Thomas Zefferer, Vesna Krnjic: "Usability Evaluation of Electronic Signature Based E-Government Solutions". In Proceedings of the IADIS International Conference WWW/INTERNET 2012, pp. 227-234, IADIS, 2012.

# USABILITY EVALUATION OF ELECTRONIC SIGNATURE BASED E-GOVERNMENT SOLUTIONS

Thomas Zefferer
*E-Government Innovation Center (EGIZ)*
*Inffeldgasse 16a, 8010 Graz, Austria*

Vesna Krnjic
*E-Government Innovation Center (EGIZ)*
*Inffeldgasse 16a, 8010 Graz, Austria*

**ABSTRACT**

Usability and security are crucial requirements of e-Government applications. Security requirements are typically met by approved cryptographic methods such as qualified electronic signatures. These methods usually rely on integration of cryptographic hardware tokens such as smart cards or mobile phones. Integration of these tokens into e-Government applications introduces additional complexity and often affects the usability of these solutions. To date, research on usability in e-Government has primarily focused on the evaluation of e-Government websites. Usability issues raised by the integration of cryptographic hardware tokens into e-Government applications have not been considered in detail so far. We filled this gap by conducting a usability analysis of three core components of the Austrian e-Government infrastructure. The evaluated components act as middleware and facilitate integration of cryptographic hardware tokens into e-Government applications. We have tested the usability and perceived security of these middleware components by means of a thinking-aloud test. This paper introduces the evaluated components, discusses the followed methodology of the conducted usability test, and presents obtained results.

**KEYWORDS**

Usability, E-Government, Security, Austrian Citizen Card, MOCCA, Mobile Phone Signature.

## 1. INTRODUCTION

In many countries, governments and public administrations make use of information and communication technologies (ICT) to improve the efficiency of administrative procedures and to ease interaction with citizens. These attempts have become commonly known under the term electronic government (e-Government). Current e-Government applications range from simple informational services (e.g. publication of relevant information on governmental websites) to complex transactional applications (e.g. filing tax documents and payments over the Internet). Transactional e-Government applications potentially comprise the transmission and processing of security and privacy sensitive data. Hence, these applications typically have to fulfill increased security requirements. To meet these requirements, approved cryptographic methods such as strong user authentication schemes and electronic signatures are employed.

Electronic signatures play an important role especially in the European Union, where qualified electronic signatures are legally equivalent to handwritten signatures according to the Directive 1999/93/EC of the European Parliament and of the Council on a Community framework for electronic signatures (EU Parliament and Council, 2000). To meet the requirements of qualified electronic signatures as defined by this directive, a secure signature creation device (SSCD) has to be used for the signature creation process. Since SSCDs typically rely on a secure hardware token, implementation alternatives are actually limited. Following the current state of the art, e-Government solutions usually require citizens to use personalized smart cards to create legally binding electronic signatures. Smart card based e-Government solutions have been deployed successfully in Austria, Belgium, Estonia, Portugal, Spain, and various other European countries. A couple of

European countries such as Austria or Estonia additionally provide citizens mobile signature solutions that employ mobile phones as hardware tokens instead of smart cards.

Regardless of the nature of the used hardware token, the question arises how these tokens can be used and accessed by e-Government applications. Currently, most countries rely on some kind of middleware that acts as intermediary between cryptographic hardware tokens and e-Government applications. This approach is also followed in Austria where several middleware solutions have been developed during the past decade. These solutions allow for a smooth integration of qualified electronic signatures and assure the security of e-Government applications.

Besides security, usability is another key success and acceptance factor of e-Government solutions. Schultz et al. have shown that the demand for usability often conflicts with given security requirements (Schultz et al., 2001). While an appropriate level of security requires the application of complex cryptographic methods and protocols, the increased complexity often significantly affects usability. It is thus hardly surprising that usability is often neglected in e-Government applications with high security requirements. This is problematic as it potentially leads to a scenario, in which e-Government applications are virtually restricted to expert users. To make e-Government solutions usable for all social and educational classes, usability has to be recognized as important requirement for e-Government applications and solutions.

