1.08 Objavljen znanstveni prispevek na konferenci
1.08 Published Scientific Conference Contribution

Ksenija LONČARIĆ[*], Hrvoje STANČIĆ[**]

REACHING COMPUTATIONAL TRUST: REQUIREMENTS FOR IMPLEMENTING TRUSTED E-GOVERNMENT

Abstract:

Implementation of e-government requires certain level of transparency and development in order to be successful and trusted. With the improvement of national strategies, regulations and legal framework as a starting point, the competent institutions should take into account security improvements as the most important aspect of achieving trusted e-government. The main goal of achieving the interconnection between different national governmental bodies and services at the transnational level is achieved by exchange of identification and authentication credentials. In this paper the authors introduce the main difficulties the EU countries have in implementing national e-government and achieving the interoperability between e-services.

Keywords:

e-Government, e-service, computational trust, digital records, single sign-on system

Izvleček:

Doseči računalniško zaupanje: zahteve za vzpostavitev zaupanja vredne e-uprave

Vzpostavljanje uspešne, zaupanja vredne e-uprave zahteva določen nivo transparentnosti in razvoja. Za pristojne institucije mora biti najpomembnejši vidik pri doseganju zaupanja vredne e-uprave izboljšanje varnosti, poleg seveda izboljšanih nacionalnih strategij in zakonskih okvirov. Glavni cilj vzpostavitve medsebojnih povezav med različnimi državnimi upravnimi telesi in storitvami na nadnacionalni ravni je dosežen z izmenjavo identifikacijskih in pristnostnih poverilnic. Avtorja v prispevku predstavljata glavne težave, s katerimi se soočajo evropske države pri vzpostavljanju nacionalne e-uprave in pri doseganju interoperabilnosti med e-storitvami.

Ključne besede:

e-uprava, e-storitve, računalniško zaupanje, digitalni zapisi, enojen vpisni sistem

Trust, understanding and respect are key ingredients of successful relationships. Depending on the type and complexity of relationship between two or more cooperative parties, one can argue that these characteristics also represent some of the biggest challenges to overcome. Gaining trust in the seemingly lifeless structure we call technology is not easy and it requires a lot of planning, cooperating and openness to new ideas. The trust relationship between people and information systems is no

[*] *Ksenija Lončarić, Faculty of Humanities and Social Sciences, University of Zagreb, Ivana Lučića 3, Zagreb, Croatia, contact: kloncaric58@gmail.com.*

[**] *Ph.D. Hrvoje Stančić, associate professor, Faculty of Humanities and Social Sciences, University of Zagreb, Ivana Lučića 3, Zagreb, Croatia, contact: hrvoje.stancic@zg.t-com.hr.*

different than the relationships between more conventional types of trustors and trustees. In analogy with meeting new people, the beginning of every association between two parties starts with some shape and form of education. Just like getting to know each other is the first step of every human interrelationship, learning and educating about a certain information system, process or subject is the door to a higher level of trust and understanding. Computational trust goes a step further. Digital revolution has shaped last few generations and made a big impact on the generations before. Distrust, suspicion and scepticism towards technology that prevailed in the 20th century has been reduced but it still remains among the older generation, especially when it is a question of new and improved ways of dealing with more or less traditional problems. Electronic government is a perfect example of the "new" technology bestowed upon us that raises a great deal of scepticism.

1 INTRODUCTION: TRUST CHALLENGES OF ELECTRONIC GOVERNMENT

E-government can be simply defined as a set of activities and roles in the relationship between government(s), businesses and citizens that are carried out by means of information and communication technology (ICT). With the variety of definitions and different terminologies, there are four key characteristics of e-government that should be taken into account. (1) E-government uses ICT and is entirely dependent on it. (2) E-government provides client-oriented services and should be based on a 2-way communication. (3) E-government should have a central point of access to allow (4) successful and secure exchange of information and user's personal data.

Recent research on citizens' attitude towards local e-government by Delitheou and Maraki (2010) has shown that main reasons of previously mentioned mistrust can be separated into two dimensions. The first dimension is related to the concerns and refrains citizens have towards new technology. The research has shown that lack of factual and practical knowledge is one of the main reasons citizens refrain from using e-government systems. Out of 94% of research respondents who were aware of existence of e-government and e-services it provides, only 77% actually make use of the municipal e-services. Furthermore, out of those aware of e-government majority had learnt of it by means of direct communication (49%) or through the Internet (39%) (Delitheou & Maraki, 2010, p. 41). It is important to mention that respondents mainly used e-government to obtain information and not carry out transactions (Heeks, 2006; Delitheou & Maraki, 2010). Other reasons include difficulty of navigation through e-government websites and portals, lack of encouragement from local officials, fear for safety of personal data and wariness in using municipal electronic services (Delitheou & Maraki, 2010).

