Concept of Estonian Government Cloud and Data Embassies

Taavi Kotka and Innar Liiv(✉)

Department of Informatics, Tallinn University of Technology,
10133 Tallinn, Estonia
taavi.kotka@gmail.com, innar.liiv@ttu.ee

Abstract. Cloud Computing and e-Government are increasingly important topics in state ICT development plans, including that of Estonia. In the course of developing the Estonian Government Cloud concept, it became clear that Estonia's requirements for Cloud Computing are not identical to those of other European states, and that due to its highly developed information society, Estonia needs to expand the previously accepted scope of government clouds. Therefore, the goals of this paper are: to describe and justify Estonia's peculiarities, which define the additional requirements for the development of the Government Cloud and separate us from other states; to offer solutions for how these additional requirements can be resolved in the Government Cloud, and to present the Data Embassy concept; and to present the core implementation plan for constructing the first phase of the Government Cloud concept.

1 Introduction

Public sectors all over the world are facing increasing pressure on budgets and expectations to provide a greater number of public services with better quality. Many of these issues can be solved by cloud computing. It has advantages for the public and as well as the private sector, such as cost effectiveness, flexibility, faster development and testing of new solutions, enabling innovation, etc. Several countries, such as the US, the UK, the Netherlands, Spain, France, India, China, and the Nordic countries, have an agenda for developing cloud computing in the public sector and are actively taking steps towards implementing it (see [6] for a great comparison of eight European countries and [12] addressing adoption). In the public sector it is recognized that cloud computing provides better services with fewer resources.

The European Union is also taking up cloud computing - in September 2012, the European Commission adopted a strategy for "Unleashing the Potential of Cloud Computing in Europe" [1]. The strategy outlines actions to deliver "a net gain of 2.5 million new European jobs, and an annual boost of €160 billion to the European Union GDP (around 1 %), by 2020" [1]. The strategy is designed to speed up and increase the use of cloud computing across all economic sectors in a safe and trusted environment [2].

Although it is too early to evaluate the accuracy of those numbers, given the cost savings and increase in efficiency, scalability and high availability achievable with virtualization, it is clear that governments have a huge potential to benefit by using

A. Kö and E. Francesconi (Eds.): EGOVIS 2015, LNCS 9265, pp. 149–162, 2015.
DOI: 10.1007/978-3-319-22389-6_11

cloud computing. Public data on the uptake of cloud computing shows that in a few years, around 80 % of organizations will be dependent on cloud computing [3].

Therefore cloud computing [4] and e-Government are increasingly important topics in Estonia's ICT development plans. In the course of developing the Estonian Government Cloud concept, it became clear that Estonia's requirements for cloud computing are not identical to those of other European states. Because it already has a highly developed information society, Estonia needs to expand the scope of the Government Cloud. In fact, the Estonian government has been using cloud services offered by large multinational corporations since 2009, when the national tourism website visitEstonia.com was placed in the Amazon cloud. The main reason for cloud hosting was the need for flexible server resource management and the availability of sufficient performance capacity (the application must be fast regardless of where a query is sent from). Also, some Estonian municipalities have been using cloud services, for instance for email services.

Estonia's public sector conducted an analysis of the usage of server resources in 2013 [7], which concluded that the server rooms which are currently spread out among various ministries and buildings need to be consolidated into more efficient datacenters which meet established security standards [8].

The idiosyncrasies of Estonia's information society mandate the innovation of the new Government Cloud. This paper presents the concept of the Estonian Government Cloud with its peculiarities and main principles. The concept includes an action plan for implementing the Estonian Government Cloud.

2 Current Situation and Peculiarities of the Estonian Government Cloud

For at least a decade, researchers have been intrigued by the possibility of moving state infrastructure to the cloud (e.g. [5, 11, 13–15]), presenting interesting results from variety of perspectives: requirements, goals, focus (core business vs technological challenges), adoption, and legal and technical aspects of implementation. Though, Estonia can learn from other states' experiences with government clouds, its unique context, goals, and new ambitions necessitate the innovation of novel and context-specific cloud computing solutions.

