Baltic J. Modern Computing, Vol. 4 (2016), No. 1, 68-78

E-Service Security Challenges: Availability, Integrity, Confidentiality

Pjotrs DOROGOVS

Department of Modelling and Simulation, Riga Technical University,
Kalku Str. 1, LV-1658, Riga, Latvia

pjotrs.dorogovs@gmail.com

Abstract. Nowadays when usage of web-based applications and other interaction possibilities is becoming more and more integrated into everyday life, also government provided services are being rolled out in a form of so called e-services. Such approach allows citizens to benefit from them without even living own house. On the other hand, online processing of sensitive information is requiring modern information security measures. This paper summarizes topical security challenges of development and implementation of government e-services.

Keywords. Information security, Intrusion detection, WEB-based system security, e-commerce, e-services.

1. Introduction

Vast development of e-commerce based relationship between customer and service providers over past few years had undeniable influence on dialog among citizens and local authorities. These new tendencies have led to fact that more and more government e-services are being developed and put into production especially in developing countries. Utilization of such e-services contributes to much faster and organized communication with government institutions while significantly reducing usage of paper documents and bureaucracy. Taking into account that during online processing sensitive information is being exposed to high information security risks, the problem of ensuring its' safe handling has become highly topical. Main goal of current study is to analyze common issues that tend to be source of high information security risks during processing of sensitive information when using government e-services. Current paper consists of three main parts – overview of current situation and problems, guidelines for development of e-services and overview of technical platform for hosting of e-services.

2. Related work

The problem of ensuring strong security when using government e-services was underlined in early 2000s, when availability of PCs and Internet connections to simple citizens has become common thing. Early researches, (Mehta et al., 2000) focused on categorizing types of e-services and possible e-service security features, producing overall overviews of applicable methods of ensuring needed level of security. Later

(Obaidat and Boudriga, 2007), researches started to analyze possibilities of integrating already discovered fundamental concepts and e-security tools with modern security trends such as trust management systems, biometric based security solutions, usage of public key infrastructure systems (KPI) etc.

Security related issues became so topical, even EU co-funded innovation framework program called STORK (Secure idenTity acrOss boRders linKed) was established that was aimed to establish a European eID Interoperability Platform that will allow citizens to establish new e-relations across borders, just by presenting their national eID (Stern, 2011).

3. General E-service platform overview

According to its definition, a service can be considered as an e-service if it is being delivered online and for support of which IT automatization means are being used. Four e-service "digitalization" levels can be outlined:

1st level – Informing – Information about services is available in the Internet.

2nd level – Interaction – templates and documents can be downloaded.

3rd level – Two-way interaction – identification of the client, online submission of forms and information rather that in a printed way.

4th level – Transaction processing – full processing of a service, including decision making, informing, payments etc.

This paper is focused on 3rd and 4th levels of e-services. In a concept, e-service is such government provided service for citizens, companies and government itself, that allows the maximum reduction of a physical presence and for support of which IT automatization means are being used as much as possible.

E-service cannot exist without a service (**Fig. 1**). Each service always has its description that includes such information as:

1. Documents and other input conditions necessary for a commencement of a service;
2. Description of steps of a service (process description);
3. Description of a results of a service;
4. Other information according to public description of a service.

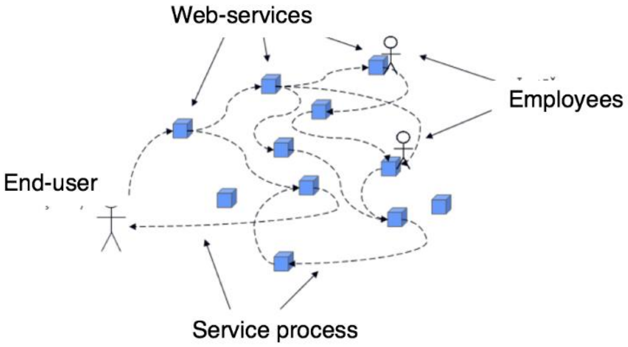
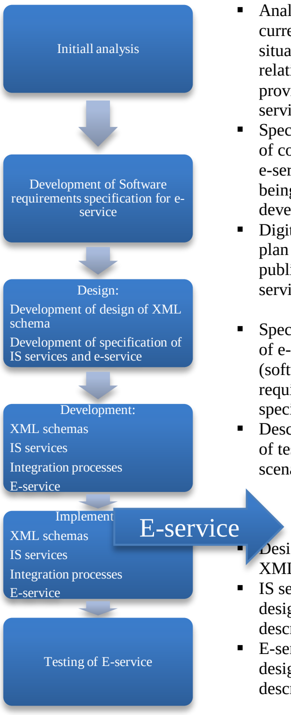


Fig. 1. E-service providing scenario

When providing services to a client, actions should be structured according to a certain sequence (business process). Service providing process usually involves various government authorities, services that are being provided by only one authority are really rare and hard to find. During execution of a process management and control is transferred to different persons, also various information systems are being used.