The importance of usability in e-Government has been subject to ongoing research. However, most related work has focused on the usability of rather simple e-Government websites so far. For instance, a quality inspection method for the evaluation of e-Government sites has been proposed by Garcia et al. (Garcia et al., 2005). The usability of different e-Government websites in the UK has been evaluated by Ma et al. (Ma et al., 2003). Recently, also the usability of Norwegian e-Government websites has been discussed (Sorum, 2011). Without doubt, the usability of e-Government websites is an important topic. However, techniques to integrate qualified electronic signatures into Web based e-Government applications definitely need to be considered as well. Otherwise, usability evaluations of current e-Government solutions threaten to remain incomplete and to miss relevant aspects.

In Austria, electronic signatures are integrated into e-Government applications by means of different middleware solutions. We have evaluated the usability of these core components of the Austrian e-Government infrastructure by means of a usability test. The basic goal of this test was to compare the usability and user acceptance of different middleware implementations and to identify persisting weaknesses. In this paper we briefly introduce the evaluated components, discuss the followed methodology of the conducted usability test, and present obtained results.

The paper is structured as follows. In Section 2 we discuss core concepts of the Austrian e-Government and introduce the evaluated components in detail. The methodology of the conducted usability test is explained in Section 3. Subsequently, obtained results are discussed in Section 4. Conclusions are finally drawn in Section 5.

## 2. EVALUATED E-GOVERNMENT COMPONENTS

The key concept of the Austrian e-Government infrastructure is called Citizen Card (CC). The Citizen Card is an abstract definition of a cryptographic token that allows citizens to securely authenticate at e-Government services and to create qualified electronic signatures. The Citizen Card concept complies with the EU Signature Directive and fulfills all requirements of a secure signature creation device. This way, the Citizen Card represents an important enabler of secure e-Government applications in Austria.

Although the term Citizen Card might suggest the use of smart cards, the Citizen Card specifications (Hollosi, 2008) are actually rather abstract and not limited to a certain technology. This flexibility has led to the development of different Citizen Card implementations. Currently, both smart card based and mobile phone based Citizen Card implementations are available in Austria.

Irrespective of the underlying technology, all Citizen Card implementations facilitate secure user authentication and creation of qualified electronic signatures. Due to the technology neutral approach, citizens can individually choose their preferred implementation. Unfortunately, this flexibility significantly increases the complexity of application development processes. In order to integrate Citizen Card functionality, e-Government applications need to support all available Citizen Card implementations. To

overcome this problem, the Austrian e-Government strategy follows the middleware based approach illustrated in Figure 1.

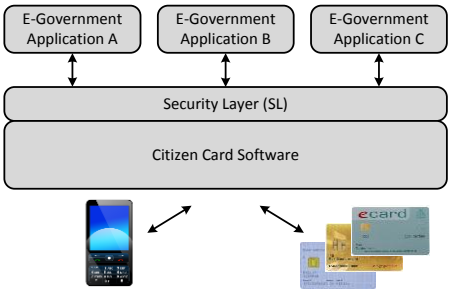


**Figure 1.** Access to Citizen Card implementations is provided by the Citizen Card Software.

The core element of this approach is the so called Security Layer (SL) interface that has been introduced and discussed by Leitold et al. (Leitold et al., 2002). The Security Layer is an abstract XML based interface that can be used by e-Government applications to access Citizen Card functionality. This way, applications do not need to integrate specific Citizen Card implementations, since all implementations can be accessed through a common interface. All implementation specific functionality is outsourced to the so called Citizen Card Software (CCS). The CCS implements access to specific Citizen Card implementations (e.g. smart cards) and provides their functionality through the common SL interface. Acting as middleware between e-Government applications and Citizen Card implementations, the Citizen Card Software plays a central role in the Austrian e-Government infrastructure. Since the SL specifications are open, different CCS implementations have emerged during the past years. The following figures show the basic concepts of the three most popular CCS implementations that are currently available in Austria.

