christian van't Hof (RI)
Geert Munnichs (RI)
Arnd Weber (ITAS)

Members of the European Parliament in charge:

Mrs. Silvia-Adriana Ţicău, MEP

STOA staff in charge:

Mr. Vittorio Decrescenzo

Submission date:

August 26, 2011

EXECUTIVE SUMMARY

The security of electronic government is a core concern to citizens, governments and enterprises. As governments across the globe strive towards providing ICT enabled public services to citizens and businesses, safeguarding data and systems is of pivotal importance since it can influence governments and users willingness to adopt online services offered. The need to enhance security, privacy and trust in order to build up confidence in eGovernment services is globally recognized and the European Commission's eGovernment Action Plans require Member State commitment to the enhancement of security of eGovernment solutions at a local, regional, national and European level.

The STOA project 'Security of eGovernment Systems' aims to assist policymakers in discerning policy options for meeting future challenges in securing eGovernment systems. Supporting the mobility of citizens and businesses e.g. for patients to access their medical record in both their home state and where they receive treatment and allowing individuals to study, work, reside anywhere in the European Union is a key ambition of European policy making and regulation. 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 STOA 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 the EU. 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. Securing cross-border eGovernment services may additionally challenge existing regulations at national and EU level. The project will 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 this document we provide an elaborated scoping description of the project 'Security of eGovernment Systems' identifying seven cross-cutting security challenges for eGovernment systems set in the context of three case studies of cross-border eGovernment systems: eProcurement, border control and eHealth. The security challenges include network security, interoperability, identification, usability, privacy, access control and function creep. These cross-cutting security challenges will be examined in the context of our three case studies, each exemplifying different aspects of the security issue at hand. 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.

Contents

1. INTRODUCTION

This report is the first deliverable of the project ‘Security of eGovernment Systems’. The paper marks the end of the first phase of the project, the aim of which has been to further develop and specify the scope of the project and the scheduled tasks of the project. Work in this phase has included desk top research and talks with MEPs and security experts. In the course of this work a number of relevant issues have been considered, e.g. experience from existing eGovernment services in Europe at national and transnational level, best practice in existing eGovernment services, international examples of eGovernment services, relevant regulative frameworks, a number of national and international studies and guidelines on eGovernment and the most important security threats for eGovernment systems. Based on the preparatory study of these and other relevant security issues related to eGovernment the scope of the project has been elaborated and specified and the related work plan has been adapted.

An important aim of the first phase of the project has been to define the focus of the knowledge building in the second phase of the project. Based on the preparatory study with special attention to identifying relevant case studies for phase 2 of the project, three case studies for examining the security of cross-border eGovernment systems have been selected in the domains of procurement, border control and health.

Pre-phase work has also included the composition of a group of experts functioning as professional and scientific support to the project. The following scholars and experts have agreed to join the project’s expert group:

- Principal Research Scientist Chris Dalton, Hewlett Packard Labs, Bristol
- Professor Michael Waidner, Fraunhofer SIT Darmstadt
- Professor Juliet Lodge, University of Leeds
- Professor Antonio Lioy, Politecnico di Torino
- Project Leader Barbara Ubaldi, OECD (eGovernment initiative)

In this report we provide an elaborated scoping description of the project 'Security of eGovernment Systems' identifying the most challenging security concerns for eGovernment systems set in the context of three case studies. The cross-examination of case studies and security challenges of eGovernment systems constitute the work of the project’s next phase. The seven cross-cutting security challenges are: Network security; interoperability; identification; usability; privacy; access control and function creep. 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 report will introduce the case studies forming the core of project phase 2 as well as the cross-cutting security themes. An overview of relevant existing studies on security and eGovernment systems is also provided as well as an updated project plan. A list of interested Members of the European Parliament and expert stakeholders is enclosed as appendix 1.[1] A dissemination list of other relevant actors is enclosed as appendix 2.[2]

2. SCOPE OF 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 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). The World Economic Forum (2011) elaborates on future government architectures stressing the importance of open networked government highlighting the transformational potential of eGovernment, but also the sensitivities of cybersecurity. In the EU, the current eGovernment Action Plan 2011-2015[3] 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".

[1] The experts on the list have been found by recommendations from partners in the project and recommendations from experts that we have already established contact with. The list of interested MEPs has been gathered by choosing the relevant sub-committees in the European Parliament and selecting politicians from this. Furthermore, some of the politicians have been suggested by partners in the project since they have already had contact with these.

[2] The dissemination list has been compiled with the help of ENISA's Who-is-Who-Directory (2011) which contains information on stakeholders, authorities and organisations pertaining to network and information security. The list has been pruned to find organisations relevant to the project, and additional contact information has been gathered if none was provided. Furthermore the internet has been perused for national associations which cover the subjects of information, security and e-government. Likewise national and international organisations of science, information and technology writers and journalists have been added.

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

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.[4]

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 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 has consulted the latest eGovernment benchmarking reports including:

- the UN eGovernment Surveys (2012 forthcoming, 2010, 2008, 2005, 2004, 2003)[5]
- the coming EU 2011 – 2015 benchmarking framework[6] replacing the current i2010 benchmarking framework[7]

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

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

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

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

- and the latest EU eGovernment Benchmarking Report (2010)[8]

The project has also looked at worldwide examples of eGovernment initiatives among global eGovernment leaders such as the US, South Korea, Hong Kong, Australia and Singapore. Transatlantic and Southeast Asian experiences with safeguarding eGovernment systems will, if possible, be included in the Conference of phase 3.

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 has identified a set of interrelated security challenges facing the roll-out and operation of cross-border eGovernment systems. They include network security, interoperability, identification, usability, privacy, access control and function creep. These cross-cutting security challenges will be examined in the context of our three case studies, each exemplifying different aspects of the security issue at hand. Selecting the cases 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 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 deal with eGovernment systems which are applied throughout the majority of EU Member States. This allows us to compare different member states and / or 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 could 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.

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	Many incompatible	Differences	Many

[8] 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.

	security issues	systems	between EU Directive and national implementations. Risk of function creep	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[9] 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[10] made at the 5th Ministerial eGovernment Conference in 2009. The Action Plan supports and complements the Digital Agenda for Europe[11]- as one of seven flagship initiatives under the Europe 2020 Strategy[12]. 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-border eGovernment services may additionally challenge existing regulations at national and EU level. The project will 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 will include legal experts in our scheduled interviews. In the presentation of the project's case studies we will address 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.

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

[10] 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.

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

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

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)[13]. 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 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

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

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.

3. RESEACH DESIGN AND METHODS OF PHASE 2

Taking the strategic objectives of this project into consideration, the project consortium has 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.

In the following we provide a preliminary presentation of case studies, which will constitute the next phase of the project (phase 2).

4. PRELIMINARY PRESENTATION OF CASE STUDIES

4.1 Case I: eProcurement

According to Graux and Meyvis (2010), the value of public procurement spending in the EU is amounting to 17% of the GDP. Electronic public procurement is taking place in many EU member states. For high values beyond a certain threshold, it is mandatory to make part of the procurement process Europe-wide by publishing tenders in the EU's Official Journal. The main reasons for the continuing relevance of EU-wide procurement are lower costs because of increased competition among bidders, as well as because of anticipated savings by using electronic means, from tenders to bids, contracts and invoicing. Therefore, the EU requires EU-wide electronic procurement, in particular with Directive 2004/18/EC. Cross-border EU electronic procurement may lead to very complex procedures because of the variety of digital signature legislations and digital signature technologies (including choice of algorithms and protocols for verification, quality of the implementation of single components, quality of the signing environments, issues of storage and resigning). The choice of such legal and technical approaches leads to different costs, different prospects for usability, as well as to different risks for the liability of stakeholders including the individual users working with the stakeholders.

In eProcurement, the parties wish to identify themselves and wish to have authentic documents usable for later dispute clarification. There is a variety of digital signatures in use. While they typically comply with EU Directive 1999/93/EC, they differ in detail. Those details may make a difference if transaction records need to be proved at court (cf. Cimander 2009). The variety of signatures means that so far trans-border interoperability is largely non-existent (see the Commission-funded study by Graux and Meyvis 2010). In some countries, such as the UK and Ireland, rather only shared secrets are used for login into the procurement system. This would be less secure, Graux and Meyvis write, but no incidents have occurred, by 2010 (ibid., p. 31).

The variants of digital signatures come with significant costs for certification, smart cards, readers, etc. Furthermore, cross-border validation services may be necessary to check whether a signature complies with the legislation at the place it was made, and communicate the finding to the relying party, which may imply subsequent legal issues. Additional costs emerge from the need for resigning services. Independent bodies may need to resign records after some years if keys have become too short or if it turns out that algorithms have become insecure. Such costs, however, may lead to more assurance with regard to long run readability and with regard to reliability in court cases. We intend to identify the related experiences from the large scale PEPPOL pilot.

According to Graux and Meyvis (2010), 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. This means that the issue of records which cannot be denied at court is to be investigated in our study, and all alternatives should be put on the table. We will also explore whether the Internet can be made a safer place with no possibility for malware attacking digital signatures. This would reduce the need for secure hardware of any sort. Taking into account that no provably secure systems for digital signatures exist, it is anticipated that the whole variety of means of authentication is to become a topic of our research. It is anticipated that the players will decide on these depending on their risk perception and the costs for the respective improvements in security, i.e. risk reduction. We will also address migration paths towards more secure end-user devices as well as towards securing the Internet. It is anticipated that the above issues will be of relevance for some pending changes in EU-legislation, such as a new signature directive (Schwemmer 2011).

We also intend to address more general risks, such as those from Advanced Persistent Threats, addressing the proper working of eProcurement systems as a whole (Chien 2010, Dalton 2009). This may affect the confidentiality of data, e.g. prices of bids, confidential details of bids as in military procurement, etc., which is also threatened from inside procurement systems, e.g. if those systems are subcontracted.

