Policy and Legal Environment Analysis for e-Government Services Migration to the Public Cloud

Taavi Kotka
Tallinn University of Technology
Akadeemia tee 15A
Tallinn, Estonia
taavi.kotka@gmail.com

Laura Kask
Ministry of Economic Affairs and Communications
Harju 11, Tallinn, Estonia
laura.kask@mkm.ee

Karoliina Raudsepp
Ministry of Economic Affairs and Communications
Harju 11, Tallinn, Estonia
karoliina.raudsepp@mkm.ee

Tyson Storch
Microsoft Corporation
1 Microsoft Way
Redmond, Washington, USA 98103
tyson.storch@microsoft.com

Rebecca Radloff
Microsoft Corporation
Konrad-Zuse-Str.1
85716 Unterschleißheim, Germany
rebecca.radloff@microsoft.com

Innar Liiv
Tallinn University of Technology
Akadeemia tee 15A
Tallinn, Estonia
innar.liiv@ttu.ee

ABSTRACT
There are many benefits associated with migrating E-government services to cloud computing: continuity of operation, flexibility, a reduction in infrastructure needs and the ability to drive innovation with cloud-based data services. However, the policy and legal environment in which this migration is pursued can present unanticipated obstacles and slow down public sector innovation. The goal of this paper is to analyze the policy and legal environment in Estonia in order to understand its implications for the migration of Estonian E-government services to a government cloud.

CCS Concepts
• Applied computing~E-government

Keywords
Government Cloud; e-Government; Virtual Data Embassy; Digital Continuity; Policy Assessment; Roadmap

1. INTRODUCTION
According to International Data Corporation [1], 70% of private sector chief information officers in 2016 consider cloud-based delivery the preferred choice when implementing new services. Corporations are rapidly adopting cloud computing because of the speed, scale, and economic benefits it offers. Governments are following suit [2],[3],[4] and exploring the role cloud-based services can play in: creating scalable, interactive citizen portals; facilitating collaboration; delivering volumes of data to citizens in useful ways; and maximizing the focus on mission-critical needs while reducing ICT costs [21]. They need, however, to be sure of the security, resilience and trustworthiness of the services [21-23] they run "in the cloud."

ICEGOV '15-16, March 01 - 03, 2016, Montevideo, Uruguay

ACM 978-1-4503-3640-6/16/03…$15.00
DOI: http://dx.doi.org/10.1145/2910019.2910056

In 2013, the Estonian government began pursuing a Data Embassy Initiative. The project is in keeping with Estonia's innovative approach to e-government and grew out of its need to ensure national digital continuity no matter what [5]. Cloud computing [6], with its immense opportunities for resiliency, security and continuity in the face of physical or cyber emergencies, was a potential solution. In September 2014, the Ministry of Economic Affairs and Communications, the Ministry of Justice (Center of Registers and Information Systems), and the Office of the President of Estonia agreed with Microsoft to work on a research project to assess the feasibility of the virtual aspects of the Data Embassy Initiative [5]. In particular, the collaborative project tested how two separate government services – the official web site of the *President of Estonia* (www.president.ee) and the *Riigi Teataja*, or electronic *State Gazette* (www.riigiteataja.ee) – could be migrated and hosted on the Microsoft Azure™ cloud computing platform.

Particular attention was given to the legal protections Virtual Data Embassies could potentially enjoy. This consideration was crucial since the success of the initiative fundamentally depends on the ability of citizens to trust the security and privacy [22,23] of such embassies. Promoting and maintaining citizens' trust in Virtual Data Embassies is particularly difficult, because there are multiple actors who could access the data. Citizens must trust not only the Estonian state, but also its decision to rely on cloud service providers located in different foreign states.

The possibility of moving state infrastructure to the cloud has recently gained substantial interest and attention [7-9], [12-16]; the interested reader is referred to several extended surveys and comparisons [17-19].