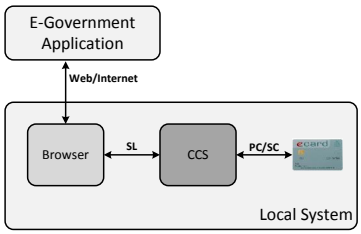


**Figure 2.** MOCCA Local.

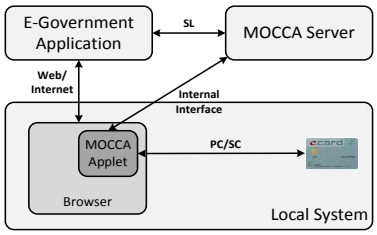


**Figure 3.** MOCCA Online.

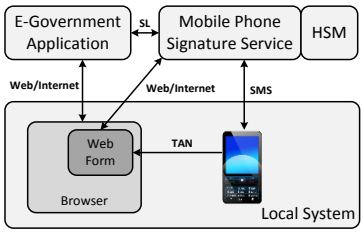


**Figure 4.** Mobile Phone Signature.

Figure 2 shows the basic architecture of the CCS *MOCCA Local*. The MOCCA (Modular Open Citizen Card Architecture) project[1] has been started in 2008 and aims to provide open source CCS solutions for Austrian citizens. MOCCA Local is one outcome of this project and implements a CCS by means of software being installed and running on the user's local system. MOCCA Local typically runs in the background and features a minimalistic user interface. If access to a locally connected smart card is requested by an e-Government application, a GUI window pops up. Through this window, users are provided with relevant information (e.g. the data that is about to be signed) and required user input (e.g. secure PIN to authorize the signature creation on the smart card) is collected.

From a usability point of view, the main drawback of MOCCA Local is the need to install software on the local computer, which can be problematic especially for technically inexperienced users. To overcome this problem, the MOCCA project has also investigated possibilities to implement an installation-free alternative. These efforts finally led to the development of *MOCCA Online*.

The basic architecture of MOCCA Online has been discussed by Centner et al. (Centner et al., 2010) and is shown in Figure 3. MOCCA Online follows a server based approach. The SL interface is not implemented by locally installed software, but by the central MOCCA Server component. E-Government applications contact the MOCCA Server in order to access citizens' smart cards. Physical access to the locally connected smart card is implemented by a Java Applet running on the citizen's local computer. MOCCA Applet and MOCCA Server together represent the CCS and exchange data through an internal interface. The MOCCA

[1] http://joinup.ec.europa.eu/software/mocca/home

Applet acts as user interface for the provision of relevant information (e.g. the data to be signed) and the collection of required user input (e.g. PINs).

MOCCA Online renders the need for local software installations unnecessary but still requires users to buy and use appropriate smart card reader devices. The goal to render smart cards completely unnecessary has been the main driver behind the development of mobile CCS solutions. In Austria, the so called *Mobile Phone Signature* (Orthacker et al., 2010) represents a mobile alternative to established smart card based approaches. The general architecture of the Mobile Phone Signature is shown in Figure 4.

Similar to MOCCA Online, a central service (Mobile Phone Signature Service) implements the SL interface. A hardware security module (HSM) that is attached to this central service acts a SSCD. The HSM is capable of creating qualified electronic signatures on behalf of users. To access Citizen Card functionality, e-Government applications send an appropriate request to the Mobile Phone Signature Service. Provision of the requested functionality (e.g. signature creation) has to be authorized by the citizen. Therefore, the Mobile Phone Signature Service requests the citizen to enter the phone number and a secret password through a Web form. The password is defined by the user during the personalization and activation process. If the provided credentials can be verified correctly, an SMS message is sent to the citizen's mobile phone containing a one-time password (Transaction Authentication Number - TAN). This TAN has to be entered in the Mobile Phone Signature Service's Web form in order to authorize execution of the e-Government application's request. The main advantage of this mobile approach is the central HSM, which renders smart cards unnecessary. By relying on a strong two-factor authentication scheme that makes use of two separated communication channels (i.e. Web and SMS), an adequate level of security is assured.