In 2013, the Ministry of Finance commissioned analyses of the necessity and opportunities for consolidating the ICT resources of the Estonian state. The study's goal was to determine the optimal infrastructure for the state based on the following assumptions [9]:

- The state's distributed IT architecture must remain – e.g. each ministry/agency must retain the role of customer and budget holder;
- The possibility of free competition must remain;
- The quality of ICT services provided to ministries/agencies must improve.

Analyses [9] emphasized the need for a consolidated networking and datacenter layer to develop high quality cost-effective services. Research and interviews conducted by ministries with experts called attention to various reasons why the Estonian

state needs to develop its own Government Cloud, and what nuances must be considered when developing it. The main reasons for building the Government Cloud are:

1. Server farm fragmentation must be eliminated and high-quality cost-effective services must be ensured.
2. There is a need to ensure the cyber defence of "digital monuments" (websites with symbolic status such as president.ee, website of the Ministry of Defence, etc.). Though these websites contain only public information, their symbolic significance means that it is nonetheless important to protect them from cyber-attacks.
3. There is a need to ensure Estonia's digital continuity and the functioning of the state in any situation or emergency.
4. There is a need to ensure the reliability and quality of cross-border services, because Estonia is starting to issue digital IDs to non-residents and building up "a state without borders."
5. Flexible cost-effective solutions for local municipalities must be developed.

All these topics are described in the following sections in more detail. The need for the Estonian Government Cloud is motivated by the desire to improve service quality, not to save costs. The people responsible for Estonia's public sector ICT spending understand that it is increasingly hard to find major opportunities for cost optimization within Estonia. Their focus is now on maintaining service quality levels in an ever-developing ICT world without a massive jump in expenditures.

2.1 Fragmentation and Service Quality Issues

The IT architecture in the Estonian state information system is distributed. State IT is managed separately by various institutions, usually across the governance areas of ministries, whose functions do not overlap. On a national level, there is a data communication service (ASO) and channel layer (eesti.ee), but there is no significant server hosting offering, and the quality of the services is fragmented between various agencies, because not all agencies have access to the necessary funding and competent human resources [7]. Currently Estonia's public sector does not have the ability to host its information systems in datacenters that guarantee high availability and security. Information systems are mostly located in spaces constructed and maintained by the agencies themselves, and these do not satisfy modern requirements for security, energy and cost efficiency. The only one to maintain larger server rooms of proper quality in the public sector is the State Infocommunication Foundation (RIKS), which hosts servers across 900 m2 of floor space. The main tasks of RIKS are providing operational radio and maritime communication, and telephone services. Additionally RIKS has installed high quality secure server spaces for institutions and companies related to the state.

In the ministerial areas of governance ICT services are managed by each agency individually. As a rule, the agency will have created an ICT unit for this purpose. Based on the needs of the agency's main area of activity, the necessary competences are either developed entirely or partially by the in-house ICT unit, or they are procured from external service providers. Such units usually have small staffs, with one employee

serving multiple roles, and personnel risks are high. Agencies within one area of governance do not have close cooperation with each other. Because of this, there is significant duplication, and resource usage is not as efficient as it could be.

Due to this fragmentation, there is a need for the state to procure secure datacenters that comply with agreed-upon service levels (server rooms including electricity, connectivity, cooling, and security; virtual machines including servers down to the operating system; storage devices; zoning and management) and to create a proper Government Data Cloud.

2.2 Protection of "Digital Monuments"

On several occasions, Estonia has experienced a wide range of cyber-attacks. These attacks have targeted primarily public websites which are not part of the state's critical infrastructure. As a result, the physical damage caused by these attacks has been relatively small and they have not endangered human lives or the functioning of the Estonian state. However, the website of the Ministry of Defence or the President's website have a symbolic status. They are "digital monuments", which must be protected from damage or defacement by any state that finds cyber defence important. Each successful attack produces damage to the reputation of the state and decreases the trustworthiness of its ICT cyberspace in the eyes of both its population and its external partners.