The main goal of this paper is to analyze the policy and legal environment in Estonia with the respect to the migration of E-government services to the government cloud.

The paper first introduces the general idea of the data embassy initiative (Section 2). Next it presents an overview of domestic (Section 3.1) and international policy (Section 3.2) relevant to the data embassy initiative. Finally, it highlights issues (Section 3.3) related to the status and prospects for data embassies under national and international law.

2. THE DATA EMBASSY INITIATIVE
Estonia is highly dependent on information technology. Estonian citizens are able to perform nearly every public and private sector

transaction in digital form, and a vigorously implemented "paperless" policy means that some essential registries, e.g. the land registry, only exist digitally and only have evidentiary value in digital form. Moreover, its innovative approach to e-identity for non-residents signals the beginning of Estonia's transformation into a "country without borders." As a result, Estonia needs to reassure not only its citizens but also its e-residents [20] of the viability and durability of the state itself and of their status within it, even in the face of cyber-attacks, natural disasters and other national or internal emergencies. Such trust in ICT is not easily won, however, and is even more difficult to maintain.

This requires more than just the preservation of critical data sets and ICT services on Estonian physical territory. A solution needs to be developed for situations, admittedly improbable, during which the Estonian state might need to operate some services outside its current borders. This is the Estonian government's concept of "digital continuity" in the context of the development of e-government [5]. In 2013, the Data Embassy Initiative emerged as a possible answer. A data embassy is defined as a physical or virtual data center in an allied foreign country that stores data of critical government information systems and mirrors of critical service applications.

2.1 Three Core Elements

In essence, the Initiative [5] consists of additional security measures that would allow Estonia to ensure continuity in government and operations, including: digital and data continuity (backup); data integrity (non-repudiation); and core government services in the event of a physical or cyber emergency. To achieve these goals, Estonia plans a three-part solution consisting of:

i) the maintenance of data backups and live services within Estonia's borders (*Government Operated Cloud*);

ii) backups at physical Estonian embassy locations or dedicated data centers in friendly countries chosen by the government (*Physical Data Embassy*);

iii) backups of non-sensitive data in private companies' public cloud (*Virtual Data Embassy*). All three parts of the Initiative should be seen as complementary to one another.

Within the government-operated cloud, Estonia plans to have additional data centers and backups for e-government services located within its physical borders. However, the concept of digital continuity, requires that the official versions of services, including government services like the State Gazette, are available and can be used as well as updated in real time and in all circumstances.

The Physical Data Embassy is a server resource that is completely under Estonian government control but located outside of Estonia's physical borders, provides additional measures of security. The Physical Data Embassy includes two approaches, both currently under exploration. The first would utilize government cloud solutions that have been developed by Estonia's closest allies. For instance, Estonia could selectively sign bilateral agreements to procure existing cloud computing in dedicated data centers of an allied country. The second option, further elaborated in the international policy section below, seeks to use existing Estonian embassies to house backups for registries, taking advantage of the embassies' established diplomatic status. This approach would extend Estonian jurisdiction to the e-government services in question and ensure that they are afforded the same protections, including immunity, as a physical embassy, consulate, or ambassadorial residence. Indeed, transforming server rooms in physical embassies into data embassies would allow Estonia to create a network that would ensure its digital continuity, even in the face of determined efforts to damage it or take it offline completely.