All three CCS implementations – MOCCA Local, MOCCA Online, and Mobile Phone Signature – meet given security requirements. To check whether these components are also able to fulfill given usability requirements, a usability test has been conducted. The followed methodology of this test is discussed in the next section.

# 3. METHODOLOGY

To evaluate the usability of MOCCA Local, MOCCA Online, and Mobile Phone Signature, the following four research questions have been defined beforehand.

- **Q1:** Do required software installations on the local system represent a barrier and reduce usability?
- **Q2:** How do users rate the overall usability of MOCCA Local, MOCCA Online, and Mobile Phone Signature?
- **Q3:** How do users rate the security and trustworthiness of MOCCA Local, MOCCA Online, and Mobile Phone Signature?
- **Q4:** Which CCS implementation do users prefer in general?

Answers to these questions have been obtained by the conducted usability test. We have applied a thinking-aloud test with 20 test users in order to evaluate the usability of the three different Austrian CCS implementations. The selected set of test users represented different social classes of the Austrian society. A well balanced distribution has been achieved regarding test users' ages, educational levels, and technical background.

The basic test run was identical for all test users and consisted of the following four phases.

- **P1 - Welcome:** Test users have been welcomed, have been provided with relevant information about the usability test, and have been asked to sign a non-disclosure agreement.
- **P2 - Background questionnaire:** At the beginning of the usability test, relevant information about the participating test user has been collected using a prepared questionnaire.
- **P3 - Execution of tasks:** In this phase, test users have been asked to carry out a sequence of predefined tasks using the three CCS implementations to be evaluated. After each task, test users have been asked to fill out a prepared questionnaire and to rate the tested component (post-task rating).
- **P4 - Conclusive interview:** After completion of all tasks, a conclusive interview has been conducted with all test users. After the interview, test users have been asked to fill out a final questionnaire (post-study rating) covering some general questions.

During Phase P3, test users have been asked to carry out predefined tasks using an off-the-shelf desktop PC. Representing a common configuration, all tests have been carried out using the Microsoft Windows 7 operating system and Microsoft Internet Explorer 8 Web browser. The desktop PC was equipped with a Reiner SCT card reader device. Test users were not allowed to use other system configurations (e.g. a different Web browser) as this would have rendered direct comparisons between test users difficult. An extension of the conducted usability test to other test system environments (e.g. alternative operating systems and Web browsers) is regarded as future work.

The used test system was equipped with Morae® Recorder software. This software allows the tracking and recording of user sessions including all user activities such as mouse movements and keyboard inputs. Additionally, comments and facial expressions of test users have been recorded with a web cam and stored together with the recorded user session for later analysis. Additionally, we have used a standard camera to record user comments during Phase P2 and Phase P4.

The filled questionnaires have represented an important data source for later analysis. To obtain as much valuable feedback as possible, we relied on semantic differentials. The method of semantic differentials (Boslaugh et al., 2008) is frequently used in social sciences and user experience research. In general, semantic differentials are used to measure the connotative meaning of an object and to further derive the attitude towards this object. We used semantic differentials to allow users to assign weighted properties to the evaluated software components.

Besides the filled questionnaires, also the recorded user sessions and user comments have been incorporated in the analysis process. These data has turned out to be extremely helpful in order to understand the collected user feedback and to identify reasons for negative ratings. Obtained results of the evaluation process will be presented in Section 4.

Most relevant information has been collected during Phase P3 of the usability test, i.e. during the execution of predefined tasks by test users. We have defined these tasks such that answers to the predefined Research Questions Q1-Q4 could be derived easily from the collected data. All test users have been asked to carry out the following five tasks.