Table 1. Development process

Input information	Step of the process	Results	Executor	Method	Standards
▪ Legal acts ▪ Procedures ▪ Description of existing services	 Initiall analysis Development of Software requirements specification for e-service Design: Development of design of XML schema Development of specification of IS services and e-service Development: XML schemas IS services Integration processes E-service Implement XML schemas IS services Integration processes E-service Testing of E-service E-service	▪ Analysis of current situation in relation to providing of service ▪ Specification of content of e-service being developed ▪ Digitalization plan of public service	▪ State register officials ▪ Project managers and analysts ▪ Developers – technical specialists	▪ Survey of involved institutions ▪ Limited volume interviews ▪ Analyses of other examples and implementations ▪ Analyses of legal acts ▪ Interviews with industry experts	▪ Models of digitalization of government service
Plan for digitalization of public service: ▪ Description of e-service ▪ Description of possible improvements		▪ Specification of e-service (software requirement specification) ▪ Description of test scenarios	▪ State register officials ▪ Project managers and analysts ▪ Developers – technical specialists ▪ Solution architect	▪ Limited volume interviews ▪ Workshops with involved parties	▪ ISO 25001 ▪ E-service development guidelines
		▪ Design of XML schema ▪ IS service design description ▪ E-service design description	▪ State register officials – technical experts ▪ Developers – technical specialists ▪ Solution architect	▪ Interviews with technical experts	▪ ISO 25001 ▪ XML resource development guidelines ▪ IS service development standard
▪ Description of e-service ▪ Test scenarios		▪ XML schemas ▪ IS services ▪ Orchestration IS services ▪ E-service	▪ State register officials – technical experts ▪ Developers – technical specialists ▪ Solution architect	▪ Development and testing of single components	▪ XML resource development guidelines ▪ Guidelines for e-service architecture development ▪ E-service standard
▪ Description of e-service ▪ Test scenarios		▪ Publication of XML schemas ▪ Publication of IS services ▪ Publication of E-service	▪ Administrators of State register portals ▪ Officials of state register portals ▪ Officials of e-service portal	▪ Publication of components of e-service	▪ E-service standard
		▪ E-service is tested	▪ Developers of e-service ▪ Officials of state register portals ▪ Officials of e-service portal		▪ E-service standard

From the technical point of view e-service is a set of different services, integration and execution processes that are working in a close cooperation and purposefully with the intention to provide a service to its user.

Although it is being considered that development of Internet based services should follow common security base-lines, for an exchange of information that contains sensitive data such as names, birth dates etc. stricter security rules and guidelines should be developed and used. On the other hand, introduction of modern means of IT security are coast and time consuming actions that should be planned in a great detail. Such planning usually involves in-depth analysis of local and international legal acts and aspects that can influence transmission and processing of above mentioned sensitive information, availability of technical resources and in-house development possibilities, actual security standards and problems. In many cases, although such analysis is needed in order to cut development costs and time, it's being withdrawn due to a lack of qualified resources. At the end known number of introduced modern e-services are either incompatible with elementary security requirements, either their development was unreasonably long and expensive. Usually e-service development is performed using waterfall methodology (**Table 1**)

All above mentioned had lead author of this paper to a conclusion that flexible, fully customizable methodology for building of modern Information technology security system should be developed

Such methodology should cover all known security trends that government institution can face during a process of development of new e-services, giving them various possibilities to overcome modern security challenges. Besides that, such methodology should cover also aspects of already operational and under liquidation services and technological resources. It should include recommendations for assessment of security risks and possible security threat mitigation actions. At later stages, obtained results can serve as a basis not only for detailed risk analysis methods or technical investigations and checks, but also for a development of security threat risk management plans.