The second dimension refers to the technological aspects of electronic government as the core reason of citizens' concerns towards e-government. As previously mentioned, research results have shown that citizens mainly use, or have been using, e-government portals and websites to get information and not make transactions. The question of trust and security of personal data now lies in the security and trust mechanisms of e-government and not in the citizen's attitude towards e-

government. Depending on the level of implementation and stages of development, the trust requirements increase accordingly. Thus, e-government services can be compared according to two main aspects of development: level of implementation and maturity of electronic government.

Heeks (2006, p. 9) distinguishes between at least five levels of e-government depending on the size and complexity of the system – local, regional, provincial, national and international level. Size and type of state administration, as two main institutional factors (Moon, 2002, p. 425), determine how e-government will be implemented. According to Heeks (2006), the majority of benchmarking studies have focused on national e-government as the primary mean of electronic communication between citizens and government while the sub-national levels of government are of same or even higher importance to the citizen. In developing countries the local government is the focus of improvement and serves as "the main point of contact for delivery of services and for delivery of national programs" (Amis, 2001, p. 2006 as cited in Heeks, 2006, p. 10). However, with the introduction of government portals as central points of access and single sign-on systems, the difference between sub-national and national levels has been reduced and the implementation projects have become more complex and challenging. Even though the main goal of e-government is to provide citizens with easy, accessible and fast way of executing transactions not all implemented systems have proved to be successful.

2 MATURITY OF ELECTRONIC GOVERNMENT

The second aspect of e-government to be used for comparative analysis is maturity of e-government. From the simple website that allows users to obtain the information to the full-service e-government, the implementation projects do not necessarily go through all stages of development. Accordingly, not all governments share the same number or range of governmental e-services they provide. Almarabeh and AbuAli (2010) distinguish 6 stages of implementation of e-government:

1. *"using internal network and setting up an email system,*
2. *enabling inter-organizational and public access to information,*
3. *allowing 2-way communication,*
4. *allowing exchange of value,*
5. *digital democracy and*
6. *joined-up government" (Almarabeh & AbuAli, 2010, p. 30).*

Layne and Lee's (Layne and Lee, 2001 as cited in Almarabeh & AbuAli, 2010; Delitheou & Maraki, 2010) maturity model focuses on e-government as an evolutionary phenomenon and consists of cataloguing, transactions, vertical and horizontal integration. Cataloguing refers to the overall government online presence that provides users with downloadable forms, contact information and access to the administrative information. Enabling online transactions via web-forms and secure database is a second stage that leads to the vertical and horizontal integration that links and

integrates systems of different levels and across different functions. The final maturity stage is achieved with a functional and secure central point of access and single sign-on system that allows users to securely and easily access e-services.

In the process of implementation of e-government few things have to be taken into account. Firstly, the business model must respond to the needs and wishes of users which are in this case the citizens. In first stages of development, as many authors and researches agree (Almarabel & AbuAli, 2010; Delitheou & Maraki, 2010; Heeks, 2006; Howard, 2001; Iribaren et al., 2008; Moon, 2002), e-government is nothing more than a digital way to inform people about their state administration. Government websites at this stage are designed to provide citizens with basic information about open hours, contacts, forms or structure of an administrative body. This one-way communication enables public access to information but does not provide citizens with enough information or services to become the main channel of communication. Allowing 2-way communication is a step forward towards enabling the electronic transactions between government and citizens and, depending on the type of electronic services that are being provided, these transactions should be secure. Secondly, with integration of different functions and different levels of e-government in the later stages of development citizens expect e-services to be trustworthy and that competent institutions have implemented security improvements. Exchange of identification and authentication credentials between integrated e-services must be the main goal of process optimization and the main way to achieve interoperability of implemented governmental e-services on a national level. However, in order to achieve complete interoperability the legal framework and regulations must be clearly defined.