- **T1:** Install the Citizen Card Software MOCCA Local on the local system.
- **T2:** Use MOCCA Local to file a demo e-Government application.
- **T3:** Use MOCCA Online to file a demo e-Government application.
- **T4:** Activate the Mobile Phone Signature for your mobile phone.
- **T5:** Use the Mobile Phone Signature to file a demo e-Government application.

A valid smart card based Citizen Card was the only prerequisite for test users. The first three tasks covered the evaluation of the smart card based CCS implementations MOCCA Local and MOCCA Online. The last two tasks covered the evaluation of the Austrian Mobile Phone Signature. In order to cancel out learning effects that might have biased the obtained results, we split the group of test users randomly into two subgroups. Group A started with Task T1 and carried out all tasks in the order shown above. In contrast, Group B was asked to start with Task T3 followed by T1, T2, T4, and T5 instead. This way, half of the test users started with evaluating MOCCA Local, while the other half started with testing MOCCA Online. Since the use of MOCCA Local or MOCCA Online was required to carry out Task T4 and T5, these two tasks have been carried out at the very end by both user groups. As the Mobile Phone Signature follows a completely different approach than the two smart card based solutions MOCCA Local and MOCCA Online, learning effects could be neglected.

# 4. RESULTS

Following the methodology discussed in Section 3, the usability test has been carried out with 20 test users in total. Obtained results of the conducted usability test and answers to the predefined research questions are presented in the following subsections.

## 4.1 Usability of installation-based CCS

In order to answer Research Question Q1, we evaluated whether the required installation process of MOCCA Local represents a barrier for users and hence reduces usability. To install MOCCA Local using Java

Webstart technology, test users had to navigate to a given website and click a launch button. After that, test users were asked to manually install a certificate into the used Web browser. Figure 5 shows that most test users rated the usability of the installation process positively. This corresponds to the observations that have been made during the test runs. Most users were able to complete the installation on their own.

An analysis of the recorded user sessions revealed that for some user the required certificate installation was problematic. To answer Research Question Q1, we can conclude that the required software installation process of MOCCA Local does not raise severe usability issues. Still, installation routines for certificates should be simplified in order to make this a feasible task also for inexperienced users.

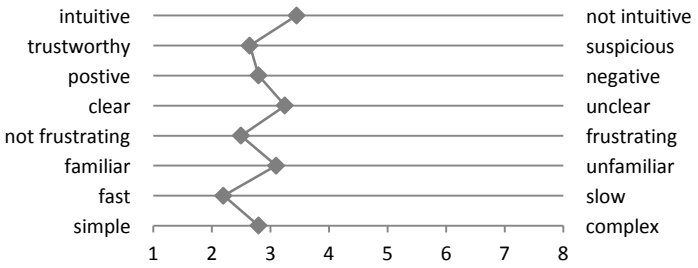


**Figure 5.** Evaluation results of the installation process of MOCCA Local.

## 4.2 Usability of different CCS implementations

According to Research Question Q2, we analyzed how the use of MOCCA Local, MOCCA Online, and Mobile Phone Signature had been rated by the test users in terms of usability. All test users have been asked to file a demo e-Government application using their Citizen Card and each of the three evaluated CCS implementations as defined by Tasks T2, T3, and T5.

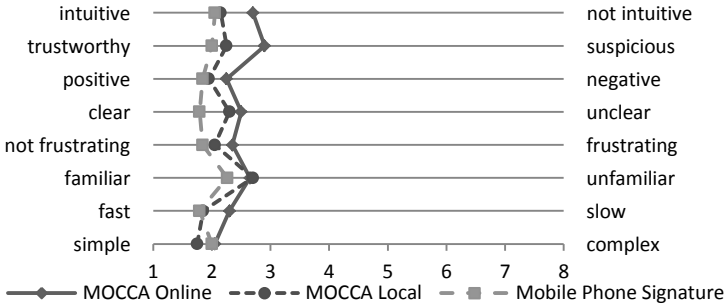


**Figure 6.** Perceived usability of different CCS implementations.

Figure 6 illustrates the results that have been obtained from analysis of the collected user. In general, all tested CCS implementations have been rated positively. Direct comparison of the obtained results shows that users rated the Mobile Phone Signature's usability best in most categories, followed by MOCCA Local and MOCCA Online.