Though the fragmentation of Estonian state infrastructure is a boon for state security in that it makes it harder to stage a mass assault, it also complicates the prospect of protecting Estonia's "digital monuments." The variation in technical expertise and human resources across state agencies leaves some "digital monuments" without the requisite levels of protection. Although "monumental websites" contain only public information and nothing sensitive it is still important to protect them from cyber-attacks to maintain international reputation and keep "monuments" available for the population.

2.3 Digital Continuity

Active implementation of the "paperless governance" policy has brought Estonia to a situation in which some essential registries, e.g. Land Register (contains information on land ownership) exist only digitally and only have evidential value in digital form. The threat of cyber-attacks or a situation, in which Estonia would be occupied and would lose its independence for an indefinite length of time, have led to an additional requirement for the Data Cloud solution of the Estonian state: ensuring digital continuity regardless of the prevalent conditions in the territory of Estonia.

Furthermore, digital continuity requires more than just the preservation of critical data sets and IT solutions on Estonian territory; a solution must also be found for a situation in which the Estonian state does not have control over the datacenters located within its own territory. The need may also arise for operating some services outside the borders of Estonia. The challenge here is to develop a solution whereby the Estonian state would endure even despite an occupation of its territory.

2.4 A Country Without Borders

Estonian society is highly dependent on ICT. Estonian citizens are able to perform nearly every public and private sector transaction in digital form, including signing any document. Now Estonia has an ambitious plan to start issuing Estonian e-identities to non-residents. This might significantly alter the country's visibility and functioning. This in turn requires the country to reach beyond its own borders, closer to potential and existing "customers", and to realize the dream of a "state without borders".

So far, the Estonian electronic identity has not been extended to foreigners who are permanent residents of countries other than Estonia. Recently the Estonian government has approved the concept of issuing digital IDs to non-residents. Since the end of 2014, foreigners have been able to receive a secure Estonian e-identity. This creates a unique opportunity to create a new set of remotely usable global services [10]. E-residence provides a globally innovative suite of public and private services that are usable irrespective of location: convenient business services, bank transactions, tax reporting, medical counselling, etc. E-residence can be based on existing Estonian e-services, developing them further and adding new ones.

The state intends to create a solid foundation for new business opportunities in this area. However, the development of the necessary infrastructure and range of services requires the coordination and joint effort of the public and private sectors. To support the spread and success of e-residency, digital continuity must be ensured, and the risk that an e-resident might lose their land, money or stocks as a result of a security breach must be ruled out. Therefore certain guarantees for e-residency continuity are required, especially from the perspective of proving ownership (primarily the Commercial Register and Land Register).

E-residency is pushing Estonia closer to potential customers with its public and private services, which entails additional cloud computing development needs both inside and outside of Estonian borders.

2.5 Cost-Savings Need for Local Municipalities

The pressure to save costs drives municipal governments to optimize processes, to look for flexible solutions, and to seek out more economical licensing policies for the use of everyday tools (such as email, file management, productivity software, etc.). Automation and the use of IT solutions are an excellent method to achieve this. An increasing number of companies, such as Google, Microsoft, Apple, etc. are offering cloud-based solutions, allowing state and municipal agencies to use resources and software based on their changing needs. In addition, agencies no longer need to purchase separate licenses for each workstation: pricing is based on actual usage. This flexibility is very attractive to municipal governments as well.

A typical municipality runs over 100 different systems for local government administration (area planning, kindergartens, social services, schools, roads, cemeteries, clinics, care for the elderly etc.). Estonia has over 200 municipalities, therefore, it is extremely difficult to find solutions for cost-effective digital services. This is true with respect to everything from office productivity software to horizontally cross-penetrating

software categories, such as ERP, document management, open governance, etc. Though the exchange of sensitive data between municipalities is uncommon, the existence of this practice forces us to consider data security and protection issues.

3 Concept of the Estonian Government Cloud and Data Embassies

This concept has been developed based on the peculiarities of the Estonian Government Cloud. It describes three main principles:

1. Cloud solution located within Estonia's national borders
2. Opportunities and dangers of using international public clouds
3. Necessity of Data Embassies.