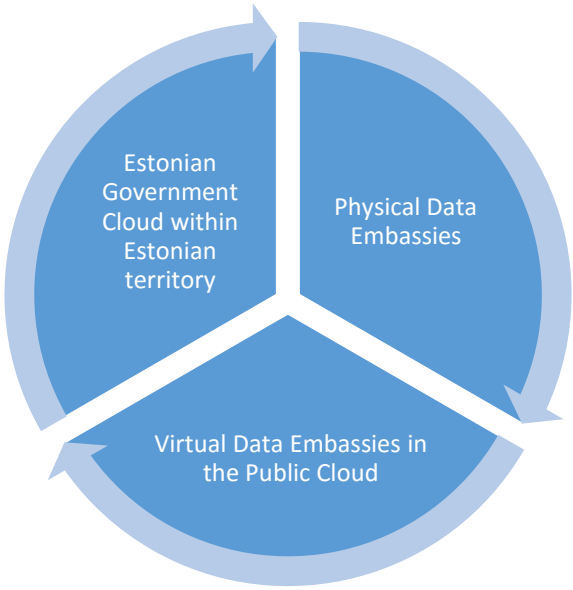

Figure 1. Three core elements of the Data Embassy Initiative.

The third element of the initiative, the Virtual Data Embassy Solution – seeks to further augment digital continuity by using appropriate commercial cloud computing products and services as an additional security measure for Estonian e-government services. This aspect forms the core of this report, which focuses on the feasibility of such an approach, explores solutions to challenges encountered, and identifies a number of benefits that the solution would offer. Notably, while Virtual Data Embassies might offer a higher guarantee of availability, certain data or services (i.e. those pertaining to state secrets) may not, at present, be hosted in a privately-owned cloud service due to data protection, privacy, and data integrity concerns. Nevertheless, while the use of public clouds does not eliminate all risk, their capacity to deal with the most widespread cyber-attacks currently exceeds that of many organizations. Moreover, their location outside of the physical borders of Estonia and within the global cloud environment makes the public cloud well suited to meeting the digital continuity goals of the Virtual Data Embassy Solution.

3. POLICY AND LEGAL ENVIRONMENT

There are no legal restrictions under existing Estonian domestic law against migrating government services to a Virtual Data Embassy in a public cloud, with limited exceptions. These include data relating to "critical" services, as defined by the Emergency Act. It was also established that the Estonian data in a Virtual Data Embassy could be protected under international law from compelled disclosure. To enable migration of government services with restricted data, however, changes to laws must be addressed, for example to clarify digital continuity. Furthermore the migration of restricted data raises other legal issues that have not been specifically addressed in domestic law and international practice.

In particular, the Virtual Data Embassy Solution is unique because it seeks to be recognized by the international community as having legal protections associated with diplomatic and consular missions

while applying these protections to novel technologies and circumstances. It applies existing international laws, many of which are based in treaties that were ratified nearly fifty years ago, in new ways, and its success depends on acceptance by governments around the world. This means that the research project had to examine not only the feasibility of the technical implementation, but also its legal feasibility, in particular with regard to the availability of diplomatic, consular and sovereign immunities for data stored on the Virtual Data Embassy. The following sections address this question, taking as starting points the legal and policy landscapes in Estonia, and internationally.

3.1 Domestic Policy and Legislative Environment Overview

Estonia is a pioneer in e-government and ICT adoption and use. This has been true both in terms of technological and legislative adoption. Over the last decade, Estonia has continuously fostered an inventive and forward-thinking legislative environment to support its commitment to a digital society. The basic policy documents governing e-government in Estonia, as identified by the Project team, are the Principles of the Estonian Information Policy, approved in 1998, and reviewed in 2005 and 2010. In 2007, the Estonian Information Society Strategy 2013 entered into force, for the first time clearly setting out the government objective of developing information society in the country as a strategic choice. In late 2012, the government built on the document with the Estonian Digital Society Strategy 2020, committing the country to a dramatic leap forward when it comes to e-government, with the introduction of concepts such as virtual data embassy, digital identity, and virtual residence for non-citizens [20].

In addition to these e-government policies, successive Estonian governments have adopted and implemented various security policies and frameworks. The first such policy was the 2005 Information Security Policy, which was implemented as Estonia was conducting its first e-elections. It was updated in 2009. Another notable framework is the 2008 System of Security Measures for Information Systems, which establishes security measures for information systems processing data in state and local government databases and for related information assets. The 2013 Security Measures for Vital Service Information Systems and for the Related Information assets establishes that a provider of a vital service must ensure the constant application of security measures and the reporting requirements for institutions. Concurrently, the National Cybersecurity Strategy was adopted in 2007 with a review published in the summer of 2014. The latter outlines the government cybersecurity objectives, including those for the Virtual Data Embassy Solution.