4.2 Case II: The biometric passport

All European member states are obliged to implement the biometric passport, equipped with an RFID chip that stores the facial scan of the passport holder. This is defined in Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States. The objective is to combat passport fraud and have one internationally compatible identification system. Still, the way in which the biometric data is gathered, stored and used, differs among member states. Some member states only gather the facial scans, while others also use the fingerprint. Some member states opt for decentralised storage of the data, for reasons of privacy and data protection, others store the data centrally. Some states use the stored biometric data only for one-on-one verification to prevent fraud, while others want to use it to identify crime suspects and combat terrorism. This will lead to a broad variety of security issues, which differ among member states. Moreover, we discern a certain tension between the European directive and the national laws placed on top of it.

As an identification system, work is underway to reach one international compatible system. Still, it is difficult to implement the same level of data security among states concerning the scanning devices and protocols. Also, member states diverge in their implementation phases: some are already fully functional, while others are still at the beginning. Can the biometric passport be used in all member states in a similar way? Can the identification data be exchanged between member states? Moreover, member states appear to add functionality to the system. The biometric passport was originally designed to combat fraud. For example, the portrait picture is not only stored physically on the passport, but also electronically on an RFID chip. This will make it more difficult for someone to just replace the picture. Also, once the data is stored centrally, it should make it more difficult for one person to request different passports at different municipalities under a false name. 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. For example, looking for matches of fingerprints or video images from a crime scene and the central database.A fraud detection measure then evolves into a crime scene investigation tool, a function creep for which the system was not built for in the first place, leading to new security challenges. Which member states elaborated on the functionality of the system, and with what kinds of results?

Biometric data is considered to be sensitive, personal data. Some studies demonstrated the chip can be hacked and the communication with its reader can be eavesdropped and replicated. Data transfer between the RFID chip in the passport and reader is encrypted, but the key did not prove long enough, as Hoepman et al (2006) demonstrated. How well is this data protected on the chip of the passport? Once the data is also stored, either at the municipality, or nationally: how well can this data be protected against security treats such as hacking, data loss and data pollution? Also, European nations differ in terms of privacy concerns. Germany for example opted against central storage for reasons of data protection. Other countries aim at central storage, in order to be able to use the data for criminal investigation. The UK and the Netherlands both started with centralised storage, but later on decided to reverse or postpone this measure. What are the privacy concerns raised by privacy advocates, politicians and citizens?

Aside from the national differences in privacy policy, the European privacy policy framework is evolving too. For example the Directives 95/46/EC and 2002/58/EC, concerning European privacy guidelines is currently under revision, urging for example the owners of large data systems to perform privacy impact assessments. More in general, the whole notion of what actually are personal data is under revision too. This will also affect the use of biometrics for identification, as the European data protection officer Peter Hustinx suggests. (Hustinx 2011) How will the use of biometric data by nation states concur with changes European data protection legislation?

In sum, the case study of the biometric passport is of interest for this project because it demonstrates how an eGovernment-related European Directive can have different forms of national implementation. It also demonstrates the complexity of implementing identification techniques and possible privacy issues resulting from that.

4.3 Case III: eHealth records and transactions

European healthcare establishments are facing substantial challenges over the next decades forcing European policy makers to re-think how European healthcare is provided. Important challenges include demographic developments such as ageing, which are likely to increase the demand for healthcare services, and a rise in patients suffering from chronic diseases. Another emerging challenge is the growing competition within the healthcare market. This development may increase the mobility of both patients and health professionals. Dominant also are the growing expectations and empowerment of patients, trends which will affect the future healthcare sector in the sense that patients will ask for more personalised and high-quality services and will take over some traditional healthcare tasks themselves. Key applications in eHealth such as eHealth records systems and ePrescription services are expected to improve the healthcare system and increase tailoring care to individual consumers enabling patient safety and access to cross-border care. However, the provision of cross-border eHealth services faces operational, technical and legal challenges.[14]

A core strategic policy document for eHealth is the European eHealth Action Plan which contains a series of activities during the period 2005-2010, supported by the Commission services. Council Conclusions adopted on 1 December 2009 has called upon the European Commission to update the 2004 eHealth Action Plan. This has been followed up by the EC-facilitated "eHealth Governance Initiative", the overall objective of which is to collaborate on the design of future European eHealth strategy and infrastructure. The second eHealth Action Plan plan is envisioned for adoption by the end of 2011.[15] The Europe 2020 strategy flagships Digital Agenda for Europe and Innovation Union both incorporate an important role for eHealth: the Digital Agenda for Europe includes a number of targeted eHealth actions such as Key Action 13: “Work with Member States to equip 15% of Europeans with secure online access to their medical health data by 2015. By 2020 widespread deployment of telemedicine services”; or Key Action 14: “Adopt EU wide standards, interoperability testing and certification of eHealth systems by 2015; Agree on a minimum set of patient data to be accessed/exchanged across Member States by 2011.”

eHealth in Europe is mainly regulated by national laws of the Member State, e.g. with regard to the overall organisation of the healthcare sector (division of roles between the private and the public sector), the legal status of the healthcare profession or to the definition of patients’ rights. Recently, however, EU law has been adopted which clarifies access to healthcare in another EU country, as well as rules on reimbursement.This is the EU Directive on the application of patients’ rights in cross-border healthcare - defined as healthcare provided or prescribed in a member state other than that of affiliation (Legido-Quigley et al. 2011).[16]. Of particular interest is the setting-up and level of ambition of the network of national authorities responsible for eHealth made mandatory in the Directive (Article 14) which will consider issues related to the transferability of electronic patients’ records in cases of cross-border healthcare. Also particularly relevant for the domain of eHealth is of course the European regulatory framework for personal data protection[17] and

[14] From an operational point of view it is evident from previous studies on eHealth systems that sustainability and added value are only achieved when eHealth systems explicitly address socio-technological and organisational concerns and the interests of their potential adopters (e.g. patients, phycisians, the pharmaceutical industry, hospital administrators and primary care providers) - see for example, Vitacca M, Mazzù M, Scalvini S. (2009). Socio-technical and organizational challenges to wider e-Health implementation. ChronRespir Dis. 6(2):91-7. In the “Legally eHealth” study Doosselaere et al. (2008) focuses on three legal clusters – data protection and privacy; product liability andconsumer protection; competition and trade law.

[15] For further details, see http://ec.europa.eu/information_society/activities/health/ehealth_ap_consultation/index_en.htm.

[16] Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients’ rights in cross-border healthcare, available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:088:0045:0065:EN:PDF

[17] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data: http://ec.europa.eu/justice_home/fsj/privacy/law/index_en.htm.

for the protection of privacy in electronic communications.[18]According to the "Legally eHealth" study (Dooselaere et al. 2008), equally important EU-level legislation applies to the eHealth sector through product and service liability and consumer protection; and trade and competition aspects of eHealth.

The case study will examine existing national and EU eHealth records initiatives enabling cross-border patient mobility. On an EU level, the epSOS Large Scale Pilot (Smart Open Services for European Patients) involves 23 Member States, other European countries and an industry team of more than 30 companies to test secure and interoperable Patient Summaries and ePrescription services across borders allowing patients the opportunity to use cross-border eHealth services when seeking healthcare in participating epSOS pilot countries. The epSOS project develops national and cross-European eHealth infrastructural elements such as authentication of patients and health professionals, semantic interoperability and security measures which will interconnect regional and national solutions to enable cross-border access to patient data. These may contain emergency data or prescription information.

Establishing cross-border eHealth services such as Patient Summaries and ePrescription services will face the obvious challenges of diversity in languages, local classification systems and record holding as well as security and privacy of healthcare data. For instance, vital information should be freely available in an emergency, but personal data – whether accumulated or current – must be absolutely "locked down" against unauthorized or inappropriate access. Also, identification and authentication are crucial elements of networked eHealth systems to verify the identity of patients and health professionals. Patients have different rights to confidentiality and privacy in the different EU member states. Some patients are the owners of their own data – in other countries it is their clinicians or general practitioners who have this right. If electronic information is easy to share and update, it can also be easy to acquire. What is the burden of responsibility of each actor and each link in the European health service chain? What are the security requirements of the re-use of individual patient health data - a crucial concern for the advancement of public health and clinical research? What are the modes of operation for accessing person related health data on a regional, national and multinational level in a European context? What are the requirements for citizens and how safe are eHealth services such as 'Patient Summaries' in terms of integrity, data protection and privacy?

5. UPDATED PROJECT PLAN

The following project plan describes the procedure and time plan for the remaining three phases of the project. This project plan specifies the work mode and methodology of phases 2-4 and presents the necessary changes of the time plan of these phases.

5.1 Changes in the time plan

The necessity of changing the time plan should be seen in the light of the problems related to the approval of Intermediary Report 1 and the delay of signing the contract for phase 2 of the project. In the original project plan it was foreseen that the work of planning the

[18]Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

conference in phase 3 could begin during phase 2. Since this is no longer possible phase 3 will be prolonged. The changes in the time plan are as follows:

Phase 2:
Duration: 6 months from the signing of contract of phase 2

Phase 3:
Duration: 6 months from the signing of contract of phase 3

Phase 4:
Duration: 2 months from the signing of contract of phase 4

5.2 Phase 2: Knowledge building

Phase 2 will be aimed at building knowledge on the selected security challenges of e-Government systems by analysing the three cases of eProcurement, the biometric passport and eHealth records. The focus of the phase 2 studies is further described above in the elaborated scoping description.

The three case studies will be performed by desk studies using existing literature and studies on the subject as well as interviews with relevant experts and practitioners with knowledge of the specific cases. The methodology of phase 2 is further described above in section 3.

The results of phase 2 will be:

- Intermediate report 2: A report (70-100 pages) about (1) the outcome of our research and interviews and (2) a description of the scope of the conference in phase 3

5.3 Phase 3: Expert/stakeholder debate on the perspectives of EU eGovernment systems

In the third phase of the project a conference about security challenges for eGovernment systems and possible policy options is planned and carried out. The conference will debate the central security and feasibility issues of EU eGovernment systems and the perspectives for establishing EU eGovernment services. The conference will build on presentations from experts and stakeholders, and debate with MEPs about policy options related to EU eGovernment systems.