2.1 InterPARES Trust research results

Each stage of development and implementation requires corresponding level of security. The aforementioned citizens' mistrust towards e-government is led by their fears for safety of their personal data generated by the lack of information. The Croatian research team of the InterPARES Trust project[1] conducted a comparative analysis[2] of selected governmental e-services which has shown that making information available to the public should be the main goal of e-government projects. The research team had adopted a categorization of 20 e-services into two main categories: 12 e-services for

[1] *"InterPARES Trust (2013-2018) is a multi-national, interdisciplinary research project exploring issues concerning digital records and data entrusted to the Internet. Its goal is to generate theoretical and methodological frameworks to develop local, national and international policies, procedures, regulations, standards and legislation, in order to ensure public trust grounded on evidence of good governance, a strong digital economy, and a persistent digital memory." (https://interparestrust.org/) The Croatian research team, led by Ph.D. Hrvoje Stančić, associate professor at the Faculty of Humanities and Social Sciences, consisted of PhD level and graduate level research assistants and project partners – Faculty of Organization and Informatics in Varaždin, Croatian State Archives, National and University Library in Zagreb, University Computing Centre (SRCE), Digital Information-documentation Office of the Government of the Republic of Croatia, Financial Agency (FINA), and Teched Consulting Services.*

[2] *Comparative Analysis of Implemented Governmental e-Services (2014) (Stančić, 2015b).*

citizens (Government to Citizens, G2C) and 8 e-services for businesses (Government to Business, G2B)[3]. The goal was to analyse implemented governmental e-services in the selected EU countries and to present mandatory elements e-services must have to be considered trusted. The results have shown that the key elements of trusted e-services, such as user-oriented service, publicly available information and secure and transparent data protection, were not identified amongst the researched e-services. Many of researched government portals did not contain enough information about citizen's personal data protection, security mechanisms or did not offer any solution to the problem of long-term personal data preservation. Overall, the biggest problem detected was "the absence of publicly available information important for establishing trust in e-services." (Stančić, 2015a, p. 4).

Building on top of the results of the comparative analysis, the research team conducted the analysis[4] of "implemented governmental e-services in the context of national single sign-on systems in order to detect the possibilities of exchanging identification and authentication credentials." (Stančić, 2015a, p. 6). Single sign-on (SSO) systems allow users to gain access to multiple independent systems using unique credential combination without having to authenticate their identity with each new access request. Without SSO system citizens gain access to governmental e-services or other information systems and websites using different kinds of credentials and steps of verification. To avoid having to remember multiple credentials and to reduce the risk of fraudulent actions SSO system is used to achieve interoperability between independent, yet connected, systems. In the context of national governmental e-services, SSO connects national administration bodies in order to raise the level of security by implementing the single point security and trust mechanisms.

2.2 Electronic government in the EU

The interoperability analysis has shown that the EU member states' maturity level of the implemented governmental e-services vary greatly on the national level. The research shows that while all member states have implemented some form of electronic government, 19 member states (68%), including Austria, Belgium, Croatia, Cyprus, Denmark, Estonia, Finland, France, Hungary, Italy, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Slovenia, Slovakia and Spain, have reached higher levels of maturity. This includes government portal as a central point of access, integrated single sign-on system that supports client-oriented services, enabled transactions,

[3] *Electronic services for citizens (G2C) include income taxes, job search, social security benefits, personal documents, car registration, application for building permission, declaration to the police, public libraries, birth and marriage certificates, enrolment in higher education, announcement of moving and health-related services. Electronic services for businesses (G2B) include social contribution for employees, corporate tax, VAT (Value Added Tax), registration of a new company, submission of data to the statistical office, custom declaration, environment-related permits and public procurement. This categorization is described in Digitizing Public Services in Europe: Putting ambition into action, a 9th Benchmark Measurement by European Commission from December 2010 (Stančić et al., 2015b).*

[4] *Analysis of the Interoperability Possibilities of Implemented Governmental e-Services (2014-2015) (Stančić et al., 2015a).*

secure and reliable data protection system and other characteristics of a trustworthy information system. While there are differences in stages of development as well as maturity, electronic governments also differ in services they provide. Croatia, Malta, Portugal had all 12 e-services for citizens connected through their SSO system with Finland and Lithuania as close seconds with 11 connected e-services. Social security benefits, application for building permissions and request and delivery of birth/marriage certificates had highest frequency of electronic implementation. The main problem that the research team has detected is lack of publicly available information needed to ensure that governmental e-services are trustworthy.

E-government benchmark study (2016) has shown that the e-government implementation in Europe has improved since the first assessment in 2012. The progress has been realized and investigated on four benchmarks: user centricity, transparency, cross-border services and key technological enablers. Since 2012, online availability of e-services and online usability has reached 81% and 83% which shows increase of 9 and 4 points. However, the speed and ease of usage did not show as much progress. Transparency benchmark has increased by 8 points in 2014-2015 in relation to the 48% in 2012. Business-related services have shown greater progress than citizen-related services even though "the latter increased more since the first measurement (13 points against 11 for the business)" (European Commission, 2016, p. 5). Finally, the last benchmark has shown that the new technologies, such as mobile internet, are not used to their potential even though they have "a huge impact in terms of usage and applications" (European Commission, 2016, p. 5). Although there have been improvements since 2012, the differences in progress between countries have increased. The standard deviation between best and worst performers has been growing and it is described as a "Digital Diagonal" that joins Baltic, Scandinavian and Central European Countries such as Belgium, Luxembourg, Germany, France, Netherlands and Denmark. Croatia, Slovenia, Hungary, Poland, United Kingdom and other countries remain behind the European average.