In 2008, Estonia also adopted ISKE (a Three-Level IT Baseline Security System), a system of security measures for information systems that contain and process non-state secret data in state and local government databases. ISKE establishes procedures for the specification of security measures, creating a three-level baseline security system for high-, medium-, and low-risk systems, as well as describes organizational, physical and ICT security measures for protecting data. ISKE is based on IT-Grundschutz, a German standard that complies with the ISO 27000 family of standards, while offering granular technical information to support implementation. While ISKE largely maps to IT-Grundschutz, the Information Systems Authority, the Estonian regulatory authority that manages ISKE, has added some Estonia-specific content. In particular, ISKE contains additional content that is relevant to Estonia's national identification cards and X-road.

In addition to Estonia's ICT development and information security policies, the Estonian laws which guide government actions during emergencies are also relevant in the context of the Virtual Data Embassy Solution. This is important for the concept of digital continuity, in particular to establish when the usage of the Virtual Data Embassy would be activated to ensure continuity of government services during different types of emergencies. Estonian legislation recognizes three levels of emergency: a state of war, a state of emergency, and an emergency situation. Firstly, during a state of war, the War-Time National Defense Act (1994) applies; in addition, the Emergency Act (2009) applies to the extent that it does not conflict with the former. Secondly, during a state of emergency, the State of Emergency Act (1996) applies. Thirdly, during an emergency situation, only the Emergency Act (2009) applies.

3.2 International Policy and Legal Environment Overview

This section considers certain international laws that might apply to Estonian government data and critical services hosted in data centers located outside Estonia's physical borders and owned and operated by a third-party provider. When considering government data hosted with a third party, including a cloud service provider, numerous areas of international law are potentially relevant. These include sovereignty, data protection, data custodianship, diplomatic protection, consular protection, and sovereign immunity. This research project recognizes that while many international laws pre-date the internet and additional work between governments is needed to address previously unanticipated circumstances, existing laws can be applied to cover new technologies and circumstances.

This is a complex area, particularly as the data is owned by a sovereign. Although Estonia could present a well-founded argument that its data is protected from compelled disclosure, the untested state of the law makes it impossible to be certain whether a claim of international legal protection would be respected, either by the host state or by third-countries. The questions of whether the protection afforded is that of an embassy or consular facility and whether Estonia seeks protection as an extension of the sovereign state itself also pose challenges. This underscores the need for an international legal framework, based on the principles of transparency, due process, and respect for human rights and privacy, which sets out clear processes for governmental access to the data in the cloud.

Estonia could pursue several options in order to protect its data. The Vienna Convention on Diplomatic Relations (VCDR) and/or the Vienna Convention on Consular Relations (VCCR) could be applied. For example, Article 24 of the VCDR provides that "the archives and documents of the mission shall be inviolable at any time and wherever they may be." This could apply to modern storage methods, including those that store government data outside of embassy premises. It follows that Estonia could have a solid basis to argue that data associated with its diplomatic mission should retain this protection even when held by a third-party cloud provider. Indeed, the U.S. State Department's position is that documents can retain their Article 24 protection when in the hands of third-parties acting as an agent or contractor to the state (the reader is referred to [11] 198-88).

Similarly, Article 33 of the VCCR provides that archives and documents "of the consular post" are inviolable. The VCCR's definition of consular function includes a notable catch-all for "any other functions entrusted to a consular post by the sending state," provided the host state does not object. Estonia might also seek

protection of its data under the customary international law principle of sovereign immunity. The doctrine has been interpreted to extend to all non-commercial property of a state situated abroad, so the government could assert that its data is considered "non-commercial property" situated abroad in a data center located outside of Estonia. As regards all of these issues, the Virtual Data Embassy presents novel circumstances, and hence there is no clear precedent for the application of these various protections to the particular circumstances.