## 4.3 Security and trustworthiness

Besides usability, the security and trustworthiness of used components is crucial for the acceptance of e-Government solutions. According to Research Question Q3, we have analyzed whether the three evaluated CCS implementations appear secure and trustworthy for users. To answer this question, test users have been asked to rate the perceived level of security and trustworthiness for all three CCS implementations. Ratings have again been collected by means of a questionnaire.

Figure 7 illustrates the obtained results for the three evaluated CCS implementations. Again, the Mobile Phone Signature achieved the best results. 84% of all test users rated the Mobile Phone Signature as secure and trustworthy. MOCCA Local obtained only slightly worse results. 74% of all test users perceived MOCCA Local as secure and trustworthy. Analysis of the recorded user sessions and of information extracted from the conducted interviews revealed main reasons for potential suspiciousness. During the

installation process of MOCCA Local, users were asked to install a certificate in the used Web browser. This is necessary in order to establish an appropriate trust relationship between the Web browser and MOCCA Local. Unfortunately, the trust status of the used certificate was not accepted by default by the used Web browser. Hence, test users were faced with a security warning during the installation of this certificate. While most users simply ignored it, some test users were unsettled by the shown security warning.

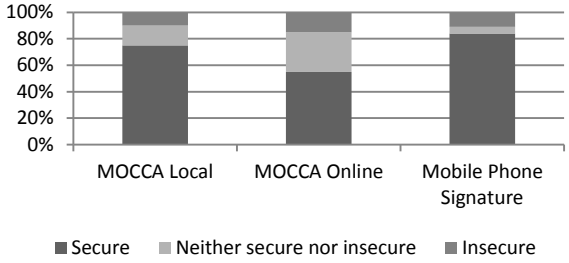


**Figure 7.** Perceived security and trustworthiness of the evaluated CCS implementations.

MOCCA Online obtained the worst ratings regarding security and trustworthiness. Still, 55% of all test users assumed MOCCA Online to be secure and trustworthy. Similar to MOCCA Local, suspiciousness was mainly caused by shown security warnings. Since the Java Applet of MOCCA Online accesses local resources (i.e. the user's smart card), the Applet needs to be signed. Again, the trust status of the signing certificate was not accepted by the used Web browser. Hence, a security warning was shown during the loading of the Applet.

To answer Research Question Q3 we can conclude that users basically attested all three CCS implementations an appropriate level of security and trustworthiness. Still, there is some room for improvement especially for smart card based solutions, which definitely need to improve their handling of SSL certificates. A direct comparison of the three CCS implementations shows that the Mobile Phone Signature appears to be the most secure and trustworthy solution, followed by MOCCA Local and MOCCA Online.

## 4.4 Personal preferences

Personal preferences of individual test users have been identified in the course of conclusive interviews. All test users have been asked whether they will continue to use their Citizen Card and which of the three tested CCS they prefer. Most test users have been convinced of the Citizen Card and stated to use it in the future for e-Government procedures. Regarding the preferred CCS, the Mobile Phone Signature has turned out to be the favored alternative. Figure 8 illustrates the obtained results. The Mobile Phone Signature has been selected by more than 50% of all test users to be the favored CCS. 20% of the test users stated that MOCCA Online is their preferred solution. For approximately 15%, MOCCA Local is the favored implementation alternative. In order to answer Research Question Q4, we can conclude that the Mobile Phone Signature is definitely the favored CCS implementation for citizens.