While significant efforts have been made to accelerate the modernization of existing government models and implementation of electronic government, not all countries have shown good results. Figures 1-4 show change in performance in EU28+ countries related to the biennial average in absolute performance for 2014-2015 (European Commission, 2016, pp. 30-31). It is clear that some countries such as Malta, Austria, Portugal and Estonia show the highest rankings in almost all benchmarks. The user centricity benchmark measured user-oriented services at national levels. As shown in Figure 1, many countries have shown above average results. Majority of EU28+ countries has measured above average in absolute performance with Malta, Austria, Estonia, Portugal, Finland and Denmark at the top. However, some countries, even though they have measured poorly in absolute performance, have shown some improvements and change in performance. Slovakia has measured well below average in absolute performance but the change in performance in relation to 2012 has been well above average. In cross-border mobility, which is an important element for achieving interoperability on the transnational level, majority of EU28+ countries got relatively average results. Sweden has shown significant progress in performance and was ranked the highest in absolute performance. The lowest ranked countries remained

Romania, Slovakia, Hungary, Greece, Bulgaria, Croatia and others. Transparent government is very important in building the trustworthy structure but the results of this benchmark were not very promising. Majority of countries did not show much improvement over the course of four years and are average or below average in change in performance indicator. Denmark got by far the best results with Island ranking as second. In absolute performance Malta has again gained the best results with little improvement. The lowest average results can be measured in key enablers. The EU28+ countries measured either well above or well below average in both indicators. Key enablers or new technologies and innovations are important in projecting the future for e-government. As such, it is important to make use of available technologies to further expand and improve the existing models. As it has been noted in the study, "the full implementation of SSO functionality (100%) has been achieved by nine countries (Austria, Denmark, Estonia, Spain, France, Island, Latvia, Malta and Portugal)" (European Commission, 2016, p. 32). Electronic identification, authentication services, SSO and other key enablers are necessary and indispensable in building the trustworthy network of governmental e-services.