Conference scope
The conference will be structured around 4-5 issues. These issues could be e.g. 'most relevant security threats', 'most relevant means to improve security', 'EU e-signature', 'future secure eGovernment systems at EU-level'. These are indicative examples, as the precise scope and issues of the conference will be decided on the basis of the well-authenticated conference scope description delivered at the end of phase 2.

The work in this phase will include identifying and inviting relevant speakers, planning the conference and carrying out the conference. All speakers will be asked to make a paper (approximate 3-5 pages) as background to their presentation at the conference. These papers will be given to the participating MEPs one week before the conference, in order to optimise their benefit and the overall quality of the conference debates.

The day after the conference the expert group (if necessary supplemented with a few experts/stakeholders from the conference) will discuss the outcome of the conference and give suggestions for future policy options in relation to establishing secure EU eGovernment services. This will be input for phase 4 of the project.

The results of phase 3 will be:

- A conference with a debate involving experts/stakeholders/MEPs
- Intermediate report 3: A conference report (30-50 pages) consisting of speakers' papers and the main conclusions from the debate
- A Policy Brief: Summary of expert workshop (5-10 pages) as input for the policy option assessment in phase 4

5.4 Phase 4: Policy options assessment and project conclusions

In the last phase of the project the results of all previous phases will be compiled and evaluated and on the basis of that, policy options related to security of future EU eGovernment services will be assessed. The policy option assessment will be done by the project consortium based on the results of case studies, the conference and the workshop and supplemented with Internet-based support from the expert group. The policy option assessment will include consideration of the following questions:

- What are the most relevant security threats hanging over eGovernment and what are the possible measures to counter them?
- What are the security related barriers of a European Interoperability Framework for eGovernment services?
- Can the removal of security-related barriers to cross-border e-procurement services enhance the EU Single Market?
- What are the policy options and the main security issues to be tackled for a mutual recognition and interoperability of e-Signature and its alternatives?
- What EP initiatives could be envisaged for fostering eGovernment capacity building through more secure services?

The policy option assessment will furthermore include options identified during phase 2 and 3 of the project. Options are anticipated to provide input to update of directives, e.g. any updates of the Procurement and Signature Directives or to relevant privacy guidelines and directives. Other options may concern initiatives for, e.g. fighting malware and denial of service attacks, such as EP-supported moves towards suitable computer certifications, towards auditing requirements used in the procurement of IT-systems, towards network improvements or towards ways to address the "commons" nature of measures to improve security.

The policy option assessment will be based on Intermediate report 2 and 3 as well as the Policy Brief and other relevant input from the conference and the expert workshop connected to the conference. The assessment will result in a number of policy options of relevance for the European Parliament.

The results of the last phase will be:

- A final report (70-100 pages) that sums up the results of the project and gives conclusions about the security issues related to eGovernment systems, possible solutions, and policy options

6. REFERENCES INCLUDING OTHER RELEVANT STUDIES ON SECURITY AND EGOVERNMENT

The following section contains references as well as relevant studies on security and eGovernment. These studies will be included in the knowledge building phase. The list is not exhaustive and supplementing studies will be included.

6.1 General studies – Security of eGovernment

- Belanger, F., and Hiller, J.S., (2006) "A Framework for E-Government: Privacy Implications," Business Process Management Journal (12:1), pp. 48–60
- 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.
- Doosselaere, C., Herveg, J., Silber, D., and Wilson, P. (2008). Legally eHealth - Putting eHealth in its European Legal Context, study report on behalf of DG Information Society and Media, European Commission, available at: http://www.epractice.eu/files/media/media1971.pdf
- 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, Data Breach Notifications: http://www.enisa.europa.eu/act/it/dbn/
- ENISA, Security and Resilience in Governmental Clouds: http://www.enisa.europa.eu/act/rm/emerging-and-future-risk/deliverables/security-and-resilience-in-governmental-clouds
- European Commission, Study on user satisfaction and impact in EU27: http://www.epractice.eu/files/media/media2599.pdf
- European Commission (2010).Digitizing Public Services in Europe: Putting ambition into action - 9th Benchmark Measurement: http://ec.europa.eu/information_society/newsroom/cf/item-detail-dae.cfm?item_id=6537
- Grawrock, D.: The Intel Safer Computing Initiative. Intel Press, 2006.
- 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.
- House of Lords, Protecting Europe against large-scale cyber-attacks: http://www.publications.parliament.uk/pa/ld200910/ldselect/ldeucom/68/68.pdf
- 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.
- Layne, K. and Lee, J. (2001). Developing fully functional e-government: A four stage model , Government Information Quarterly 18 (2), 122-136
- Lenk, K. andTraunmüller, R: (2000). A framework for electronic government, Proceedings of DEXA 2000, 340-345.
- Mitrakas, A., Hengeveld, P., Polemi, J. and Gamper, J. (2007). Secure E-Government web services. Hershey PA: Idea Group Inc.

- OASIS (2010). eGov Pitfalls Guidance, available at http://www.oasis-egov.org/sites/oasis-egov.org/files/eGov_Pitfalls_Guidance%20Doc_v1.pdf.
- OECD, Denmark: Efficient e-Government for Smarter Public Service Delivery: http://www.oecd-ilibrary.org/governance/denmark-efficient-e-government-for-smarter-public-service-delivery_9789264087118-en;jsessionid=aps85ge2vqua.delta
- OECD (2009). Rethinking e-Government Services - User-Centred Approaches: http://www.keepeek.com/Digital-Asset-Management/oecd/governance/rethinking-e-government-services_9789264059412-en
- UN,2010 Global E-Government Survey: http://www2.unpan.org/egovkb/global_reports/10report.htm
- M. Friedewald, D. Wright, S. Gutwirth, P. D. Hert et al., Privacy and Trust in the Ubiquitous Information Society: http://isi.fraunhofer.de/isi-de/publ/download/isi09b52/Privacy-and-Trust-Ubiquitous-Information-Society.pdf?pathAlias=/publ/downloads/isi09b52/Privacy-and-Trust-Ubiquitous-Information-Society.pdf. Karlsruhe, 2009
- Dunleavy, P., Margetts, H., Bastow, S. and Tinkler, J. (2006) Digital-era Governance: IT Corporations, the State and e-Government. Oxford University Press.
- France Belanger, Janine S. Hiller, (2005) "A framework for e-government: privacy implications", Business Process Management Journal, Vol. 12 Iss: 1, pp.48 – 60
- Choudrie, J.; Raza, S.; and Olla, P., "Exploring the Issues of Security, Privacy and Trust in eGovernment: UK Citizens' Perspective" (2009). AMCIS 2009 Proceedings. Paper 347. http://aisel.aisnet.org/amcis2009/347
- Silcock, R. (2001). What is eGovernment? Parliamentary Affairs, Vol.54, pp.88-101.
- 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.
- Yin, R. K. (2002). *Case Study Research, Design and Methods*, 3rd ed. Newbury Park, Sage Publications.

6.2 Studies specifically for eProcurement

- Chaum, David, Hans van Antwerpen: *UndeniableSignatures*; Crypto'89, LNCS 435, Springer-Verlag, Berlin 1990, 212-216.
- Chien, Erik (2010): W32.Stuxnet dossier. http://www.symantec.com/connect/blogs/w32stuxnet-dossier
- Cimander, Ralf; Hansen, Meik; Kubicek, Herbert: Electronic Signatures as Obstacles for Cross-Border eProcurement in Europe – Lessons from the PROCURE project. 2009. http://www.epractice.eu/en/library/292080.
- Dalton, Chris: A hypervisor against ferrying away data. Interview by Franco Furger and Arnd Weber. In: OpenTC Newsletter April 2009, http://www.opentc.net/publications/OpenTC_Newsletter_07.pdf.
- Graux, Hans; Meyvis, Eric: 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.
- KPMG: ÖffentlichesBeschaffungswesen. Gutachtenfür den Deutschen Bundestag. Berlin 2002.

- Lapp, Thomas; Reimer, Helmut: Signaturen und kein Ende? Datenschutz und Datensicherheit 11, 2009, 647.
- PEPPOL, eSignature deliverables: http://www.peppol.eu/results/esignature-deliverables
- PEPPOL, eOrderingdeliverables: http://www.peppol.eu/results/eordering
- PEPPOL, eInvoicing deliverables: http://www.peppol.eu/results/einvoicing
- PEPPOL, eCatalogue deliverables: http://www.peppol.eu/results/ecatalogue
- PEPPOL, Virtual Company Dossier deliverables: http://www.peppol.eu/results/virtual-company-dossier
- Quiring-Kock, Gisela: PKI für Bürger – transparent, sicher, datenschutzgerecht? In: Datenschutz und Datensicherheit, 7/2009, 396-398. http://www.springerlink.com/content/d16g77507t677118/fulltext.pdf.
- 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.
- Schwemmer, Jürgen: Bundesnetzagentur. Presentation given at CAST-Forum „Public Key Infrastructures", Darmstadt, Jan. 27, 2011.
- STORK,Electronic Signatures as Obstacle for Cross-Border E-Procurement in Europe: https://www.eid-stork.eu/dmdocuments/public/ElectronicSignaturesAsObstaclesForCross-BorderEProcurementInEurope_LessonsFromThePROCUREProject.pdf