Clearly, foundations exist that support extending a sovereign's right to the inviolability of its data to the internet and cloud storage. Governments around the world need to begin to come together in support of an interpretation of both treaties and customary international law that recognizes sovereign data protection rights and obligations.

3.3 Findings

Although Estonia has a well-developed ICT policy landscape, it has not yet adopted an overarching cloud computing policy. Nevertheless, recalibrating Estonia's existing information assurance frameworks might be prudent, as cloud computing dramatically changes the ways in which data moves across platforms, devices, services, and borders. The primary drivers for legislative reform are the digital continuity concept, which is central to the Data Embassy Initiative, and the need to operate some services outside Estonia under other circumstances, e.g. for e-residents [20]. In the following sub-sections, we discuss the conclusions of the research project across three policy areas: security; data protection; and, digital continuity.

3.3.1 Information Security Provisions

When analyzing security provisions, the research project focused on the ISKE standard, highlighted above. ISKE is based on the German IT-Grundschutz and sets the standard that helps the government estimate its availability, integrity and confidentiality needs. Similarly to IT-Grundschutz, ISKE is applicable to cloud computing but does not specifically address it. Moreover, ISKE's application to cloud services might be challenging because the output of the methodology it outlines is a collection of specific security measures. Requiring cloud service providers to implement these would eliminate the opportunity to take advantage of the cloud service provider's most up-to-date resources and expertise. As a result, an update of ISKE's auditing provisions might be necessary.

In the interim Estonia should continue to leverage ISKE to evaluate all the components of its information domain that are external to the cloud system, e.g. the network, client systems and software. This would allow the public cloud system to be treated as an independent component. This approach is also supported in IT-Grundschutz for components that cannot be adequately modeled using the catalog or that were not foreseen in the standard's scope [12]. This means that a supplemental security analysis for the cloud service component would be needed to verify that the cloud service provider successfully meets specific security objectives. This could for example be aligned with ISO/IEC 27001/2. Specifying the security requirements at the level of the security objectives would allow cloud service providers flexibility in implementing controls that match today's evolving threat environment.

3.3.2 Data Protection

As highlighted above, two legislative documents govern data protection in Estonia: the Personal Data Protection Act and the Public Information Act. Together they dictate how different types of Estonian public sector information can be handled. For example, information with no restrictions placed upon it (Article 28 of Public Information Act) could be stored in the cloud. However, per Chapter 5 of the Act, this is not true for all public sector information. For the latter, justified interest in doing would have to be demonstrated. For personal data further restrictions on cloud usage may be introduced. Hosting the data in the Estonian Government operated cloud on servers located within embassies abroad would ensure the security of this type of data and achieve compliance with the Data Protection Act.

Another important point to consider is that existing law stipulates that the cloud provider, for example the provider of the Virtual Data Embassy, must become an authorized processor of data and therefore must comply with the instructions of the chief processor. According to Public Information Act (Article 43), the chief processor of a database is the state or local government agency, other legal person in public law or person in private law performing the public duties requiring the introduction of the database and the administration of services and data. They may also, based on a procurement contract or a contract under public law, authorize a person in private law to perform the tasks of processing of data and housing of the database. This means, as there is not a direct mandate for the outsourcing of database hosting to the private sector, an amendment to Public Information Act might be advisable.

3.3.3 Digital Continuity

The research project examined whether there is a need for new legislation to be introduced to enable the implementation of the Virtual Data Embassy Solution, e.g. a Digital Continuity Act, or whether an amendment of existing rules, e.g. to the Emergency Act (2009), would suffice. The challenge of any such legal framework would be to ensure the *de jure* "complete preservation and persistence" of Estonia and its *de facto* functioning, to a certain extent, in the cloud. Since the Virtual Data Embassy solution requires putting data outside of Estonia's territory, developing legal framework to ensure de jure and de facto functioning may present unique challenges.