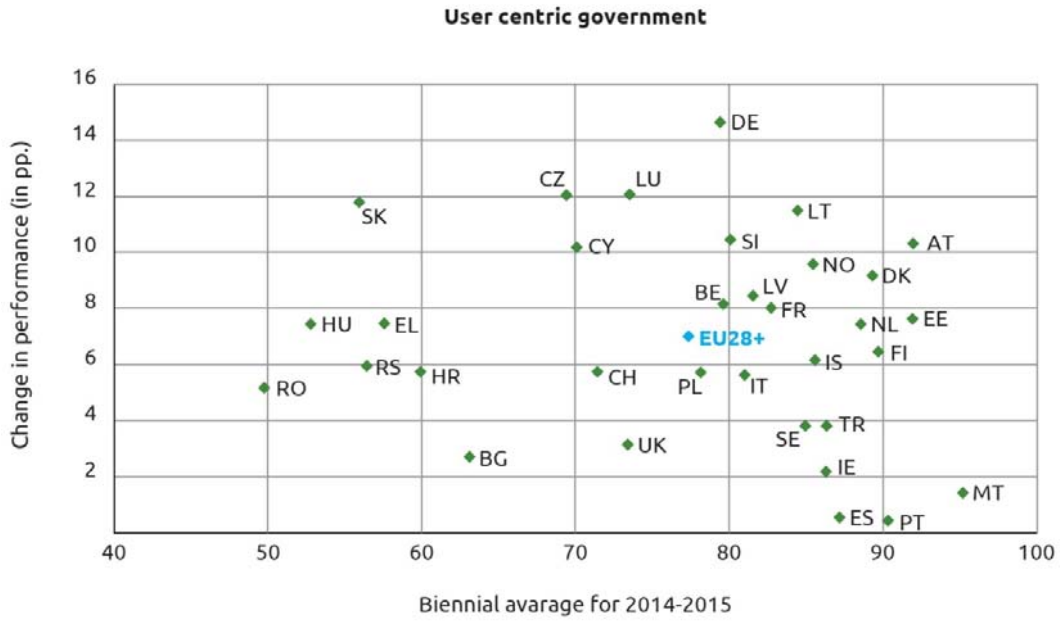

Figure 1. User centricity benchmark

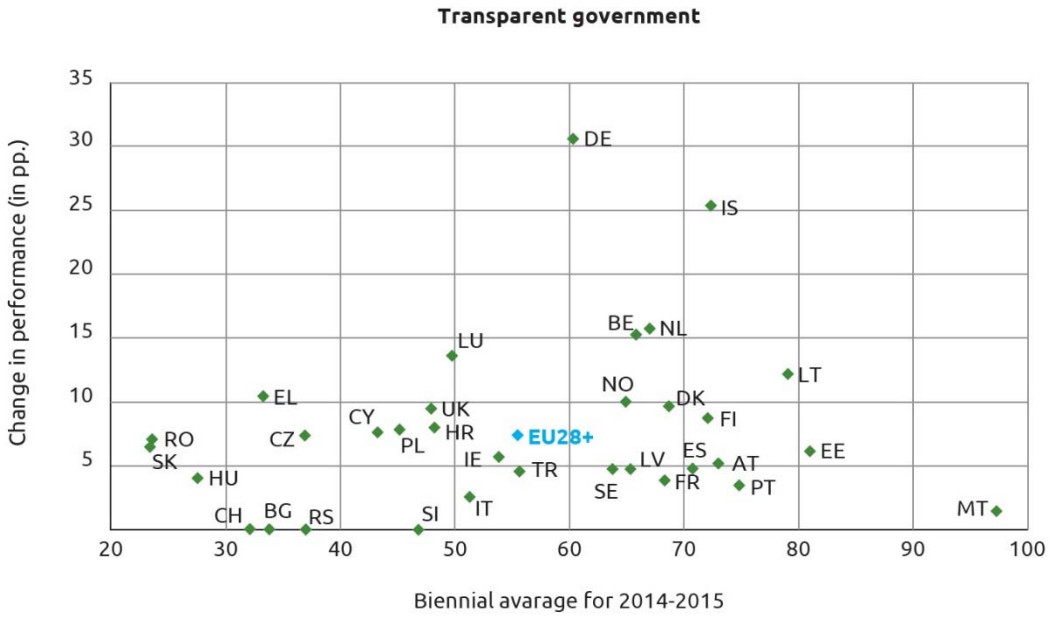

Figure 2. Transparent government benchmark

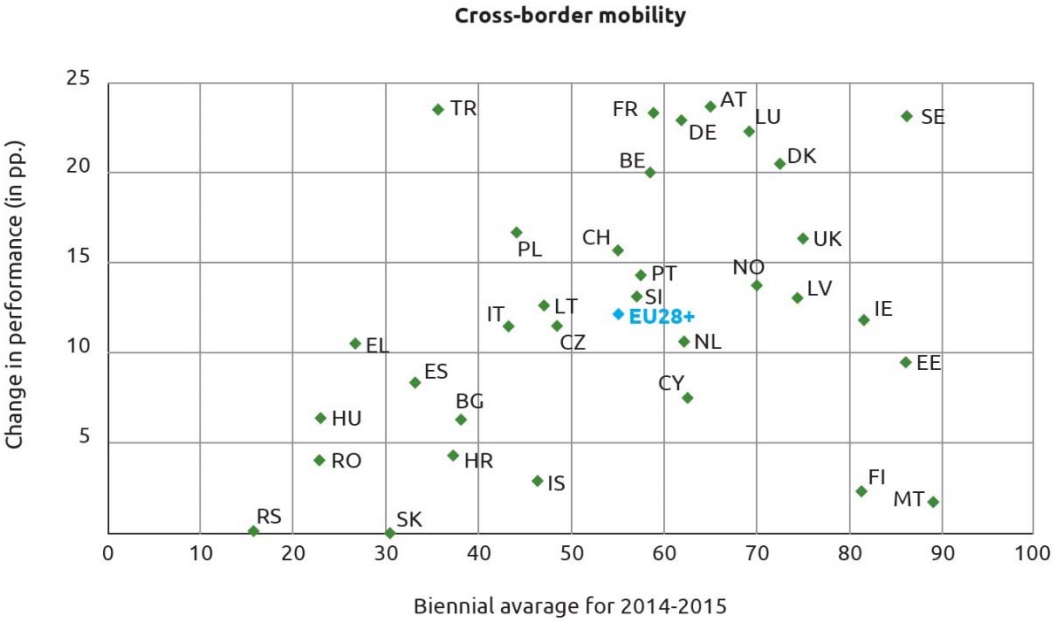

Figure 3. Cross-border mobility benchmark

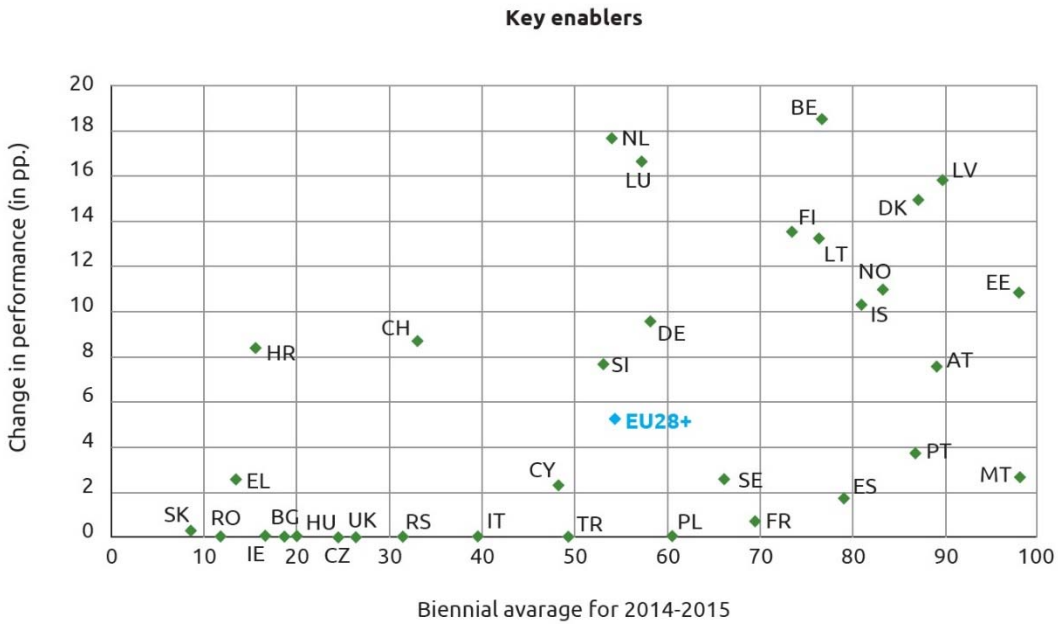

Figure 4. Key enablers benchmark

Overall, EU28+ countries have shown major improvements and steps forward but the "Digital Diagonal", that has been mentioned in the study as one of the problems of uneven modernization and progress, is something European Union as a whole has to work on. Delivery of user-oriented services at national and cross-border levels, as shown in the study, is achieved by simplification and elimination of administration processes by moving them online. Implementation of quality transparent e-services is unfortunately still lacking in large parts of Europe (European Commission, 2016, p. 38). To improve transparency, user centricity, cross-border mobility and to make use of new technologies new policies have to be created and implemented. Some of the obstacles countries have to overcome lie in the legal framework and strategies.

3 CHALLENGES IN LEGAL FRAMEWORK AND STRATEGIES

The InterPARES Trust project's research "Analysis of the Interoperability Possibilities of Implemented Governmental e-Services" has found out (Stančić et al., 2015a) the it is not only important that the users trust SSO systems (and governmental e-services available through them) but also that the SSO systems should trust each other and be able to exchange information. The research of the SSO systems in the 28 European member states showed that the European SSO systems are not yet interconnected. At the time of research, the leading project researching in that direction was the Stork 2 project – the continuation of previous STORK 1 phase. In our opinion the main challenge in the coming years will be to exchange sensitive information in a trusted manner. Illustration of the challenge can be shown by the health-related e-service example of cross-border exchange of patients' information between e-health e-services of different countries when a patient of one country needs a treatment in another country. At that point certain challenges might surface like could the patient limit what information a doctor in a foreign country would be allowed to access? Will certain set-

up limitations still be valid when accessing the data using another country's SSO? Should there be an "override" possibility for the set-up limitations in case of an emergency (e.g. when the patient is not conscious)? Similar situations could surface using other e-services interconnected through national SSO systems.

The mentioned research study has also indicated that the legal framework should not only follow, but be proactively developed along the technical development in order to set the stage, accommodate and regulate cross-border data exchange and SSO interconnections. Therefore, national legal regulations of the European countries will have to be changed or broadened and then harmonized in order to encompass new situations that will be made possible by interconnecting SSO systems at the European level. It is important not only to view the complexity of SSO implementation from the technical point of view, but also to have defined and clear legal regulations and frameworks on national and transnational level in order to provide fully functional, safe and complete interoperability of the interconnected governmental e-services. The first step in that direction might be achieved by enabling the exchange of identification and authentication credentials through national SSO systems. Further steps might involve actual exchange of documents and records.