6.3 Studies specifically for biometric passports

- ENISA,Privacy Features of European eID Card Specifications: http://www.enisa.europa.eu/act/it/eid/eid-cards-en
- ENISA, Security Issues in Cross-border Electronic Authentication: http://www.enisa.europa.eu/act/it/eid/xborderauth
- ENISA, Mapping security services to authentication levels: http://www.enisa.europa.eu/act/it/library/deliverables/map-auth-lev
- ENISA, Privacy and Security Risks when Authenticating on the Internet with European eID Cards: http://www.enisa.europa.eu/act/it/eid/eid-online-banking
- Hof, C. van't, R. VvanEst and F. Daemen (2011) "Check in / check out. The Public space as an Internet of Things" Rotterdam: NAi Publishers
- Hoepman, J. H., EngelbertHubbers, Bart Jacobs, MartijnOostdijk,Ronny WichersSchreur (2006) "Crossing Borders: Security and Privacy Issues of the European e-Passport" Nijmegen: Institute for Computing and Information Sciences Radboud University Nijmegen
- Munnichs, G. , M. Schuijf and M. Besters (2010) "Databases. Over ICT-beloftes, informatiehonger en digitale autonomie." The Hague: Rathenau Institute
- Hof, C. van 't (2008) "RFID and Identity Management in Everyday Life" Brussels: STOA
- Hustinx, P. (2011) Biometrics in a revised EU Data Protection Framework. Presentation on the 7th EBF Seminar Biometrics and Privacy, Brussels, 15 June 2011

- Böhre, V. (2010) "Happy Landings? Het biometrischpaspoortalszwartedoos" The Hague: WRR
- Snijder, M. (2011) "Het biometrisch paspoort in Nederland: crash of zachte landing" the Hague: WRR
- 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

6.4 Studies specifically for eHealth Records

- Calliope, EU eHealth Interoperability Roadmap: http://www.calliope-network.eu/Consultation/tabid/439/Default.aspx
- Commission of the European Community (2003). E-health - making healthcare better for European citizens: An action plan for a European E-health Area; Commission of the European Community; Brussels, 2003.
- epSOS Large Scale Pilot project website http://www.epsos.eu/home/
- Ruotsalainen P, Pohjonen, H. (2003). European security framework for healthcare. Stud Health Technol Inform. 2003;96:128-34.
- Blobel, B. and Roger-France, F. H. (2001). A systematic approach for analysis and design of secure health information systems. Int J Med Inform. 62 (2001) 51–78.
- Roger-France, F. H. (2011).eHealth in Belgium, a new "secure" federal network: role of patients, health professions and social security services. Int J Med Inform. 80 (2):12-6.
- Legido-Quigley, H. et al. (2011). Cross-border healthcare in the European Union: clarifying patients' rights. BMJ 2011; 342.

Appendix 1

Name	Nationality	Title	Field of Interest	Contact information
Experts				
Armgard von Reden	DE	Government Programs Executive at IBM	Political and data protection issues	?
Caspar Bowden	UK	Chief Privacy Advisor for Microsoft	Data protection policy, privacy enhancing technology research, identity management and authenticatio	casparb@microsoft.com
Chris Dalton	UK	Principal Research Scientist at HP Labs Bristol	Pragmatic approaches to getting strong security properties into Internet systems and services	chris.i.dalton@hp.com
Christian Wernberg-Tougaard	DK	Member of ENISA Permanent Stakeholders Group	Innovation and transformation using ICT	christian@wernberg.org
Claire Vishik	US	Trust & Security Technology & Policy Manager at Intel Corporation (member of the permanent stakeholders group of ENISA)	Hardware security, trusted computing, privacy enhancing technologies, some aspects of encryption and related policy issues.	claire.vishik@intel.com
Dr Stefan Fafinsk	UK	Research Fellow within the School of Law at the University of Leeds	Computer misuse, cybercrime and Internet law. Mapping and measuring cybercrime, the criminogenic potential of Internet technologies, their social impact and policy	s.f.fafinski@leeds.ac.uk
Dr. Ian Brown	UK	Senior Research Fellow at Oxford Internet Institute	Public policy issues around information and the Internet, particularly privacy, copyright and e-democracy. He also works in the more technical fields of information security, networking and healthcare informatics.	i.brown@cs.ucl.ac.uk
Dr. Thilo Weichert	DE	Privacy Commissioner of Schleswig-Holstein		
Eelco Stofbergen	NL	Manager GOVCERT.NL	Information Security, Cyber crime, Cyber security, Cyber warfare, Incident Response, IT Auditing, IT Governance	eelco.stofbergen@govcert.nl
Elisabeth De Leeuw	NL	Self Employed at IdTopIQ	Information security - identity assurance - IT and society	http://nl.linkedin.com/in/elisabethdeleeuw
Frans Kolkman	NL	Manager Operations at Dutch National Cybercrime Program	Cybercrime and detective work	http://www.linkedin.com/in/franskolkman
Gwendal Le Grand	FR	Head of IT experts group at CNIL	Security and Investigations	Via linkedin
Gwendolyn Carpenter	UK	Independent Strategy Consultant	Citizen-centric aspects of eGovernment projects, with an emphasis on practical solutions and actual country experience.	Via linkedin
Helmut Leopold	AT	Director at AIT Austrian Institute of Technology		
Ivan Damgård	DK	Co-founder of Cryptomathic		
Jakob Willer (Afløste Ib Tolstrup)	DK	Director of The Telecommunications Industry Association in Denmark		jw@teleindu.dk
Jean-Marc Suchier	FR	Director, European Programmes, Sagem Sécurité	Biometrics	jean-marc.suchier@sagem.com
Jelle Attema	NL	Advisor at ECP-EPN	Interoperability	jelle.attema@ecp-epn.nl
Jeremy Millard	DK	Senior Consultant at the Danish Technological Institutue	Leading an impact assessment of the European eGovernment 2010 Action Plan, the eGovernment 2020 Vision Study on Future Directions of Public Service development for the European Commission. Delivery, as well as pan-European studies on eParticipation and on ICT in regional	jrm@teknologisk.dk
Johannes Landvogt	DE	IT-Beauftragter für den Datenschutz und die Informationsfreiheit beim BfDI		ref6@bfdi.bund.de
John Borking	NL	Researcher e-law at University of Leiden		j.j.f.m.borking@law.leidenuniv.nl
Jon Ølnes	NO	Senior Advisor at Difi - Agency for Public Management and eGovernment	nfrastructural aspects of security and trust, and in particular, e-ID and e-signature	jon.olnes@difi.no
Julia Ferger	DE	European Commission, Internal Market and Services Directorate-General		
Juliet Lodge	UK	Professor at Jean Monnet Centre of Excellence, University of Leeds	Ethics and information and communication technologies; EU accountability and transparency; ethical egovernance, eborder management,biometrics, cross-border ecooperation for policing, justice and commerce; EU institutions and politics	j.e.lodge@leeds.ac.uk
Jaap Kuipers	NL	Founder at Platform Identity Management Nederland	Identity management, OpenID, CardSpace,DigiD, SAML, A-Select, Trust Federations,	http://nl.linkedin.com/in/jaapkuipers
Kasper Skov-Mikkelsen	DK	Director of The Danish Trade Organisation for Safety and Security		ksm@sikkerhedsbranchen.dk
Kees C. Donker	NL	Innovation & Technology Exec IBM Benelux		http://nl.linkedin.com/pub/kees-c-donker/1/34a/69b
Kurt Einzinger	AT	Member of the Austrian Data Protection Agency, Member of ENISA Permanent Stakeholders Group		?
Lee Andrew Bygrave	AUS (NO)	Department of Private Law, University of Oslo	Internet Governance: Infrastructure and Institutions	lee.bygrave@jus.uio.no

Appendix 1

Name	Nationality	Title	Field of Interest	Contact information
Lena Andersen	DK	Head of Office at the Danish Data Protection Agency		la@datatilsynet.dk
Luis Vidigal	PO	Member of the Directorate of APDSI (Associação para a Promoção e Desenvolvimento da Sociedade da informação), Portugal		
Magnar Aukrust	NO	Deputy Director General at Ministry of Justice and the Police	Biometrics	magnar.aukrust@jd.dep.no
Mario Savastano	IT	Institute of Bio-structures and Bio-imaging, University of Naples "Federico II"		mario.savastano@unina.it
Marnix Dekker	NL	Application Security Officer at European Network and Information Security Agency (ENISA)	Information Security, Identity Management, IT architecture and design, Service-oriented architectures, Quality Assurance, IT process and system design, design and analysis of network and security protocols.	dekker.marnix@gmail.com
Meryem Marzouki	FR	Senior researcher at the French National Scientific Research Center	Internet governance and the transformation of the rule of law, privacy and personal data protection issues	Meryem.Marzouki@lip6.fr
Michael Dickopf	DE	Head of Department, Beschaffungsamt des Bundesministeriums des Innern		
Michael Hange	DE	CEO of Bundesamt für Sicherheit in der Informationstechnik, Germany		
Michael Waidner	DE	Director at Fraunhofer SIT	Security in Information Technology	michael.waidner@sit.fraunhofer.de
Mogens Ritsholm	DK			
Morten Juul Nielsen	DK	Chief of Security at Microsoft in Denmark	IT-security	mortenjn@microsoft.com
Morten Klitgaard Friis	DK	Cand. scient. IT Risk Management, KPMG	IT Risk Management	mkfriis@kpmg.dk
Maarten Hillenaar	NL	CIO Dutch Ministry of Internal Affairs		http://nl.linkedin.com/pub/maarten-hillenaar/0/462/6b1
Peter Hustinx	NL	European Data Protection Supervisor	Development of data protection legislation from the start, both at the national and at the international level	
Peter Landrock	DK	President of Cryptomathic		landrock@cryptomathic.com
Prof. Dr. Christoph Busch	DE	Fraunhofer-Institut für Graphische Datenverarbeitung IGD		christoph.busch@igd.fraunhofer.de
Ralph Bendrath	DE	Data protection on the internet	Internet privacy	bendrath@zedat.fu-berlin.de
Ross Anderson	UK	Professor of Security Engineering at Cambridge University	Reliability of security systems, security of clinical databases, privacy and freedom issues.	Ross.Anderson@cl.cam.ac.uk
Rüdiger Grimm	DE	Professor for IT-risk management, University of Koblenz-Landau, Germany	Application challenges of IT security, e.g. User Rights Management, E-Voting, E-Identification, E-Commerce, IT-Forensics	grimm@uni-koblenz.de
Rüdiger Grimm	DE	Professor for IT Risk Management at the University in Koblenz	IT security, e.g. User Rights Management, E-Voting, E-Identification, E-Commerce, IT-Forensics	grimm@uni-koblenz.de
Simone Fischer-Hübner	DE	Professor in Computer Science at Karlstad University		simone.fischer-huebner@kau.se
Stephan Engberg	DK	Founder of Priway	User-centric Identity management, Trust & Security	stephan.engberg@priway.com
Stephan Klein	DE	CEO of Bremen Online Services, Germany (Peppol)	Card-based payment systems	sk@bos-bremen.de
Søren Duus Østergaard	DK			
Thomas Beergrehn	SWE	CEO of EU-supply	Strategy and improvements of time to market in hi-tech industries, including large change management programs at telecom vendors, full service operators, IT services and Internet software companies.	thomas.beergrehn@eu-supply.com.
Tim Stevens	UK	Associate Fellow of the International Centre for the Study of Radicalisation & Political Violence (ICSR)	Information Technologies; Cyberspace and Strategy; Information Warfare and Propaganda	timothy.stevens@kcl.ac.uk
Vincent Böhre	NL	Director of Operations at Stichting Privacy First	International law, human rights, privacy issues, data protection, biometrics	
Yih-Jeou Wang	DK	Chief Adviser at Danish National IT and Telecom Agency, Head of Unit OECD E-Government Project	Policy and strategy development of Information Society and e-government	yjw@itst.dk or yih-jeou.wang@oecd.org