The analysis determined that the Emergency Act already sets out the guidelines for behavior in case of an emergency (Article 2), i.e. the government should form a permanent crisis committee. This committee could act as the authority that has the right to activate the mechanisms for digital continuity. However, even with the appropriate authority established, further and more in-depth analysis is warranted on emergency procedures to be put in place. The Emergency Act has clear processes to analyze the likelihood of emergencies and the tools and capabilities needed for an effective response. The Estonian government could engage in an effort to understand the scope and extent of its ICT needs currently being met through the vital services set forth in Article 34. It is equally necessary to grasp nascent emergency needs and capabilities, which may not yet be so vital as to require "the continuous operation of a vital service…. [and] the consistent functioning of the organizer of the vital service and the ability to restore the consistent functioning after an interruption." An amendment of the Act to facilitate this capability for emerging needs could benefit Estonia in a number of areas beyond the scenarios involving ICT, such as medicine, public health, and transportation.

Article 7 of the Emergency Act already lays out the need for an Emergency Response Plan, but the text of the Act is silent as to the scenarios for which a response plan shall be prepared. Some governments have specifically incorporated ICT into their national

response plans, recognizing that technology is going to play an important role in a major emergency. This might be appropriate here as well, since many government services in Estonia only exist in digital form. Thus, it is particularly important that they are restored immediately to minimize any disruption. The Emergency Response Plan, alongside other methods for ensuring continuity, creates qualitatively better opportunities for de jure preservation of the Republic of Estonia and also provides certain opportunities for the state to partially function de facto.

Ensuring digital continuity requires more than the preservation of critical data sets and ICT solutions on Estonian territory. The need may arise for operating some services outside of Estonia's borders and the ultimate challenge for digital continuity is to develop a solution where the Estonian state would endure despite a volatile security situation. Simply defining the guidelines for behavior in line with the Emergency Act might be insufficient and the implementation of the Digital Continuity Act could be necessary. If a volatile international security situation were to arise, the Digital Continuity Act would ensure the de jure "complete preservation and persistence" of Estonia and its de facto if limited functioning in the Government Cloud. It would also ensure the functioning of the Government Cloud in parallel with the state's regular information systems.

Digital continuity is particularly important for managing data back-up and service functionality in different national security situations. A legislative framework focusing on digital continuity should, for example, define the circumstances under which critical data and services need to be operational and backed up from outside of Estonia, and which services need to be operational from outside the country within 24 hours in case of a serious threat to Estonian security. The activation mechanisms for defining those conditions should be established in a manner similar to the War-Time National Defense Act. In addition, a procedure needs to be determined for regulating the instance a secondary site becomes the primary site, and if and when the database is switched back to Estonia's physical territory.

The need to act will depend on the level of threat. For instance, a substantial database stored within Estonia's borders during peacetime due to its restricted content, might need to be migrated to the Virtual Data Embassy in an emergency because armed conflict would outweigh the risks of international legal uncertainty regarding the status of the Virtual Data Embassy. Three national security environments could initially be used to define data storage and service functionality:

- **Full Control**: Under the full control mode of operations, the Estonian government operates from within its territory in-country and the core ICT operational staff has no constraints with regard to their physical location or logical ability to access computer services.
- **Fragile Control**: Under the fragile control mode of operations, the Estonian government operates from within its territory but the core technical and policy staff may have constraints with regard to their physical location or logical ability to access computer services. For example, this could be due to a significant cyber-attack or a volatile security situation.
- **No Control:** Under the no control mode of operations, the Estonian government operates outside of its territory and it is expected that the core technical and policy staff may have multiple constraints on their physical location or logical ability to access computer services. In this scenario, the Data Embassy must be fully able to support a "failover to cloud" procedure that leaves the properly elected officials in control of the entity and computing resources that represent Estonia's government and society.