Usually lack of centralized coordination of development and support of e-services leads to common problems that include also security issues. The more complex government structure is established, the harder it is to firstly develop and make an agreement on standardized requirements and later to organize various institutions in usage of these requirements. Such process requires intensive work with all involved parties and is very resource and time consuming. Unfortunately, in some cases it is simply impossible to find consensus on certain problematic points these later leads to situations when services are being developed that are inconsistent with agreed requirements. In these cases, different procedures should be invoked and special actions undertaken to ensure compliance with at least minimal security and performance requirements. Situation is even more worsened if there is different understanding of "minimal" requirements among different institutions and involved parties. For example, due to special internal procedures for one of the institutions usage of certain cryptographic protocols is strictly forbidden which makes it impossible to organize data processing in different institution where there are no such restrictions. Such special cases have to be addressed in special steering committees that occasionally lengthen the process and makes the outcome unpredictable. Any way guidelines for security requirements can be agreed leaving details for later stages.

It is obligatory to plan security governance in three levels – strategic, operational and tactical. By organizing governance in above mentioned levels it should be possible to determine priorities, necessary finances and other resources, plan and implement common security activities, coordinate supporting and development activities. Key-points for guidelines for e-service security requirements should include all of above mentioned. There should be clear indications and recommendations for both development and hosting activities.

3.1. Approaches and means of addressing a problem

It is recommended to assign security responsible person in such way addressing common situation with lack of documentation or documentation not being in-line and fully mapped to current situation. Clear indication of anticipated final versions of all security and development documents should be given to development team. In addition, special attention paid at latter stages to ensure all documents are received timely and of acceptable quality. If possible, best practices and recommendations that are coming from various security communities should be followed. Internal security documentation should be prepared taking into consideration real-life principles there for such principles as “Security by obscurity” should be avoided. Implementation of innovations in the field of security has to analyzed giving priority to proven methods, protocols, algorithms and standards. Earlier works showed that white-listing is more preferable that black-listing when talking about IT security. This can be easily proven by comparing definitions of mentioned models – it is easier to control any environment when having full awareness of possible process inside this environment, that is why “positive” models (white listing), that only allows something that is already defined, in such cases are more recommended that “negative” models (black listing) that on other hand are disallowing everything that is defined thus living possibilities for unknown processes to be treated as positive. Fail-safe processes and mechanisms should be built in such a way so that failures or faults are tracked through same execution path as operations that have been disallowed. May government organization are starting to implement layered security policies and mechanisms. Such “Defense in depth” approach is increasing security of sensitive systems as a single entity. Failure of one security mechanism that is caused be possible security attack, will not compromise performance and availability of system as a whole because other security mechanisms will continue to provide some security processes to ensure protection. Nevertheless, even strongest layered security system must be kept as simple as possible. Special attention to the fact that the more complex, the harder it is to assess security therefore risks of security holes are higher should be paid when designing new security system. Other issue that is usually withdrawn is End-to-end security that is hard to implement and even harder to support, because it implies for appliance of security rules for entire system and covers all possible information flows from the origin to the final destination (e.g. trusted identity or attribute provider to service provider). When designing or implementing End-to-end security principles attention should be paid to all intermediate entities – “Origin” should authenticate to the “destination”, the “destination” should authenticate to “origin” and “destination” must check that received request is designed specially to him. Finally yet importantly, encryption be default is good manner of trustable security system. Unless a special cause exists, authenticated encryption should be implemented and used. Such approach is ensuring that private and sensitive data is not being transmitted in a plain text.

3.2. General requirements for e-service development contracting authorities

During development phase of a new e-service all of the contracting authorities should strictly follow special rules and procedures that will allow fluent integration of a newly developed e-service into existent platform. Ideally all contracting authorities should involve only such human resources that have been trained according to agreed security rules and that have been instructed to strictly follow them. All of a security measures being introduced into new e-service should be documented in details. If possible it is recommended to draw up check-lists for all development stages.

Table 2. List of possible attacks

Attack	Description	Corresponding threat
Spoofing	Spoofing is a possibility to hide one's real identity and is a situation in which one person or program successfully masquerades as another by falsifying data, thereby gaining an illegitimate advantage	• Impersonation of a citizen • Impersonation of system
Guessing	Guessing is a simple attack in which an attacker attempts to recover a secret used in a communication (e.g. encryption key, password etc.)	• Impersonation of a citizen • Impersonation of system
Communication eavesdropping	A network layer attack that focuses on capturing packets from the network transmitted by other computers and reading the data content in search of any type of information	• Impersonation of a citizen • Impersonation of system, • Privacy – user data
Session hijacking	A security attack on a user already authenticated session over a protected network	• Impersonation of a citizen • Impersonation of system
Replay Attack	Form of network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed.	• Impersonation of a citizen • Impersonation of system
Man-in-the-middle Attack	An attack where a user gets between the sender and receiver of information and sniffs any information being sent.	• Impersonation of a citizen • Impersonation of system • Identity data forge • Privacy – user data
User profiling	Profiling is the recording and classification of user behaviors.	• User profiling
Incorrect design and implementation	Possible vulnerability in the design or the code made during implementation process.	• System malfunction • System Denial of Service