Politicians

Name	Nationality	Committee	E-mail
Herbet Reul	DE	Chairman of the Committee on Industry, Research and Energy	herbert.reul@europarl.europa.eu
Patrizia Toia	IT	Vice-chairman of the Committee on Industry, Research and Energy	patrizia.toia@europarl.europa.eu

Appendix 1

Name	Nationality	Title	Field of Interest	Contact information
Jens Rohde	DK	Vice-chairman of the Committee on Industry, Research and Energy		jens.rohde@europarl.europa.eu
Anni Podimata	GR	Vice-chairman of the Committee on Industry, Research and Energy		anni.podimata@europarl.europa.eu
Evžen TOŠENOVSKÝ	CZ	Vice-chairman of the Committee on Industry, Research and Energy		evzen.tosenovsky@europarl.europa.eu
Jo LEINEN	DE	Chairman of the Committee on the Environment, Public Health and Food Safety		jo.leinen@europarl.europa.eu
Corinne LEPAGE	FR	Vice-chairman of the Committee on the Environment, Public Health and Food Safety		corinne.lepage@europarl.europa.eu
Carl SCHLYTER	SE	Vice-chairman of the Committee on the Environment, Public Health and Food Safety		carl.schlyter@europarl.europa.eu
Bogusław SONIK	PL	Vice-chairman of the Committee on the Environment, Public Health and Food Safety		boguslaw.sonik@europarl.europa.eu
Dan JØRGENSEN	DK	Vice-chairman of the Committee on the Environment, Public Health and Food Safety		dan.jorgensen@europarl.europa.eu
Malcolm HARBOUR	UK	Chairman of the Committee on the Internal Market and Consumer Protection		malcolm.harbour@europarl.europa.eu
Eija-Riitta KORHOLA	FI	Vice-chairman of the Committee on the Internal Market and Consumer Protection		eija-riitta.korhola@europarl.europa.eu
Bernadette VERGNAUD	FR	Vice-chairman of the Committee on the Internal Market and Consumer Protection		bernadette.vergnaud@europarl.europa.eu
Lara COMI	IT	Vice-chairman of the Committee on the Internal Market and Consumer Protection		lara.comi@europarl.europa.eu
Louis GRECH	MT	Vice-chairman of the Committee on the Internal Market and Consumer Protection		louis.grech@europarl.europa.eu
Emilie TURUNEN	DK	Member of the Committee on the Internal Market and Consumer Protection		emilie.turunen@europarl.europa.eu
Heide RÜHLE	DE	Member of the Committee on the Internal Market and Consumer Protection		heide.ruehle@europarl.europa.eu
Juan Fernando LÓPEZ AGUILAR	ES	Chairman of the Committee on Civil Liberties, Justice and Home Affairs		juanfernando.lopezaguilar@europarl.europa.eu
Kinga GÁL	HU	Vice-chairman of the Committee on Civil Liberties, Justice and Home Affairs		kinga.gal@europarl.europa.eu
Sophia in 't VELD	NL	Vice-chairman of the Committee on Civil Liberties, Justice and Home Affairs		sophie.intveld@europarl.europa.eu
Salvatore IACOLINO	IT	Vice-chairman of the Committee on Civil Liberties, Justice and Home Affairs		salvatore.iacolino@europarl.europa.eu
Kinga GÖNCZ	HU	Vice-chairman of the Committee on Civil Liberties, Justice and Home Affairs		kinga.goencz@europarl.europa.eu

Appendix 2

Name	Website	E-mail	Country
Austria			
National authorities in network and information security			
Federal ICT Strategy		ikt@bka.gv.at	
Austrian Data Protection Commission		dsk@dsk.gv.at	
Informationssicherheitskommission		ISK@bka.gv.at	
BVT - (Federal Ministry of the Interior, Federal Agency for State Protection and Counter Terrorism) - Personal Protection and Physical Security		BMI-II-BVT-3@bmi.gv.at	
Federal Chancellery, Dep.Media Affairs/ Information Society		v4post@bka.gv.at	
TKK (Telekom-Control-Kommission Rundfunk & Telekom Regulierungs-GmbH)	signatur@signatur.rtr.at	rtr@rtr.at	
A-SIT		office@a-sit.at	
Computer Emergency Response Teams (CERTs)			
ACOnet-CERT		cert@aco.net	
CERT.AT		cert@cert.at	
GovCERT		post@govcert.gv.at	
Industry organisations active in network and information security			
Sicher-im-Netz.at		austria@microsoft.com	
Academic organisations active in network and information security			
Graz University of Technology		info@tugraz.at	
University Klagenfurt		uni@uni-klu.ac.at	
University Linz		webmaster@jku.at	
Upper Austria University of Applied Sciences		sib@fh-hagenberg.at	
Other bodies and organisations active in network and information security			
IISA (Initiative Information Security Austria)		office@iisa.at	
Belgium			
National authorities in network and information security			
Federal Public Service for Home Affairs		info@ibz.fgov.be	
Federal Public Service for Telecommunications and Information Society		e9-info@economie.fgov.be	
Federal Public for Service Consumer Protection		info@ibz.fgov.be	
Federal Public for Service Information and Communication Technology (FedICT)		info@fedict.belgium.be	
Federal Public Service Directorate-General Enforcement and Mediation		eco.inspec@economie.fgov.be	
BIPT (Belgian Institute for Postal Services and Telecommunications)		info@bipt.be	
Federal Computer Crime Unit		info@ibz.fgov.be	
Privacy Protection Commission		commission@privacycommission.be	
Computer Emergency Response Team (CERT)			
BELNET CERT		cert@belnet.be	
Industry organisations active in network and information security			
Agoria		info@agoria.be	
ISSA Belgium		president@issa-be.org	
LSEC		info@lesc.be	
Other bodies and organisations active in network and information security			
Belcliv–Clusib (Belgian Club for Internet Security)		Clusib@vbo-feb.be	
Internet Rights Observatory		secretariat@Internet-observatory.be	
Safer Internet Belgium		infonl@saferInternet.be	
Bulgaria			
National authorities in network and information security			
Communications Regulation Commission		info@crc.bg	
Ministry of the Interior (Cyber crime)		chief@cybercrime.bg	
Ministry of Defence		presscntr@mod.bg	
State Commission on Information Security		dksi@government.bg	

Appendix 2

Name	Website	E-mail	Country
National Laboratory of Computer Virology		office@nlcv.bas.bg	
Computer Emergency Response Team (CERT)			
CERT Bulgaria		cert@govcert.bg	
Industry organisations active in network and information security			
Association of Bulgarian Telecommunication Companies		office@astel.bg	
BAIT (Bulgarian Association of Information Technologies)		bait@bait.bg	
Cyprus			
National authorities in network and information security			
Office of the Commissioner of Electronic Communications and Postal Regulation		info@ocecpr.ogr.cy	
Ministry of Communications and Works		permsec@mcw.gov.cy	
Ministry of Interior - Civil Registry and Migration Department		pnathanael@crmd.moi.gov.cy	
Office of the Commissioner for Personal Data Protection		commissio-ner@dataprotection.gov.cy	
Computer Emergency Response Team (CERT)			
Computer Centre University of Cyprus		csirt@ucy.ac.cy	
Industry organisations active in network and information security			
CCS (Cyprus Computer Society)		ccs@spidernet.com.cy	
Diogenes		info@diogenes.com.cy	
Academic organisations active in network and information security			
University of Cyprus Department of Computer Science		manak@cs.ucy.ac.cy	
University of Cyprus Information Security Office		security@ucy.ac.cy	
CyNet (Cyprus Research and Academic Network)		secretariat@cynet.ac.cy	
Service of Systems of Information and Technology - Cyprus University of Technology		administration@cut.ac.cy	
Other bodies and organisations active in network and information security			
Cyprus Consumers' Association		cyconsas@spidernet.com.cy	
CyberEthics		info@cyberethics.info	
Safeweb		info.safeweb@cs.ucy.ac.cy	
Czech Republic			
National authorities in network and information security			
National Security Office		nbu@nbu.cz	
Ministry of Interior		public@mvcr.cz	
Czech Telecommunication Office		posta@mpo.cz	
Office for Personal Data Protection		info@uoou.cz	
Computer Emergency Response Teams (CERTs)			
CESNET-CERTS		steering@cesnet.cz	
CSIRT.CZ		abuse@csirt.cz	
CZNIC-CSIRT		csirt@nic.cz	
Other bodies and organisations active in network and information security			
SOS (Consumers Defence Association of the Czech Republic)		sos@consumers.cz	
Denmark			
National authorities in network and information security			
National IT and Telecom Agency - Ministry of Science, Technology and Innovation		itst@itst.dk	
IT Security Panel		vtu@vtu.dk	
Danish Security Intelligence Service		rpch@politi.dk	
Computer Emergency Response Teams (CERTs)			
CSIRT.DK		csirt@csirt.dk	
DK-CERT		cert@cert.dk	
GOVCERT.DK		contact@govcert.dk	
KMD IAC		alarmcenter@kmd.dk	
Industry organisations active in network and information security			
DI ITEK		itek@di.dk	

