SCIENCE AND TECHNOLOGY OPTIONS ASSESSMENT
OPTIONS BRIEF No 2013-02, September 2013

Security of eGovernment Systems

Aim of the project

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

The project analysed and discussed security of eGovernment systems and services with special attention to the possibilities of future EU eGovernment services by gathering typical examples of existing national and international eGovernment services in Europe, analysing the most relevant security issues and possible response/solutions to these issues, debating policy options for advancing of EU eGovernment services and assessing and delivering specific policy options.

Overarching policy options

The most important contribution of the project is the development and assessment of 11 overarching policy options. The policy options are grouped by four overall aims.

Aim 1: Improving the resilience of European eGovernment systems.

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

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

This comprehensive security strategy aims to address all use of IT-systems in Europe and comprises policy measures to be taken in the short run (e.g. the use of security checklists), in the mid-term (including directions for future legislation, for example by making certifying software development processes mandatory) and in the long-term by describing more 'radical' new ways of ensuring security, such as a "clean slate" design such as pushed by US DARPA.

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

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

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

Depending on the threats, the production of more secure components should be aimed at, be it operating systems, application software or tamper resistant components. The use of certified product evaluations or certified development processes could be made mandatory, but will be very hard to enforce if components are

produced outside the EU. Also, the discussion and implementation of product liabilities could help for creating demand for better software.

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

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

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

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

Aim 2: Increasing privacy protection.

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

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

Privacy by Design is currently included in the revised draft regulation for data protection in the EU (EC 2012), referred to as 'Data Protection by Design'. This will increase incentives to implement Privacy by Design (PbD) for both suppliers of IT-systems that process personal data and for (government) organisations that procure such systems. To further stimulate the adoption of PbD, the development of a public knowledge base is necessary which includes reference architectures, design patterns, anonymisation and pseudonymisation techniques, thereby specifying what 'Privacy by Design' entails, showcasing practical experiences and improving the level of knowledge in EU about Privacy by Design in general. The knowledge base, and possibly the mandatory use of it, strengthens the skills and capabilities of IT-suppliers, IT-professionals and programmers to implement privacy enhancing features in their systems.

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

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

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

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

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

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

Aim 3: Achieving interoperability.

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

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

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

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

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

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

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

Based on a STOA study by the same title published in September 2013 (PE 513.510)

Editor:
ETAG - European Technology Assessment Group

Authors:
Anders Jacobi, Mikkel Lund Jensen, Linda Kool, Geert Munnichs and Arnd Weber

For further information, please contact:
Peter Ide-Kostic, STOA Unit
Directorate European Added Value and Impact Assessment, DG Internal Policies
European Parliament
Rue Wiertz 60 - RMD 00J0016, B-1047 Brussels
E-mail: stoa@europarl.europa.ep

www.europarl.europa.eu/stoa/