3.1 Government Cloud on Estonian Territory

The core of the Estonian Government Cloud concept is a classic datacenter solution, which differs very little from models used elsewhere in the world. The main difference stems from Estonia's small size, which makes it difficult to achieve competition and save costs through large-scale procurement. Estonia currently has plans for at least two datacenters with combined heat and power plants. The public sector, excluding municipal authorities, requires around 2000 m^2 of datacenter space in total. Considering that Estonia needs a primary and a secondary site, the total requirement is on the order of 4000 m^2.

Additionally, the management of cloud computing resources must be sufficiently flexible. Even a small country like Estonia has peak times (e.g. periods of e-elections, the period of electronic tax return filing, etc.). Therefore, it is necessary to involve resources provided by the private sector in the Government Cloud solution that is located on Estonian territory. This may account for as much as a third of the total capacity used by the state.

A separate issue is the mutual network-level separation and firewalling of the resources of different agencies. It is needed to create a set of security classes which define the parts of the Government Cloud which exist in a public IP space or in a special network zone.

Figure 1 illustrates the components of the Government Cloud: a primary datacenter, a secondary datacenter, a private-sector-provided resource. In the drawing there is depiction of X-Road which is a technical and organizational environment for enabling secure Internet-based data exchange between the public and private sector enterprises and institutions.

3.2 Use of International Public Clouds

The Estonian government has been using cloud services offered by large multinational corporations since 2009, when the national tourism website visit visitEstonia.com was

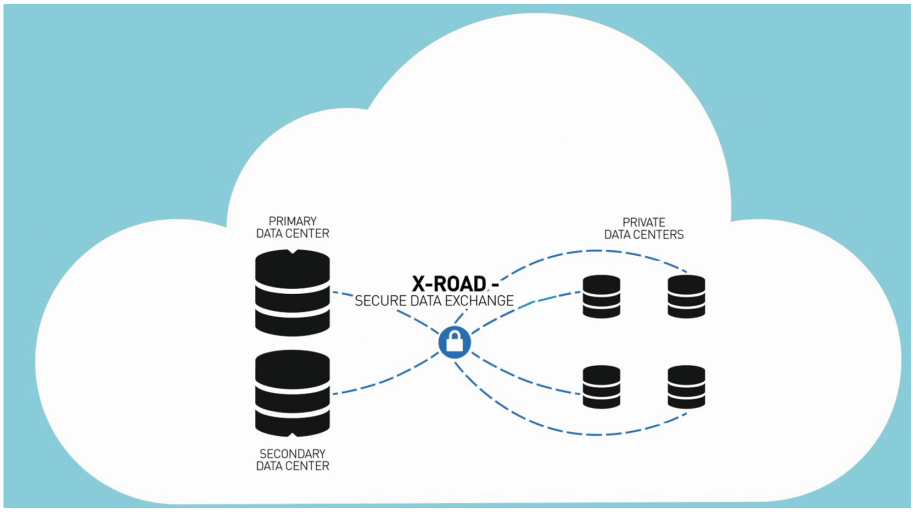

Fig. 1. The government Cloud inside Estonian territory

placed in the Amazon Cloud. The main reason for cloud hosting was the need for flexible server resource management. In addition to load tolerance, the customer (Enterprise Estonia) primarily required the availability of sufficient performance capacity (the application must be fast regardless of where the query has been sent from), which necessitated that the portal be "moved closer" to its primary target audiences, and the solutions offered by the international public cloud enabled this.

Additionally, international public clouds reduce the issue of licensing and software costs. Therefore it is logical that IaaS, PaaS and SaaS service models offered by large multinational corporations must be considered in the architecture of the Government Cloud.

In Estonia it is possible to use Cloud software for email, team collaboration, file management, etc., even if the Cloud is outside of Estonian territory. Estonia's Data Protection Inspectorate does not see an inherent problem in using cloud services and moving the information outside of the state's borders. According to Estonian legislation it does not matter if the service is offered from inside Estonia or from outside, as long as the data is protected. The limited sensitive information on the municipal level mainly includes personal data and procurement-related information.