Appendix 2

Name	Website	E-mail	Country
Other bodies and organisations active in network and information security			
Uni-C		uni-c@uni-c.dk	
The Danish Data Protection Agency		dt@datatilsynet.dk	
FR (Forbrugerrådet)		bf@fbr.dk	
ANDK		info@medieraadet.dk	
Estonia			
National authorities in network and information security			
Ministry of Economic Affairs and Communications		info@mkm.ee	
Estonian Technical Surveillance Authority		info@tja.ee	
Estonian Informatics Centre		cert@cert.ee	
Estonian Data Protection Inspectorate		info@dp.gov.ee	
Estonian Educational and Research Network		eenet@eenet.ee	
IT Crimes Office, Central Criminal Police		keskkriminaalpolit-sei@kkp.pol.ee	
Computer Emergency Response Teams (CERTs)			
CERT EE		cert@cert.ee	
SKY-CERT		roductsecurity@skype.net	
Industry organisations active in network and information security			
ITL (Estonian Association of Information Technology and Telecommunications)		info@itl.ee	
EITS (Estonian Information Technology Society)		eits@eits.ee	
Other bodies and organisations active in network and information security			
AS Sertifitseerimis-keskus		info@sk.ee	
Cybernetica Ltd		info@cyber.ee	
Look at World Foundation		info@vaatamaailma.ee	
ETL (Estonian Consumers Union)		tarbliit@uninet.ee	
Finland			
National authorities in network and information security			
Ministry of Transport and Communications Finland		infosec@mintc.fi	
Information Security Group of the Ubiquitous Information Society Advisory Board		infosec@mintc.fi	
Ficora (Finnish Communications Regulatory Authority)		info@ficora.fi	
Ministry of Finance		valtiovarainministerio@vm.fi	
VAHTI (Government Information Security Management Board)		vahtijulkaisut@vm.fi	
Ministry of the Interior		sm.kirjaamo@intermin.fi	
Data Protection Ombudsman		tietosuoja@om.fi	
Computer Emergency Response Teams (CERTs)			
CERT-FI		cert@ficora.fi	
Ericsson PSIRT		psirt@ericsson.com	
Funet CERT		cert@cert.funet.fi	
NOKIA NIRT		cert@nokia.com	
Industry organisations active in network and information security			
FiCom (Finnish Federation for Communications and Teleinformatics)		info@ficom.fi	
EK (Confederation of Finnish Industries)		ek@ek.fi	
Academic organisations active in network and information security			
VTT (Technical Research Centre of Finland)		info@vtt.fi	
Lappeenranta University of Technology		info@lut.fi	
University of Oulu		oulun.yliopisto@oulu.fi	
University of Tampere		registry@uta.fi	
University of Turku		tucs@abo.fi	
Other bodies and organisations active in network and information security			

Appendix 2

Name	Website	E-mail	Country
NESO (National Emergency Supply Organisation)		info@nesa.fi	
CSC (IT Center for Science Ltd)		security@csc.fi	
Finnish Consumer Agency and Consumer Ombudsman		posti@kuluttajavirasto.fi	
FISA (Finnish Information Security Association)		info@tietoturva.org	
France			
National authorities in network and information security			
ANSSI (French Network and Information Security Agency)		communication@ssi.gouv.fr	
CFSSI (Centre of Education and Training in Information Security)		cfssi@ssi.gouv.fr	
Certification body of the French Network and Information Security Agency		certification.anssi@ssi.gouv.fr	
OCLCTIC		oclctic@interieur.gouv.fr	
Computer Emergency Response Teams (CERTs)			
COSSI (ITSOC) (24/7)		cossi@ssi.gouv.fr	
Cert-IST		cert@cert-ist.com	
CERT-LEXSI		cert@lexsi.com	
CERT-Renater		certsvp@renater.fr	
Industry organisations active in network and information security			
Alliance TiCS		info@alliance-tics.org	
Other bodies and organisations active in network and information security			
ARCEP (Electronic Communications and Post Regulatory Authority)		conso@art-telecom.fr	
Clusif		clusif@clusif.asso.fr	
CLCV		clcv@clcv.org	
DUI (Délégation aux Usages de l'Internet)		confiance@education.gouv.fr	
OSSIR		Secretariat@ossir.org	
Germany			
National authorities in network and information security			
Federal Ministry of the Interior		poststelle@bmi.bund.de	
Federal Office for Information Security		bsi@bsi.bund.de	
BIT (Federal Office for Information Technology)		poststelle@bva.bund.de	
Federal Commissioner for Data Protection and Freedom of Information		poststelle@bfdi.bund.de	
Federal Ministry of Economics and Technology		info@bmwi.bund.de	
Federal Network Agency		poststelle@bnetza.de	
Federal Criminal Police Office		info@bka.de	
Computer Emergency Response Teams (CERTs)			
CERT-BUND		certbund@bsi.bund.de	
CERT-VW		cert-vw@volkswagen.de	
CERTBw		certbw@bundeswehr.org	
CERTCOM		cert@certcom.de	
ComCERT		contact@cert.commerzbank.com	
dCERT		dcert@dcert.de	
DFN-CERT		info@dfn-cert.de	
FSC-CERT		fsc-cert@fujitsu-siemens.com	
GNS-CERT		cert@gnsec.net	
BFK		info@bfk.de	
PRE-CERT		precert@pre-secure.de	
RUS-CERT		cert@uni-stuttgart.de	
SAP CERT		cert@sap.com	
S-CERT		S-CERT@S-CERT.de	
SECU-CERT		security@secunet.de	
Siemens-CERT		cert@siemens.com	
T-COM-CERT		cert.t-com@telekom.de	

Appendix 2

Name	Website	E-mail	Country
Telekom-CERT		cert@telekom.de	
Industry organisations active in network and information security			
Bitkom		bitkom@bitkom.org	
eco		berlin@eco.de	
VATM		vatm@vatm.de	
VDE		itg@vde.com	
ZVEI		zvei@zvei.org	
Academic organisations active in network and information security			
University of Applied Sciences Gelsenkirchen, Faculty of Computer Sciences, Institute for Internet Security		information@internet-sicherheit.de	
University of Bamberg, Faculty of Information Systems and Applied Computer Sciences		dekanat@wiai.uni-bamberg.de	
International School of IT Security		info@is-its.org	
University of Bonn, Institute of Computer Science IV, Communication and Distributed Systems		office4@cs.uni-bonn.de	
University of Hildesheim, Institute of Computer Science		webmaster@iis.uni-hildesheim.de	
Technical University Ilmenau		iwm@tu-ilmenau.de	
Leibniz University Hanover, Faculty of Law, Institute for Legal Informatics (IRI)		sekretariat@iri.uni-hannover.de	
Passau University, Institute of IT-Security and Security Law		isl.office@fim.uni-passau.de	
TU Braunschweig Institut für Betriebssysteme und Rechnerverbund		info@ibr.cs.tu-bs.de	
b-it (Bonn-Aachen International Center for Information Technology)		info@b-it-center.de	
Universität Karlsruhe, Fakultät für Informatik, Institut für Kryptographie und Sicherheit (IKS)/ Europäische Institut für Systemsicherheit (EISS		EISS_Office@ira.uka.de	
Other bodies and organisations active in network and information security			
Deutschland sicher im Netz e.V. (DsiN)		info@sicher-im-netz.de	
Initiative D21		kontakt@initiatived21.de	
vzbz		info@vzbv.de	
Klicksafe.de		info@klicksafe.de	
TeleTrusT		info@ TeleTrusT.de	
Greece			
National authorities in network and information security			
Ministry of Transport and Communications		ict@yme.gov.gr	
General Secretariat for Information Systems, Ministry of Economy and Finance		info@gsis.gr	
EETT (National Telecommunications and Post Commission)		info@eett.gr	
ADAE (Hellenic Authority for Communication Privacy)		info@adae.gr	
Hellenic Data Protection Authority		contact@dpa.gr	
Computer Emergency Response Teams (CERTs)			
AUTH-CERT		cert@auth.gr	
GRNET-CERT		grnet-cert@grnet.gr	
Industry organisations active in network and information security			
SEPE (Federation of Hellenic Information Technology & Communications Enterprises)		info@sepe.gr	
SEPVE (Association of Information Technology Companies of Northern Greece)		sepve@sepve.org.gr	
Academic organisations active in network and information security			
ICS–FORTH (Institute for Computer Science - Foundation For Research and Technology Hellas)		ics@ics.forth.gr	
GRNET (Greek Research and Technology Network)		info@grnet.gr	
Other bodies and organisations active in network and information security			
INKA (General Consumers' Federation of Greece)		inka@inka.gr	
KEPKA (Consumers' Protection Center)		consumers@kepka.org	
E.K.PI.ZO (Association for the Quality of Life)		info@ekpizo.gr	
SafeNetHome		info@saferInternet.gr	
Hungary			
National authorities in network and information security			