4 COMPUTATIONAL TRUST

This finally brings us to the issue of computational trust. Chandrasekaran and Esfandiari (2005) differentiate between "social trust" and "trusted third party" trust. They define social trust as "reputation-based trust management systems (which) are based on experiences of earlier direct and indirect interactions". Opposed to that, the trusted third party trust is achieved by the PKI infrastructure and involvement of certification authorities as the trusted third parties. The social trust (and reputation) approach may not be appropriate as the main source of trust with the governmental e-services since it is more informal way of achieving trust. That approach requires users' evaluation and the trust is built upon their opinions and experiences. For example, social trust is important for choosing a more trusted seller on online selling services or a higher quality accommodation with an online hotel booking service. Achieving computational social trust requires modelling of direct and indirect trust, global and local trust as well as risk assessment. This might prove useful for quality or functionality check of a particular governmental e-service but not in the context of computational trust between the services themselves or between national SSO systems. The trusted third party approach is much better for that particular purpose because the exchange of certificates establish the trust between the interconnected services.

The Stork 2 project's Final version of technical specifications for the cross-border interface (2015, p. 97) mention that in the cross-border transfer of documents the two systems may a) invoke a separate validation service and transmit the whole signed document, b) invoke a separate validation service and transmit the hash-value / certificate, or c) implement a full-fledged validation service. The Stork 2 project has

finished before the eIDAS regulation[5] came to power and the mentioned possibilities a)-c) may be achieved by creating "(qualified) trust service" and "(qualified) electronic registered delivery service". eIDAS regulation defines "trust service" as an electronic service which consists of "a) the creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services, or b) the creation, verification and validation of certificates for website authentication; or c) the preservation of electronic signatures, seals or certificates related to those services" (eIDAS, p. 84). A qualified trust service is a service that meets the requirements for the trust service. Further, the "electronic registered delivery service" is defined as "a service that makes it possible to transmit data between third parties by electronic means and provides evidence relating to the handling of the transmitted data, including proof of sending and receiving the data, and that protects transmitted data against the risk of loss, theft, damage or any unauthorized alterations" (eIDAS, p. 86). To be qualified "electronic registered delivery services shall meet the following requirements: a) they are provided by one or more qualified trust service provider(s); b) they ensure with a high level of confidence the identification of the sender; c) they ensure the identification of the addressee before the delivery of the data; d) the sending and receiving of data is secured by an advanced electronic signature or an advanced electronic seal of a qualified trust service provider in such a manner as to preclude the possibility of the data being changed undetectably; e) any change of the data needed for the purpose of sending or receiving the data is clearly indicated to the sender and addressee of the data; and f) the date and time of sending, receiving and any change of data are indicated by a qualified electronic time stamp" (eIDAS, p. 107).

Also, a blockchain-based service may be used as a separate validation service for transmission and verification of the hash-value of documents. Blockchain, or a distributed ledger technology (DLT), relies on a distributed network in which all nodes store information on all transactions. Timestamp is used to confirm the date and time of all transactions – hash-values being entered in the blockchain. The trust is bestowed upon a qualified majority for confirmation of a transaction while the content of the document being transmitted is not disclosed. By using a blockchain solution, whether set up on a public or private blockchain, one can confirm integrity of a document/record, the time of creation/transmission, the sequence of documents/transmissions achieve non-repudiation and improve validation and long-term preservation of digitally signed documents even after their certificates expire[6].

[5] *Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC came to power in all EU member states at 1 July 2016.*

[6] *InterPARES Trust project's study "Model for Preservation of Trustworthiness of the Digitally Signed, Timestamped and/or Sealed Digital Records (TRUSTER Preservation Model)" is addressing this issue.*

5 CONCLUSION

While developing e-services, governments should plan not only to offer online equivalents of the paper-based processes but new functionalities appropriate to the digital environment. Of course, a big step forward is making information available online, making it possible to get certain documents in the electronic form or use governmental e-services in order to speed up the process of issuing required documents. However, not all e-services are connected in a sense of exchange of data even if citizens can access them using a Single sign-on system. In some cases, as it was confirmed in the comparative analysis of implemented governmental e-services, e-services do not exchange data. Further step that has yet to be achieved is interconnection of governmental e-services among the EU member states. That could be achieved by interconnection of national SSO systems. In order to do that the computational trust mechanisms has to be developed and implemented. eIDAS regulation has laid grounds for that, although for certain aspects the blockchain-based technologies might be used. By taking steps in that direction the trusted e-government seems as an achievable goal.