The price and quality of services offered by international cloud providers are also tempting from the perspective of protecting so-called "digital monuments". To reduce the likelihood of a successful attack on websites with national symbolic significance, it is pragmatic to outsource their defence, and host President.ee, Valitsus.ee (Government Office), the Ministry of Defence website, etc., in an international public cloud. The information on these websites is not sensitive, and the server farms and information distribution will make attacks on them unreasonably costly. This distribution can be done using the services offered by Amazon, Microsoft or Google, for example. The use of these public clouds does not entirely eliminate risk, and their availability is not

Fig. 2. The Estonian Government Cloud includes international public clouds

100 % guaranteed, but their capacity to deal with the most widespread attacks is greater than that currently existing in many ministries and agencies. Therefore, the Estonian-soil-based Government Cloud must be augmented to include companies that offer international cloud computing services. The augmented service is illustrated on Fig. 2. Certain reservations need to be maintained about holding sensitive information in international public clouds, even if that information is encrypted. Storing sensitive information in international public cloud is not acceptable due to substantial damages and reputation risks associated with data leaks, especially regarding to recent cases (PRISM, Snowden case, etc.).

On the other hand, the use of international public cloud services for backing up sensitive information is possible in a crisis and war-time situation, where the necessity to maintain digital continuity outweighs the risks of possible leaks of sensitive data. It is also acceptable that in an emergency situation, critical services such as parliamentary or Government tools could be operated from public clouds located outside of Estonian territory. In addition to protecting the information provided by these applications, it is also possible to use the encryption capability provided by the core infrastructure of the Estonian state.

Estonia already uses various international public cloud SaaS, PaaS and IaaS services. Therefore it is important to involve these international public cloud providers in the Estonian Government Cloud concept. However, it must be considered that as the state does not have full control of the storage and location of this data, there is a chance that the data may leak.

3.3 Use of Data Embassies

Estonia's need for digital continuity and its desire to provide additional guarantees to e-residents are two of the biggest factors that differentiate its cloud computing needs from those of other countries. Estonia needs to have a server resource that is 100 %

under the control of the Estonian government, but is located outside of Estonian territory. Currently there are specific procedures which are followed to backup necessary data and applications, so the service availability can be restored using the backup copy if necessary. However, in order to ensure digital continuity, some registers (such as the State Gazette, the online depository of all legislation in Estonia) should have an active copy that can be used in real time and updated according to the law, even if the Estonian state no longer has control over datacenters located in Estonian territory, or there is another crisis or emergency that makes the operation of the State Gazette application from within Estonia impossible.

Therefore, the Estonian state must own server resources outside of its own territory, those resources must be 100 % under Estonian state control, and must be usable not only for data backup, but also to operate services if necessary. To ensure this, there are two solutions proposed:

(1) Using Estonian embassies which are already established outside of Estonian territory. By ensuring the necessary technological resources, embassies could house backups for registers. With limited construction work, larger embassies can establish special environments for regular data and application backups, mirroring and service operations. Even transitioning to this model and a weekly backup schedule would give the Estonian state a significant benefit compared to the current model, as the current quarterly or twice-annual backups do not maintain the information sufficiently up to date, and digital continuity is not entirely ensured.

However, the use of Estonia's physical embassies presents certain problems. These embassies do not have sufficient technical competence to offer the level of technical support that is necessary to maintain the infrastructure and react in a crisis. In a situation where an enemy is making a cyber-attack on Estonian IT solutions located both on Estonian territory and in our embassies, the embassies generally will not have sufficient capability to protect themselves.

Additionally, embassies do not have control over the telecommunications service they are offered. It is possible that as part of an assault, an embassy's internet connection would be disabled by a telecoms operator that is controlled by the adversary; or the network segment that is being attacked would simply be disabled in order to save other resources on the same network from overload.

In summary, we cannot rely on Estonia's embassies alone, because in addition to the problems outlined above, embassies are also not physically constructed according to proper standards in order to meet the data security requirements.