Appendix 2

Name	Website	E-mail	Country
National Communications Authority Hungary		info@nhh.hu	
Data Protection Commissioner of Hungary		adatved@obh.hu	
Computer Emergency Response Teams (CERTs)			
CERT-Hungary		info@cert-hungary.hu	
HUN-CERT SZTAKI		cert@cert.hu	
NIIF-CSIRT		csirt@mail.ki.iif.hu	
Industry organisations active in network and information security			
IVSZ (Hungarian Association of IT Companies)		iroda@ivsz.hu	
eSec.hu (Hungarian Cyber Security Package)		info@esec.hu	
Melasz (Hungarian Association for Electronic Signature)		elnokseg@melasz.hu	
Other bodies and organisations active in network and information security			
MSZT (Hungarian Standards Institution)		info@mszt.hu	
NHIT (National Telecommunications and Information Council)		info@nhh.hu	
Ireland			
National authorities in network and information security			
ComReg (Commission for Communications Regulation)		info@comreg.ie	
Irish Information Security Forum (IISF)		secretary@iisf.ie	
Computer Emergency Response Teams (CERTs)			
HEAnet-CERT		cert@heanet.ie	
Industry organisations active in network and information security			
ICT Ireland		info@ictireland.ie	
ISA (Irish Software Association)		isa@ibec.ie	
ISSA Ireland		info@issaireland.org	
Academic organisations active in network and information security			
University College Dublin, School of Computer Science and Informatics		csi.secretary@ucd.ie	
Other bodies and organisations active in network and information security			
HEAnet		info@heanet.ie	
Italy			
National authorities in network and information security			
ISCOM		iscom@comunicazioni.it	
Ministry for Public Administration and Innovation		redazioneweb@funzionepubblica.it	
CNIPA (National Centre for Informatics in the Public Administration)		comunicazione@cnipa.it	
Italian Personal Data Protection Authority		garante@garanteprivacy.it	
OCSI (National security certification and accreditation body)		ocsi@istsupcti.it	
Computer Emergency Response Teams (CERTs)			
CERT-IT		cert-it@dsi.unimi.it	
CERT ENEL		cert@soc.enel.it	
GARR-CERT		cert@garr.it	
Govcert.IT		info@govcert.it	
Industry organisations active in network and information security			
AITech-Assinform		segreteria@aitech-assinform.it	
Clusit		amministrazione@clusit.it	
Other bodies and organisations active in network and information security			
Sincert (National system for the accreditation of certification and inspection bodies)		sincert@sincert.it	
Latvia			
National authorities in network and information security			
Ministry of Transport		satiksmes.ministrija@sam.gov.lv	
CSIRT–DDIRV (State Information Network Agency)		info@ddirv.lv	
Data State Inspectorate		info@dvi.gov.lv	
Ministry of Regional Development and Local Governement		pasts@raplm.gov.lv	

Appendix 2

Name	Website	E-mail	Country
Computer Emergency Response Teams (CERTs)			
CERT NIC.LV (National CERT)		cert@nic.lv	
Industry organisations active in network and information security			
LIKTA (The Latvian Information Technology and Telecommunications Association)		office@likta.lv	
LTA (Telecommunication Association of Latvia)		info@telecom.lv	
LIA (Internet Association of Latvia)		office@lia.lv	
LDTA (Association of Computer Technologies of Latvia)		ldta@itnet.lv	
Other bodies and organisations active in network and information security			
Latvian Electrical Engineering and Electronics Industry Association		letera@latnet.lv	
ISACA - Latvia Chapter (Information Systems Audit and Control Association)		info@isaca.lv	
Lithuania			
National authorities in network and information security			
Ministry of Transport and Communications		transp@transp.lt	
Information Policy Department, Ministry of the Interior		korespondencija@vrm.lt	
Police Department (under the Ministry of the Interior)		info@policija.lt	
RRT (Communications Regulatory Authority of the Republic of Lithuania)			
Information Society Development Committee under the Government of the Republic of Lithuania		info@ivpk.lt	
State Data Protection Inspectorate		ada@ada.lt	
Computer Emergency Response Teams (CERTs)			
CERT-LT		cert@cert.lt	
Industry organisations active in network and information security			
Infobalt (Association of Information Technology, Telecommunications and Office Equipment Enterprises of Lithuania)		office@infobalt.lt	
Academic organisations active in network and information security			
Litnet (Academic and Research Network in Lithuania)		info@litnet.lt	
Other bodies and organisations active in network and information security			
State Consumer Rights Protection Authority		tarnyba@nvtat.lt	
Luxembourg			
National authorities in network and information security			
Ministry of the Economy and Foreign Trade, Communications Department		info@eco.public.lu	
CASES (Cyberworld Awareness and Security Enhancement Structure)		contact@cases.lu	
ILR (Institut Luxembourgeois de Régulation)		ilr@ilr.lu	
CTIE (Centre des Technologies de l'Information de l'Etat)		info@ctie.etat.lu	
HCPN (Haut-Commissariat à la Protection Nationale)		secretariat@hcpn.etat.lu	
CNPD (Commission national pour la Protection des Données)		info@cnpd.lu	
ULC (Union Luxembourgeoise des Consommateurs)		ulc@pt.lu	
Computer Emergency Response Teams (CERTs)			
ASBL CSRRT-LU (Computer Security Research and Response Team Luxembourg)		csrrt@csrrt.org	
CIRCL (Computer Incident Response Centre Luxembourg)		info@circl.lu	
RESTENA-CSIRT		csirt@restena.lu	
Academic organisations active in network and information security			
University of Luxembourg (Interdisciplinary Centre for Security, Reliability and Trust)		snt@uni.lu	
Public Research Centre Henri Tudor		info@tudor.lu	
Public Research Centre Gabriel Lippmann		contact@lippmann.lu	
Other bodies and organisations active in network and information security			
CLUSIL (CLUb de la Sécurité de l'Information Luxembourg)		contact@clusil.lu	
ISACA Luxembourg Chapter		isacalux@gmail.com	
Malta			
National authorities in network and information security			
Malta Communications Authority		info@mca.org.mt	
Ministry for Infrastructure, Transport and Communications		info.mitc@gov.mt	

Appendix 2

Name	Website	E-mail	Country
Computer Emergency Response Teams (CERTs)			
mtCERT		mtcert.mitts@gov.mt	
Other bodies and organisations active in network and information security			
Malta Information Technology Agency		callcentre.mita@gov.mt	
CA Malta (Consumers' Association of Malta)		info@camalta.org	
The Netherlands			
National authorities in network and information security			
Ministry of Economic Affairs		ezinfo@postbus51.nl	
Ministry of the Interior and Kingdom Relations		bzkinfo@postbus51.nl	
Ministry of Justice		justitie@postbus51.nl	
OPTA (Independent Regulator for Post and Electronic Communications)		info@opta.nl	
CBP (Data Protection Authority)		info@cbpweb.nl	
Computer Emergency Response Teams (CERTs)			
GovCert.NL		info@govcert.nl	
Industry organisations active in network and information security			
ICT-Office		info@ictoffice.nl	
VNO-NCW (Confederation of Netherlands Industry and Employers)		informatie@vno-ncw.nl	
Academic organisations active in network and information security			
SAFE-NL (Platform for Security, Applications, Formal Aspects and Environments in The Netherlands)		jhh@cs.ru.nl	
Other bodies and organisations active in network and information security			
ECP-EPN (Platform for the Information Society in the Netherlands)		info@ecp-epn.nl	
Media Plaza (Security Plaza)		seminar@mediaplaza.nl	
ICTU		info@ictu.nl	
Sentinels (ICT security research programme (2004–12))		info@sentinels.nl	
NVB (The Netherlands Bankers Association)		info@nvb.nl	
NLnet Foundation		info@nlnet.nl	
Poland			
National authorities in network and information security			
Ministry of Interior and Administration		wp@mswia.gov.pl	
Office of Electronic Communications		uke@uke.gov.pl	
Bureau of the Inspector General for the Protection of Personal Data		kancelaria@giodo.gov.pl	
ABW (National Internal Security Agency)		poczta@abw.gov.pl	
Polish Committee for Standardisation		prezesekr@pkn.pl	
Office for Competition and Consumer Protection		uokik@uokik.gov.pl	
Computer Emergency Response Teams (CERTs)			
CERT.GOV.PL		cert@cert.gov.pl	
CERT Polska		cert@cert.pl	
Industry organisations active in network and information security			
KIGEiT (The Polish Chamber of Commerce for Electronics and Telecommunication)		kigeit@kigeit.org.pl	
PIIT (The Polish Chamber of Information Technology and Telecommunications)		biuro@piit.org.pl	
Other bodies and organisations active in network and information security			
FK (Polish Consumer Federation National Council)		biuro@federacja-konsumentow.org.pl	
Portugal			
National authorities in network and information security			
UMIC (Knowledge Society Agency)		umic@umic.pt	
ICP-Anacom		info@anacom.pt	
Computer Emergency Response Teams (CERTs)			
CERT.PT		report@cert.pt	
Industry organisations active in network and information security			
Anetie (Portuguese Information Technologies and Electronics Association)		geral@anetie.pt	

Appendix 2

Name	Website	E-mail	Country
Apritel (Portuguese Association of Electronic Telecommunication Companies)		apritel@apritel.org	
Other bodies and organisations active in network and information security			
DECO (Consumer organisation)		decolx@deco.pt	
Internet Segura		geral@Internetsegura.pt	
Seguranet		seguranet@crie.min-edu.pt	
Romania			
National authorities in network and information security			
Ministry of Communications and Information Technology		office@mcti.ro	
National Authority for Communications and Information Technology		anrcti@anrcti.ro	
Computer Emergency Response Teams (CERTs)			
RoCSIRT		team@csirt.ro	
Industry organisations active in network and information security			
Aries (Romanian Association for Electronic and Software Industry)		office@aries.ro	
Other bodies and organisations active in network and information security			
ISACA - Romania Chapter		contact@isaca.ro	
APC-Romania (Association for Consumers' Protection)		office@apc-romania.ro	
Slovakia			
National authorities in network and information security			
Ministry of Finance		podatelna@mfsr.sk	
Government Plenipotentiary for Information Society		urad@government.gov.sk	
The Office for Personal Data Protection		statny.dozor@pdp.gov.sk	
National Security Authority		info@nbusr.sk	
Industry organisations active in network and information security			
ITAS (IT Association Slovakia)		itas@itas.sk	
Academic organisations active in network and information security			
Department of Computer Science, Faculty of Mathematics, Physics and Informatics, Comenius University		ki@dcs.fmph.uniba.sk	
Faculty of Informatics and Information Technologies, Slovak University of Technology in Bratislava		info@fiit.stuba.sk	
Other bodies and organisations active in network and information security			
SASIB (Slovak Association for Information Security)		info@sasib.sk	
ZSS (Association of Slovak Consumers)		zss@zss.sk	
Slovenia			
National authorities in network and information security			
Post and Electronic Communications Agency of the Republic of Slovenia		info.box@apek.si	
Ministry of Public Administration, Directorate for e-Government and Administrative Processes		gp.mju@gov.si	
SIGOV-CA (Slovenian Governmental Certification Authority)		sigov-ca@gov.si	
SIGEN-CA (Slovenian General Certification Authority)		sigen-ca@gov.si	
Ministry of Higher Education, Science and Technology, Directorate for the Information Society		gp.mvzt@gov.si	
Office for the Protection of Classified Information		gp.uvtp@gov.si	
Information Commissioner		gp.ip@ip-rs.si	
Computer Emergency Response Teams (CERTs)			
SI-CERT (Slovenian Computer Emergency Response Team)		cert@cert.si	
Industry organisations active in network and information security			
Chamber of Commerce and Industry - Association of Informatics and Telecommunications		info@gzs.si	
Academic organisations active in network and information security			
Laboratory for Cryptography and Computer Security, Faculty of Computer and Information Science, University of Ljubljana		tajnistvo@fri.uni-lj.si	
ARNES (Academic and Research Network of Slovenia)		arnes@arnes.si	
Other bodies and organisations active in network and information security			
SETCCE (Security Technology Competence Centre)		info@setcce.org	