		• System availability • Operation security
Unauthorised access	Viewing private accounts, messages, files or resources without permission or qualification from the owner	• System malfunction • System Denial of Service • System availability
Fuzzing	Technique used to discover coding errors and security loopholes in software, operating systems or networks by inputting massive amounts of random data, to the system.	• System malfunction • System Denial of Service • System availability • Operation security
Race condition	A race condition occurs when two or more threads can access shared data and they try to change it at the same time.	• System Denial of Service
Denial of Service Attack	an attempt to make a machine or network resource unavailable to its intended users	• System availability • Operation security
Social engineering	Psychological manipulation of people into performing actions or divulging confidential information	• Unawareness of privacy issues • Usability of privacy protecting tools • User – Accidental misuse • User – Forced misuse

For example a complete list of possible attacks (**Table 2**) and risks that it theory could threaten system that is being currently developed should be produced and kept actual during full development process. Such list of possible attacks should help responsible personal to identify and map linked threats and deepen their understanding about needed future steps to mitigate those.

Many common mistakes are being made during all phases of e-service development process – including drafting of technical specifications, development as such, testing and putting of e-services into production. For example, changes to security measures are not being documented, security documents are not being updated accordingly that is causing known problems at latter stages when changes to certain functionalities of e-services are needed. One of a widespread problematic issue is inability to specify exact platform on which e-service will be hosted and exact components that should be considered when developing is under progress, therefore in some cases it is hard to plan and implement such resources and interconnections that would allow basic functioning of an e-service even in case of failures. Also it is possible that initial requirements do not take into account already available and tested resources and do not specify recovery tools.

4. Technical side of e-service platforms

Since introduction of e-service platform as such is tended to faster and more organized communication with government institutions while significantly reducing usage of paper documents and bureaucracy also hosting platform must comply with certain rules and requirements.

Besides such common information security points as availability, integrity and confidentiality it also has to give end-users significant potential to use government services in an easy and understandable way. For this purposes it is best to host only one portal that would compile all available e-services in one homogeneous way. Such approach should allow end-users to start using new e-services without additional training. It would also contribute to a faster more reliable way of communication between citizens and government institutions. Also data quality problem can be addressed and some common mistakes solved even before they arise.