(2) An improved solution is the Data Embassy concept. The goal is to procure resources under bilateral agreements from the Government Clouds of states that are friendly to Estonia. The Estonian state would sign a bilateral treaty, under which Estonia will rent special floor space or an enclosed room in an existing datacenter that has been constructed and operates according to necessary standards. The corresponding perimeter would be physically separated, equipped with security devices in order to ensure that the Estonian state maintains complete control over the servers within that agreed-upon perimeter. Similarly to a physical embassy, Estonian jurisdiction would be

applicable within that established perimeter, and it would have all the same provisions (including immunity) as a physical embassy or an ambassadorial residence.

A Data Embassy solution of this kind (Fig. 3) would be significantly better than server rooms constructed on the premises of Estonia's physical embassies. The datacenter of a state that is friendly to Estonia, would have been constructed as a dedicated data storage facility, with the possibilities of various risks (overheating, power outages, network overload, cable damage, etc.) having been minimized. Dedicated datacenters have their own requirements for service quality assurance, and they can employ professional staff, trained to maintain service availability in an emergency and to repel cyber-attacks. The advantages of Estonian Data Embassies are shown in the illustration below.

Furthermore, the Data Embassy concept is in line with 1963 Vienna Convention on Consular Relations.

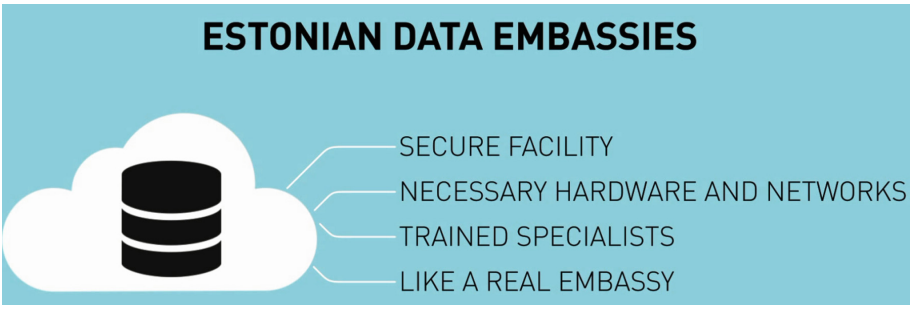

Fig. 3. The Estonian Government Cloud includes international public clouds

Server rooms in physical embassies and dedicated Data Embassies would together create a network that would ensure Estonian digital continuity and be extremely costly for an enemy to damage or take down.

Such a network is illustrated in Fig. 4, but of course one must bear in mind that all Data Embassies are connected to all other embassies over the internet, using encryption to exchange data. The illustration is also not completely accurate because Estonia needs more server resources nearby.

In conclusion the conceptual model of the Estonia's Government Cloud contains three interdependent layers:

1. Cloud solutions on Estonian territory, requiring the construction of primary and secondary datacenters, and involving private sector resources for at least a third of the entire required capacity.
2. Public Cloud services provided by major multinational corporations and used with an awareness of the risk that information hosted there may leak to third parties.
3. A Data Embassy network, comprised of server rooms physically constructed in Estonia's foreign embassies and server resources hosted in datacenters of states friendly to Estonia.