Appendix 2

Name	Website	E-mail	Country
Jozef Stefan Institute Laboratory for Open System and Networks		info@e5.ijs.si	
Cepris (Centre for Legal Informatics)		info@cepris.si	
ZPS (Slovene Consumers' Association)		zps@zps.si	
SAFE-SI		info@safe.si	
Spain			
National authorities in network and information security			
Ministry of Industry, Tourism and Trade - State Secretariat for Telecommunications and Information Society		info@mityc.es	
National Intelligence Centre - Cryptological National Centre		cni@cni.es	
Computer Emergency Response Teams (CERTs)			
CCN-CERT		nfo@ccn-cert.cni.es	
Industry organisations active in network and information security			
AETIC (Spanish Electronics, Information Technology and Telecommunications Industry Association)		aetic@aetic.es	
Asimelec (Spanish Electronic and Communications Multisectorial Industry Association)		asimelec@asimelec.es	
ANEI (National Association of Internet Enterprises)		anei@a-nei.org	
ISMS Forum Spain		info@ismsforum.es	
Sweden			
National authorities in network and information security			
National Post and Telecom Agency		pts@pts.se	
Swedish Data Inspection Board		datainspektionen@datainspektionen.se	
MSB (The Swedish Civil Contingencies Agency)		registrator@msbmyndigheten.se	
The Swedish Consumers' Association		mailinfo@sverigeskonsumentrad.se	
Computer Emergency Response Teams (CERTs)			
Sitic (Swedish IT Incident Centre)		sitic@pts.se	
SUNet CERT		cert@cert.sunet.se	
Industry organisations active in network and information security			
Swedish IT and Telecom Industries		itotelekomforetagen@almega.se	
United Kingdom			
National authorities in network and information security			
BIS (Department for Business, Enterprise and Regulatory Reform)		infosecpolicyteam@bis.gsi.gov.uk	
IS&A (Information Security and Assurance)		isa@cabinet-office.x.gsi.gov.uk	
Home Office		public.enquiries@homeoffice.gsi.gov.uk	
Information Commissioner's Office		mail@ico.gsi.gov.uk	
CESG (Communications-Electronics Security Group)		enquiries@cesg.gsi.gov.uk	
Computer Emergency Response Teams (CERTs)			
BP DSAC (BP Digital Security Alert Centre)		dctdsalertcentre@bp.com	
BTCERTCC		btcertcc@bt.com	
Cisco PSIRT		psirt@cisco.com	
CSIRTUK		csirtuk@cpni.gsi.gov.uk	
DAN-CERT		dancert@dante.org.uk	
GovCertUK		incidents@govcertuk.gov.uk	
MODCERT		cert@cert.mod.uk	
Industry organisations active in network and information security			
TUFF (Telecommunications UK Fraud Forum)			
Other bodies and organisations active in network and information security			
IISP (Institute for Information Security Professionals)		info@instisp.com	
Which?		which@which.co.uk	
NCC (National Consumer Council)		info@ncc.org.uk	
Pan-European Stakeholder Organisations			
DIGITALEUROPE (European Digital Technological Industry)		info@digitaleurope.org	
EuroISPA (European Internet Services Providers Association)		secretariat@euroispa.org	

Appendix 2

Name	Website	E-mail	Country
ETNO (European Telecommunications Network Operators' Association)		etno@etno.be	
ESA (European Software Association)		contact@europeansoftware.org	
CEPIS (Council of European Professional Informatics Societies)		info@cepis.org	
eema (European Association for e-Business and Security)		info@eema.org	
EUROSMART		eurosmart@eurosmart.com	
BEUC (The European Consumers' Organisation)		consumers@beuc.eu	
Other organisations			
Austrian Computer Society (OCG)	http://www.ocg.at/	ocg@ocg.at	AT
Federation of Belgian Informatics Associations	http://www.bfia.be/	olivier.braet@vub.ac.be	BE
Union of Automation and Informatics (UAI)	http://www.sai.infotel.bg/	sai@infotel.bg	BG
Swiss Informatics Society (SI)	http://www.s-i.ch/	admin@s-i.ch	CH
Czech Society for Cybernetics and Informatics (CSKI)	http://www.cski.cz/	cski@utia.cas.cz	CZ
Gesellschaft für Informatik e.V - (GI)	http://www.gi.de/	info@gi.de	DE
Informationstechnische Gesellschaft im Verband der Elektrotechnik Elektronik I	http://www.vde.com/	itg@vde.com	DE
German Science Journalists' Association (WPK)	http://www.wpk.org/	wpk@wpk.or	DE
German Association of Science Writers (TELI)	http://www.teli.de/	hajo.neubert@teli.de	DE
Dansk IT	http://www.dansk-it.dk/	dansk-it@dansk-it.dk	DK
Danish Science Journalists' Association	http://www.videnskabsjournalister.dk/	info@videnskabsjournalister.dk	DK
Asociación de Técnicos de Informática (ATI)	http://www.ati.es/	secregen@ati.es	ES
Spanish Association of Science Communication (AECC)	http://www.agendadelacomunicacion.com/aepc/	calvoroy@gmail.com	ES
Finnish Information Processing Association (FIPA)	http://www.ttlry.fi/	fipa@ttlry.fi	FI
Finnish Association of Science Editors and Journalists (FASEJ)	http://www.suomentiedetoimittajat.fi/	vesanias@enostone.fi	FI
French Association of Science Journalists (AJSPI)	http://www.ajspi.com/	contact@ajspi.com	FR
Hellenic Professionals Informatics Society (HEPIS)	http://www.hepis.gr/	info@hepis.gr	GR
John von Neumann Computer Society (NJSzT)	http://www.njszt.hu/	titkarsag@njszt.hu	HU
The Irish Computer Society (ICS)	http://www.ics.ie/	info@ics.ie	IE
Council of European Professional Informatics Societies (CEPIS)	http://www.cepis.org/	info@cepis.org	International
International Federation for Information Processing (IFIP)	http://www.ifip.or.at/	ifip@ifip.org	International
European Union of Science Journalists' Associations (EUSJA)	http://eusja.sciencewriters.eu/	eusja@euroscience.org	International
Euroscience	http://www.euroscience.org/	http://www.euroscience.org/contact,10262,en.html	International
Icelandic Society for Information Processing (ISIP)	http://www.sky.is/	sky@sky.is	IS
Associazione Italiana per l'Informatica ed il Calcolo Automatico (AICA)	http://www.aicanet.it/	aica@aicanet.it	IT
Associazione Informatici Professionisti (AIP)	http://www.aipnet.it/	segreteria@aipnet.it	IT
Italian Association of Science Journalists (UGIS)	http://www.ugis.it/	ugis@ugis.it	IT
Science Writers in Italy - SWIM	http://www.sciencewriters.it/	turone@sciencewriters.it	IT
Lietuvos Kompiuterininku Sajunga (LIKS)	http://www.liks.lt/	liks@liks.lt	LT
Latvian Information Technology & Telecommunications Association (LIKTA)	http://www.likta.lv/	office@likta.lv	LV
Computer Society of Malta (CSM)	http://www.csm.org.mt/	info@csm.org.mt	MT
Nederlands Genootschap voor Informatica (NGI)	http://www.ngi.nl/	info.ngi@ngi.nl	NL
Dutch Association of Science Journalists (VWN)	http://www.wetenschapsjournalisten.nl/vwn/	secretaris@wetenschapsjournalisten.nl	NL
Den Norske Dataforening (DND)	http://www.dataforeningen.no/	post@dataforeningen.no	NO
Associação de Profissionais de Informática (PROFIN)	http://www.profin.pt/	info@profin.pt	P
Polish Information Processing Society (PIPS)	http://www.pti.org.pl/	pti@pti.org.pl	PL
Asociatia Pentru Tehnologia Informatiei si Comunicatii (ATIC)	http://www.atic.org.ro/	officeATIC@atic.org.ro	RO
DF Dataforeningen i Sverige (Swedish Computer Society)	http://www.dfs.se/	info@dfs.se	SE
Slovenian Society Informatika (SSI)	http://www.drustvo-informatika.si/	info@drustvo-informatika.si	SI
Slovak Society for Computer Science (SSCS)	http://www.informatika.sk/	sscs@informatika.sk	SK
Informatics Association of Turkey (IAT)	http://www.tbd.org.tr/	tbd-merkez@tbd.org.tr	TR
British Computer Society (BCS)	http://www.bcs.org/	bcshq@hq.bcs.org.uk	UK

Appendix 2

Name	Website	E-mail	Country
Association of British Science Writers (ABSW)	http://www.absw.org.uk/	absw@absw.org.uk	UK