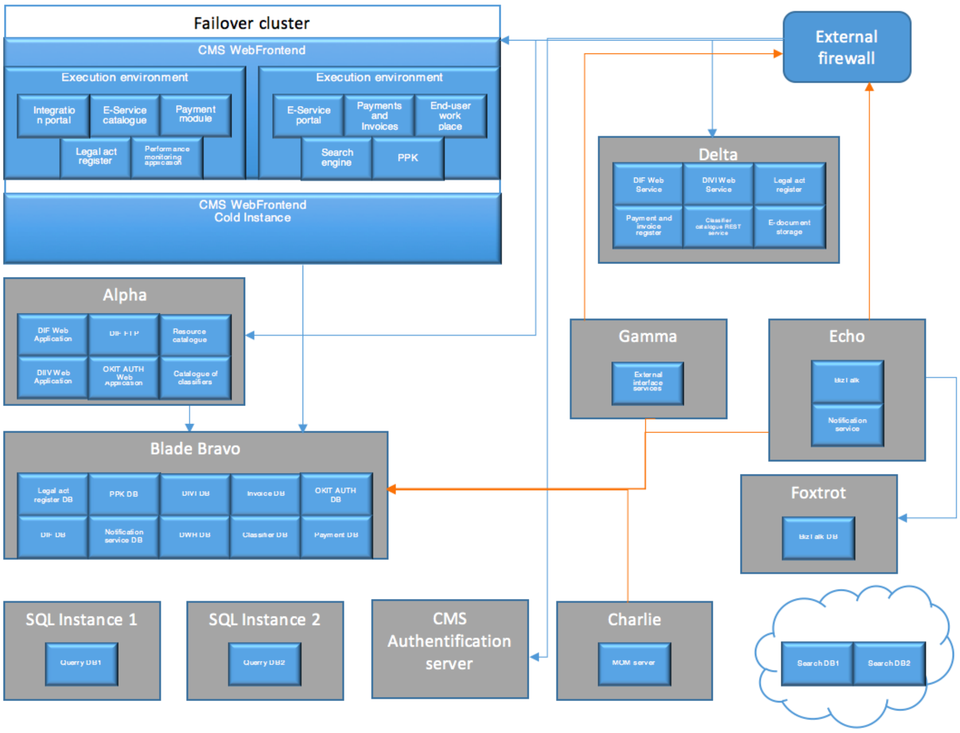


Fig. 2. E-service portal possible infrastructure

All of the above mentioned is clearly pointing to a conclusion that one technical platform is needed for hosting of all available government e-services. Unfortunately, such solution can bring up other management problems.

As it is presented in **Fig. 2**, E-service portal central infrastructure and communication stack is extremely complex state-of-the-art piece of various software and hardware components. This should be considered as the main point of introduction of IT security solutions and methods. Multi-level security system must be introduced to ensure overall defense of e-service platform.

4.1. Network security solutions

In general network security and intrusion protection systems includes any available method or recommendation that prevents attackers from gaining access to secured network, system or information asset. Most common ways to ensure high availability Intrusion protection system is usage of any kind of firewall or anti-virus software. Each type of IPS has different level of provided protection. Sometimes it's even advisable to build an IPS containing more than one security solution

Intrusion detection systems (

Fig. 3), in turn, may be considered as a type of security assuring method as for information systems as also for computers. Such system should make a comprehensive analysis of gathered information of computer, network or information system activities to proactively identify potential security breaches that might include both attacks from inside and outside of protected perimeter. The fact that data and systems cannot always be protected from outside intruders in modern Internet environment using ordinary security mechanisms such as password and file security, leads to a range of issues

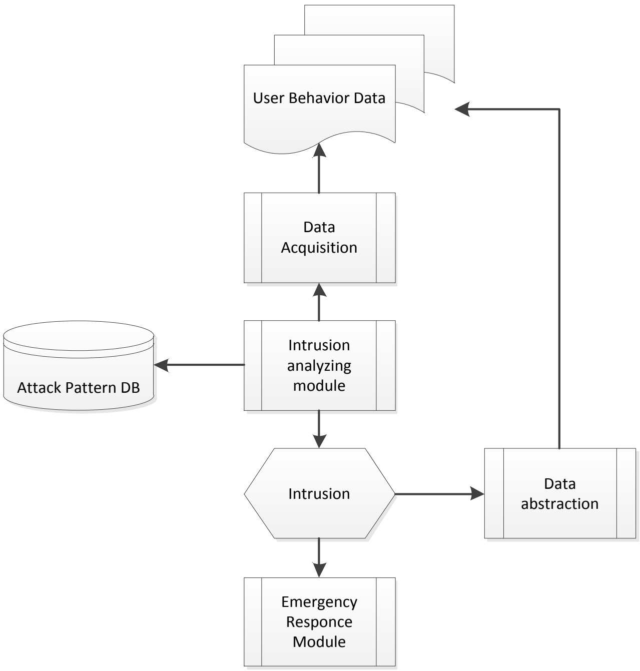


Fig. 3. General module of Intrusion detection system

For a e-service hosting WEB based platform displacement of Intrusion detection system is one of the vital issues to be solved to ensure security of information assets (**Fig. 4**). Comparing to end-user applications where IDS is likely to be deployed on host level which is otherwise defenseless (i.e. Windows based machines running previous versions of OS are unable to create even simple logs that later can be later processed by a off-line IDS), e-service hosting platforms should be protected on the network level rather than on hosts. In this case Intrusion detection system will be more effective when placed in the network perimeter, i.e. just behind and/or before the firewall, on links to partners etc. Otherwise it can be placed on the corporate WAN backbone where it is possible to monitor all the traffic that attempts to enter corporate network. In special cases to ensure high-end protection of valuable information storages or processing units solution of isolation of critical infrastructure into different network segment with its' own IDS is considered to be state-of-art technology in the field of information security.