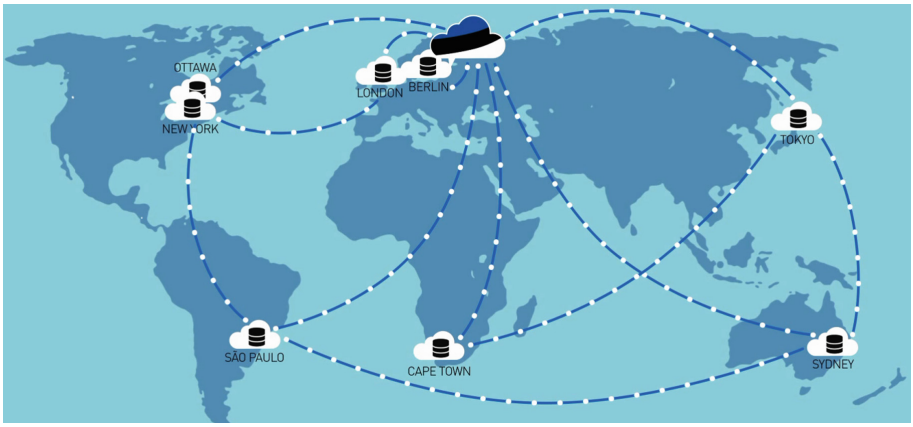

Fig. 4. The proposed network of Estonian Data Embassies

These layers working together will meet the currently identified requirements for an Estonian Government Cloud, including the challenges stemming from Estonia's particular situation: the need to reduce fragmentation, provide an increase in service quality, find cost-effective solutions for municipalities and ensure digital continuity and reliable e-services for e-residents.

4 Implementation Plan of the Estonian Government Cloud

To implement the Estonian Government Cloud, a number of activities have to be completed. The following sections provide a brief overview of the main activities necessary for implementing the three aspects of the Estonian Cloud concept.

4.1 Building the Government Cloud on Estonian Territory

In-country server resource consolidation must be finalized, and the **business model for server resource administration** and development must be implemented. Ministries and agencies must present their server resource requirements to RIKS, who will then deliver the resources out of its available supply, or arrange a further capacity procurement from the private sector, if necessary. According to RIKS action plan for 2014, RIKS will complete the development of server hosting facilities using existing facilities. The resource that will be created will be appropriate, among other things, for acting as a buffer during the consolidation of the server parks of state agencies.

RIKS has also developed an **implementation plan for new datacenters** (primary and secondary), including budget calculations, the execution of which is currently dependent on a decision by the Estonian Government. It is also necessary to begin negotiations with **private sector** enterprises which currently possess datacenters and server resources on Estonian territory that match the standards established by the

Information System Authority (RIA). This engagement will enable to develop a model for the flexible involvement of these resources in accordance with public procurement principles.

Due to the inconsistent service quality that currently exists in ministries and agencies, there have been discussions of adopting **additional regulation** to accelerate the consolidation of a single Government Cloud. Additionally, it is necessary to develop **regulation for the special circumstances** under which ministries and agencies may possess their own server resources. In all other cases, the services provided by RIKS must be used and thereby server resource consolidation is enforced.

The extent of the **responsibilities of the Cloud service's Customer (ministries and agencies) and Vendor (RIKS) must be clarified**. To make transition smooth and convenient for the customer, it will be conducted in two phases.

In first phase each Cloud service user is responsible for the functioning and backup of their IT solutions from the operating system up, and the vendor of the Government Cloud has responsibility purely for the infrastructure service. The first phase must be treated as an introduction and pilot phase on the road to a more service-oriented model.

In the second phase a comprehensive service portfolio must be implemented for the Government Cloud. This leads to the creation of opportunities for the state's IT centers and the private sector to work together to offer more complex and intricate solutions to agencies who use the Government Cloud (for example, database management, mass OS deployment, monitoring services, log collection and processing, managing specific application servers and information systems as a whole). Preparation for this phase must substantively begin in parallel with the implementation of the first phase.

4.2 Principles for Using International Private Clouds

Clear guidelines or role-played usage scenarios are required for Estonia's local municipalities, on how to technologically construct their agencies' IT solutions. Constant budgetary pressure and the more flexible licensing conditions offered by major vendors make it necessary to assess the possibility that, for example, MS Office productivity software is no longer installed on every workstation, but Office 365 is used from the cloud instead.

Estonia offers a state infrastructure for data encryption, any information generated by a private person, company or government entity can be securely encrypted, if necessary. In terms of data protection, clear instructions are needed on how to handle information (including sensitive information) produced in municipalities.

All this requires **specific guidance** from the Ministry of Economic Affairs and Communications (MKM) for the **conditions under which it is reasonable to purchase server resources or cloud applications from the private sector**, and which factors must be considered. Also, the Data Protection Inspectorate has to **develop guidelines for ministries, municipalities and agencies** to consult in order to ensure data integrity and protection.