In addition to the above, data access and levels of restriction must be considered in the context of digital continuity. For example, a government could choose that certain sensitive information, such as state secret data, is not to be stored in a privately owned public cloud due to the risk profile of the data. However, if digital continuity is under threat, for instance due to a change in the level of control, such circumstances may necessitate operating government services from the cloud, including those services with sensitive data.

Estonia already operates a central catalog for all of its national information systems, which should be updated to include information about the effect different security situations have on digital continuity. Moreover, information about the frequency and speed of data backups and the appropriate data center types should be included in the classification. This applies to data as well as services. Such classifications would allow the government to determine which registries and services can utilize privately owned public cloud services.

3.3.4 Evolving International Law

The research project's analysis demonstrated a need for broader discussion and agreement on how existing international law enables governments to protect their data when stored in third-party data centers. This new set of policy considerations is an important subset of the broader policy and legal issues arising from government surveillance. This research should encourage governments to respect sensible limitations on their ability to access user data, and to work together to develop a robust, principled and transparent international framework that resolves potential conflicts.

In conclusion, the research project found that it is possible to host Estonian government data and services in servers owned and maintained by a private sector cloud provider. However, in order to enhance the adoption of cloud computing, Estonia should consider limited amendments to existing domestic legislation, particularly regarding critical government services which use restricted data. The level of data involved and its interaction with Estonian data protection rules will be essential. It is also crucial to update the ISKE regulation to include guidelines on hosting data in the cloud. As regards to the international environment, it was found that while legal protection exists, countries may have differing interpretations of the relevant rules under domestic law, and that such varying interpretations could impact the implementation of international legal principles in any specific case. A further effort to develop a globally accepted understanding of the international legal framework in this area should be undertaken.

4. CONCLUSION

There are no legal restrictions under existing Estonian domestic law to migrating government data to a Virtual Data Embassy in a public cloud, with limited exceptions. These include data relating to "critical" services, as defined by the Emergency Act. Data in a Virtual Data Embassy could be protected under international law from compelled disclosure.

The key challenge is that the Virtual Data Embassy Solution has not yet been tested under international law and changes or clarifications to Estonian domestic law might be required in order to support faster adoption of cloud computing. More academic discussion is required on this topic.

5. ACKNOWLEDGMENTS

This paper is based on a section of an unpublished manuscript of a research project on “Public Cloud Usage for Government” and unpublished materials of doctoral dissertation of Taavi Kotka, authors did not receive payment for this publication. Authors wish to thank their colleagues, Lorraine Weeks and anonymous reviewers for helpful comments.

6. REFERENCES

[1] Worldwide and Regional Public Cloud ICT Services 2014-2018 Forecast, 2014, Retrieved November 3, 2014 http://www.idc.com/getdoc.jsp?containerId=prUS25219014

[2] European Commission: European Cloud Computing Strategy. Retrieved November 23, 2015, http://ec.europa.eu/digitalagenda/en/european-cloud-computing-strategy

[3] European Commission: Trusted Cloud Europe. Retrieved November 23, 2015, http://ec.europa.eu/digital-agenda/en/news/trusted-cloud-europe

[4] ENISA: Good Practice Guide for securely deploying Governmental Clouds. Retrieved November 23, 2015, http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/good-practice-guide-for-securelydeploying-governmental-clouds

[5] Kotka, T., Liiv, I. Concept of Estonian Government Cloud and Data Embassies. In *Electronic Government and the Information Systems Perspective: Proceedings of the 4th International Conference EGOVIS 2015 in Valencia, Spain, September 1–3, 2015* (Springer, 2015), Andrea Kő and Enrico Francesconi, (Eds.), 2015, 149-162.