Actual security threats should be taken into account both during development and putting into production stages. For all possible security risks that have been discovered during analysis phase mitigation scenarios and possibilities should be agreed. If possible it is necessary to check with partners and other contracting authorities if their solutions and/or platforms comply with your requirements, this is especially important when using third party user authentication services. Nevertheless special attention should also be paid to

- Authorization mechanisms as described above
- Usage of digital certificates
- Encryption of transport protocols
- Encryption of data
- Usage of existent Virtual Private Network (VPN) infrastructure of involved parties
- Hacking defense complexes including IP blocking and DoS attack defences
- Separation of services into different security groups.

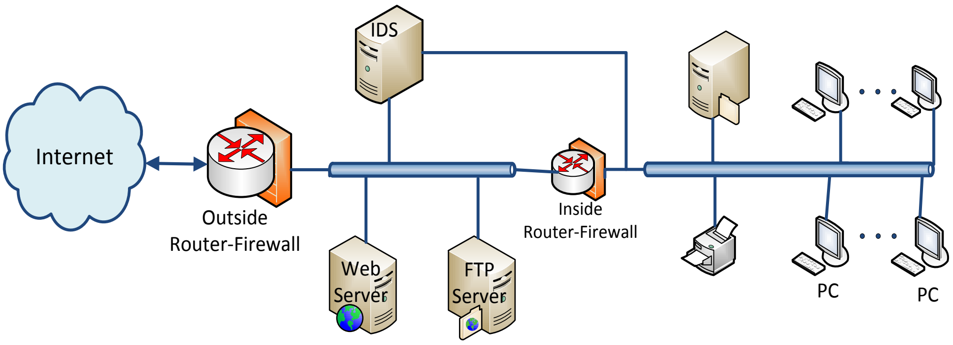


Fig. 4. Placement of Intrusion Prevention system

Among many other valuable issues it should be noted that implementation of firewalls between areas of the network with different requirements (i.e. between internet-intranet, between users-servers etc.), usage of network vulnerability scanners to double check firewalls and to find security holes that intruders can exploit, usage of host policy scanners to make sure they conform to accepted security practices and finally usage of symbiosis of NIDS, other packet sniffing utilities and host-based virus scanners to flag successful intrusions, may significantly improve overall level of information security of WEB based E-service platform.

Every connection between any of your server and a browser must use HTTPS. Previous analyses showed that end-users are not always enabling usage of X.509

certificate for TLS client authentication. Such fact should not derive from using of classical TLS authentication with a X.509 certificate at server side.

5. Conclusion

Fundamentals for implementation strategies for complex IT security systems for E-service platforms and for building of a trustable defense system were put down in 2000. Last decade proved that government e-service security systems should be planned already at the start of e-service implementation project thus allowing for introduction of modern means of security into e-service itself rather that at later stages struggling hard to met even simplest requirements. High level management should take steps to ensure that planning and development process of an e-service is done according to security best-practices. Future developments will focus on creating of flexible, fully customizable methodology for building of modern Information technology security system. It should cover all known security trends that government institution can face during a process of development of new e-services, giving them various possibilities to overcome modern security challenges

References

Hector D., Puyosa P. (2011). e-Government: Security Threats, IEEE eGovernment STC.

Jacobi A., Lund J. M., Kool L., Munnichs G., Weber A. (2013). “Security of eGovernment Systems”, Conference Report IP/A/STOA/FWC/2008-096/LOT4/C1/SC10.

Mehta M., Singh S., Lee Y. (2000) “Security in E-Services and Applications”

Merkow S. M., Breithaupt J. (2014) “Information Security: Principles and Practices”. Pearson IT Certification.

Obaidat M., Boudriga N. (2007) “Security of E-Systems and Computer Networks”. Cambridge University Press

Rust R. and Lemon K.N. (2001). E-Service and the Consumer. International Journal of Electronic Commerce 5(3) (spring), pp. 85-102

Stern M. (2011). Secure Identity Across Borders Linked. Security Principles and Best Practices. Competitiveness and innovation framework programme. ICT Policy Support Programme (ICT PSP)

Tiwana A., Ramesh B. (2001). E-services: problems, opportunities, and digital platforms Proceedings of the 34th Annual Hawaii International Conference on System Sciences (HICSS-34)-Volume 3, 3-6 Jan. 2001.

Wimmer, M., Codagnone, C. and Janssen, M. (2008). “Future of e-Government Research: 13 research themes identified in the eGovRTD2020 project”. Proceedings of the 41st Hawaii International Conference on System Sciences, USA

WEB (a). European Network of Excellence in Cryptology II, http://www.ecrypt.eu.org/

Received March 14, 2016, accepted March 22, 2016