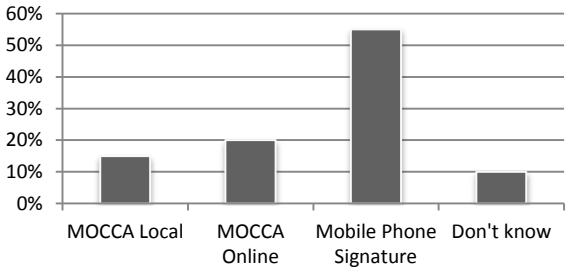


**Figure 8.** Preferred CCS implementation.

## 5. CONCLUSIONS

The goal of this work was to evaluate the usability of three core components of the Austrian e-Government infrastructure. Four research questions have been defined to cover relevant usability aspects. In order to answer these questions, a thinking-aloud test has been conducted. By analyzing the data that has been collected during these tests we were able to find appropriate answers to all previously defined research questions. In general, the conducted usability test revealed the following basic findings:

- The need for local software installation represents no serious barrier for users. However, the provided routine for the installation of certificates should be improved.
- All evaluated CCS implementations could be used without major problems and have been rated positively in terms of usability. The Mobile Phone Signature is the clear winner and appears to be the most usable solution for most test users.
- All evaluated CCS implementations have been rated positively regarding security and trustworthiness. Unsettledness has only been caused by the use of certificate with missing trust status. The Mobile Phone Signature has obtained the best ratings regarding security and trustworthiness.
- In general, the Mobile Phone Signature is the preferred CCS implementation for most test users.

While the two smart card based solutions MOCCA Local and MOCCA Online obtained comparable ratings in most categories, the Mobile Phone Signature turned out to be the clear winner in terms of popularity, security, trustworthiness, and usability. Hence, we can conclude that reliance on mobile solutions seems to be a good strategy also for future developments.

The conducted usability test delivered deeper insights into the usability of core components of the Austrian e-Government from the citizen point of view. By observing users' interactions with these components and collecting user feedback by means of different questionnaires we were able to identify persisting weaknesses and further room for improvement. Obtained results will be incorporated into future releases of the evaluated CCS implementations and help to further improve the usability of these solutions.

## REFERENCES


Altameem, T. et al, 2006. Critical success factors of e-government: A proposed model for e-government implementation. Innovations in Information Technology 2006, pp. 1-5.

Boslaugh, S. and Watters, P.A., 2008. Statistics in a Nutshell, vol. 54. O'Reilly.

Centner, M. et al, 2010. Minimal-footprint middleware for the creation of qualified signatures. *Proceedings of the 6th International Conference on Web Information Systems and Technologies*, pp. 64-69. INSTICC, Portugal.

Garcia, A. C. B. C. et al, 2005. A quality inspection method to evaluate e-government sites. *Electronic Government Fourth International Conference EGOV 2005*, pp. 198-209.

Gil-Garcia J. R. and Helbig, N., 2006. Exploring E-Government Benefits and Success Factors, vol. 1, pp. 803-811. Idea Group Inc.

Hollosi, A. et al., 2008. The Austrian citizen card. http://www.buergerkarte.at

Leitold, H. et al, 2002. Security architecture of the Austrian citizen card concept. *Proceedings of the 18th Annual Computer Security Applications Conference, ACSAC '02*, pp. 391-, IEEE Computer Society, Washington, DC, USA.

Ma, T. H. Y. and Zaphiris, P., 2003. The Usability and Content Accessibility of the E-government in the UK, *Human Computer Interaction*. vol. 2007, pp. 760-764.

Orthacker, C. et al, 2010. Qualified Mobile Server Signature. *Proceedings of the 25th TC 11 International Information Security Conference SEC 2010.*

EU Parliament and Council, 2000. Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures. *Official Journal of the European*

*Communities*, L 013:12-20.

Schultz, E. E. et al, 2001. Usability and security an appraisal of usability issues in information security methods. *Computers Security*, vol. 20(7) pp. 620-634.

Sorum, H., 2011. An empirical investigation of user involvement, website quality and perceived user satisfaction in egovernment environments. *Proceedings of the Second international conference on Electronic government and the information systems perspective, EGOVIS'11*, pp. 122-134, Springer-Verlag, Berlin, Heidelberg.