[6] Mell, P., Grance, T.: The NIST definition of Cloud Computing, National Institute of Standards and Technology, Special Publication 800-145 (2011)

[7] Cellary, W. and Strykowski, S. E-Government based on cloud computing and service-oriented architecture. *In Proceedings of the 3rd international conference on Theory and practice of electronic governance (ICEGOV '09)* (Bogota, Colombia, November, 10-13, 2009). ACM Press, New York, NY, 2009, 5-10.

[8] Pokharel, M. and Park, J. Cloud computing: Future solution for e-Governance. *In Proceedings of the 3rd international conference on theory and practice of electronic governance (ICEGOV '09)(Bogota, Colombia, November, 10-13, 2009)*. ACM Press, New York, NY, 2009, 409-410.

[9] Elbadawi, I.Cloud computing for e-government in UAE: opportunities, challenges and service models. *In Proceedings of the 5th International Conference on Theory and Practice of Electronic Governance (ICEGOV '11)*, Elsa Estevez and Marijn Janssen (Eds.). ACM, New York, NY, USA, 2011, 387-388.

[10] Denza, E. Diplomatic Law: Commentary on the Vienna Convention on Diplomatic Relations. Oxford University Press, 2008.

[11] Bundesamt für Sicherheit in der Informationstechnik (BSI), BSI standard 100-4, Retrieved November 23, 2015, http://www.bsi.bund.de/gshb

[12] Wyld, D.: Moving to the cloud: an introduction to cloud computing in Government, 2009.

[13] Gongolidis, E., Kalloniatis, C., Kavakli, E.: Requirements identification for migrating eGovernment applications to the cloud. In: Linawati, Mahendra, M.S., Neuhold, E.J., Tjoa, A.M., You, I. (eds.) ICT-EurAsia 2014. LNCS, vol. 8407, Springer, Heidelberg, 2014, 150-158.

[14] Williams, M.D.: E-government adoption in Europe at regional level. Transf. Gov. People Process Policy 2(1), 2008, 47–59.

[15] Bhiskar, A.: G-Cloud: new paradigm shift for online public services. Int. J. Comput. Appl. 22(8), 2011,24-29

[16] Khan, F., Zhang, B., Khan, S., Chen, S.: Technological leap frogging e-government through cloud computing. In: 4th IEEE International Conference on Broadband Network and Multimedia Technology (IC-BNMT), 2011, 201–206

[17] Gashamia, J.P., Chang, Y., Park, M.-C.: Cross-national study on factors affecting cloud computing adoption in the public sector: Focus on perceived risk. In: Proceedings of Pacific Asia Conference on Information Systems (2013)

[18] Zwattendorfer, B., Stranacher, K., Tauber, A., Reichstädter, P.: Cloud computing in egovernment across europe: a comparison. In: Kő, A., Leitner, C., Leitold, H., Prosser, A. (eds.) EDEM 2013 and EGOVIS 2013. LNCS, vol. 8061, Springer, Heidelberg (2013), 181-195.

[19] Smitha, K.K, Thomas, T., Chitharanjan, K. Cloud Based E-Governance System: A Survey, *Procedia Engineering (International Conference on Modelling Optimization and Computing)*, Volume 38, 2012, 3816-3823.

[20] Kotka, T., Vargas, C., Korjus, K. Estonian e-Residency: Redefining the Nation-State in the Digital Era, *University of Oxford, Working Paper Series - No 3*, September 2015, 1-16.

[21] Feith, G. : Reporting on the outcomes of the CIO network meeting of the 30th of November. In: *eGovernment Conference 2015, December 1-2*, 2015.

[22] Carter, L., Bélanger, F.: The utilization of e-government services: citizen trust, innovation and acceptance factors. Information Systems Journal 15(1), 2005, 5–25.

[23] Welch, E.W., Hinnant, C.C., Moon, M.J.: Linking Citizen Satisfaction with E-Government and Trust in Government. Jnl of Public Admin Research and Theory 15(3) 371–391.