4.3 Constructing the Data Embassy Network

The Data Embassy Network is a long-term project and therefore constructing the network has to be carried out in several phases.

The first phase includes the **deployment of three locations from the Data Embassy network**, two of which are within Europe and one is outside Europe. Two of these locations will involve the development of additional server rooms on the premises of Estonia's existing embassies, and one will involve the procurement of space by Estonia in the Government Cloud of a friendly state.

The technical requirements have already been prepared along with procedural rules for the backup and operation of registers and applications. The legal aspects of the agreements between Estonia and the friendly state, including guarantees for Estonian servers located in the datacenter of another state, are in process. The first phase involves only a physical room that the Estonian state will be using. The broader concept envisions Estonia hosting a Data Embassy in a friendly state's Cloud.

The extent of the second phase of Data Embassy development depends on the results of the first phase and the expenses.

As some registries exist only in digital form, it is essential to ensure the digital continuity of the Estonian state. Furthermore, to succeed in the plan to issue foreigners Estonian e-identities, certain guarantees for e-residents are needed, such as proving ownership of land, company or other assets. Therefore **the government has to develop principles for how registries are backed up and how frequently**. A list of registers and services, which are available even if Estonia's datacenters are not available in-country, must be created. Necessary services have to be designated for ensuring digital continuity as essential services. Action plans for risk scenarios and crisis situations need to be developed.

5 Summary

The Estonian state has built the foundation of a highly developed information society, and the population depends on the functioning of information and communication technologies in its everyday life. IT development has taken Estonia to a stage where many registers and services only exist in digital form. Scenarios where, for example, digital signatures do not work for days at a time, or the data in the Land Register is corrupted, are not acceptable to Estonian society.

This environment requires a flexible Government Cloud solution, whose growth, requirements and future capacity cannot be fully predicted today. Therefore, sufficient flexibility has to be planned in advance. The consolidation of domestic server rooms into standards-compliant datacenters, the flexible involvement of private sector resources both inside and outside the state's borders, and the construction of the Data Embassy network, will create a strong foundation for a working Government Cloud that provides a higher quality of service without increasing hosting costs.

References

1. European Commission: European Cloud Computing Strategy. http://ec.europa.eu/digital-agenda/en/european-cloud-computing-strategy
2. European Commission: Trusted Cloud Europe. http://ec.europa.eu/digital-agenda/en/news/trusted-cloud-europe
3. ENISA: Good Practice Guide for securely deploying Governmental Clouds. http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/good-practice-guide-for-securely-deploying-governmental-clouds
4. Mell, P., Grance, T.: The NIST definition of Cloud Computing, National Institute of Standards and Technology, Special Publication 800-145 (2011)
5. Wyld, D.: Moving to the cloud: an introduction to cloud computing in Government (2009)
6. 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, pp. 181–195. Springer, Heidelberg (2013)
7. Estonian Information System Authority: Riiklike andmekeskuste konsolideerimine ja ehitamine (in Estonian), Tallinn (2014)
8. IT Department of Ministry of Finance: Riigi info- ja kommunikatsioonitehnoloogia korralduse analüüs (in Estonian), Tallinn (2013)
9. Noormaa, M.: Riigi IKT analüüsi tulemused (in Estonian). Ministry of Finance, IT Department, Tallinn (2013)
10. Estonian Ministry of The Interior: Uus digilahendus annab välismaalastele võimaluse e-Eestis tegutseda (in Estonian), Tallinn (2014)
11. 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, pp. 150–158. Springer, Heidelberg (2014)
12. Williams, M.D.: E-government adoption in Europe at regional level. Transf. Gov. People Process Policy **2**(1), 47–59 (2008)
13. 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)
14. Bhiskar, A.: G-Cloud: new paradigm shift for online public services. Int. J. Comput. Appl. **22**(8), 24–29 (2011)
15. 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), pp. 201–206 (2011)