REFERENCES

- Almarabeh, T. & AbuAli, A., 2010. A General Framework for E-Government: Definition, Maturity Challenges, Opportunities and Success. *European Journal of Scientific Research,* 39(1), pp. 29-42.
- Brown, D., 2005. Electronic Government and Public Administration. *International Review of Administrative Sciences,* 71(2), pp. 241-254.
- Chandrasekaran P. & Esfandiari B. (2015). Toward a testbed for evaluating computational trust models: experiments and analysis. *Journal of Trust Management 2:8*, 1-27.
- Delitheou, V. & Maraki, M., 2010. Research into citizens' attitude towards electronic municipal services (e-local government). *Journal of Public Administration and Policy Research,* 2(3), pp. 39-45.
- eIDAS – Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. Retrieved 15. 1. 2017 from http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0910&from=EN.
- European Commission, 2016. *eGovernment Benchmark 2016: A turning point for eGovernment development in Europe,* s.l.: European Commission.
- Final version of technical specifications for the cross border interface. (2015). Stork 2 project. Retrieved 15. 1. 2017 from https://www.eid-stork2.eu/index.php?option=com_phocadownload&view=file&id=64:d411-final-version-of-technical-specifications-for-the-cross-border-interface&Itemid=174.
- Heeks, R., 2006. *Understanding and Measuring eGovernment - International Benchmarking Studies.* Budimpešta, Mađarska, s.n., pp. 1-44.
- Iribaren, M. et al., 2008. Capability Maturity Framework for e-Government: A Multi-dimensional Model and Assessing Tool. *International Conference on Electronic Government,* pp. 136-147.

- Moon, J., 2002. The Evolution of E-Government among Municipalities: Rhetoric or Reality? *Public Administration Review,* 62(4), pp. 424-433.
- Stančić, H. et al., 2015a. *Analysis of the Interoperability Possibilities of Implemented Governmental e-Services.* Retrieved 15. 1. 2017 from https://interparestrust.org/assets/public/dissemination/EU15_20160727_InteroperabilityGovEServices_FinalReport.pdf.
- Stančić, H. et al., 2015b. *Comparative Analysis of Implemented Governmental e-Services*. Retrieved 15. 1. 2017 from https://interparestrust.org/assets/public/dissemination/EU09_20160727_ComparativeAnalysisImplementedGovernmentaleServices_FinalReport.pdf.

POVZETEK

DOSEČI RAČUNALNIŠKO ZAUPANJE: ZAHTEVE ZA VZPOSTAVITEV ZAUPANJA VREDNE E-UPRAVE

Implementacija uspešne in zaupanja vredne e-uprave zahteva določen nivo transparentnosti in razvoja. Na državni ravni je bilo nekaj vidnih poskusov informiranja in izobraževanja javnosti o novih in izboljšanih načinih komunikacije z vladnimi telesi. Raziskave so pokazale, da je za pridobitev zaupanja državljanov v e-storitve potrebno zagotoviti zanesljive in zaupanja vredne informacije o zaščiti in varnosti osebnih podatkov. Poleg izboljšanih državnih strategij in zakonskih okvirov morajo pristojne institucije upoštevati varnostne izboljšave kot najpomembnejši vidik doseganja zaupanja vredne e-uprave. Na vprašanje računalniškega zaupanja na državnem nivoju bi moralo biti odgovorjeno v kontekstu procesa optimizacije kot tudi doseganja interoperabilnosti implementiranih e-storitev.

V kontekstu transnacionalne implementacije vladnih e-storitev se zahteva nov pristop. Zasebnost in varnost osebnih podatkov državljanov, prenos občutljivih informacij, pristojnosti posameznih državnih institucij, pripadajoči mehanizmi zaupanja in potreba po široki, vendar natančni zakonodaji so le nekateri od glavnih problemov pri doseganju računalniškega zaupanja. Glavni cilj vzpostavitve medsebojne povezave med različnimi državnimi vladnimi telesi in storitvami na nadnacionalnem nivoju je možno doseči z izmenjavo identifikacijskih in overjenih poverilnic.

V prispevku avtorja predstavita glavne težave držav EU pri implementaciji državnih e-vlad in doseganju interoperabilnosti med e-storitvami. Podata niz zahtev in priporočil za implementacijo zaupanja vredne e-vlade na nadnacionalnem nivoju. Avtorja menita, da lahko pristojne institucije uporabijo predlagane zahteve kot izhodiščno točko za vzpostavitev zaupanja v e-storitve.