Framework of e-government technical infrastructure. Case of Estonia

A. Kütt[1], **J. Priisalu**[1]
[1]Estonian Information System's Authority, Tallinn, Estonia

Abstract—*As information technology becomes more ubiquitous, governments of all levels must keep up with the increasing demand from the citizens for electronic services of all kinds. The service, policy and governance issues of this struggle are progressively well understood. Its technical aspects, however, are often considered to either be a commodity or covered by research in the field of enterprise architecture. Both experience in international cooperation attempts and efforts in coordinating architecture development on the state level, however, indicate that the existing approaches are not necessarily suitable for inter-enterprise coordination and governance purposes. In this paper we outline requirements for a framework suitable for framing the technical aspects of e-government, describe such a framework and discuss its application in the context of a small nation of Estonia.*

Keywords: e-government, framework, system architecture, software architecture, Estonia

1. Background and motivation

A country can be seen as a system performing a certain function by utilising a portfolio of limited resources. From this perspective, the concept of an architecture of a a country becomes meaningful. In the context of e-government, this architecture can be separated into elements dedicated to information technology and elements related to other aspects of the government. The latter is substantially covered by e-government related research while there is relatively little coverage of the former. In this paper, the authors seek to provide a conceptual architecture framework for the technical architecture of an e-government that is widely applicable and can act as a foundation of further research in the field.

2. Problem statement

Since the 1980s, there has been a solid stream of research focused on e-government, its structure, impact and governance. To a large extent, this work is focused on the service delivery and policy aspects of the issue while the technical implementation of the services and policies has received relatively little attention. Although architecture frameworks have been suggested (e.g. [1], [2]), they do not usually clearly separate between functional and technical aspects of information systems. Therefore application of these frameworks for technical architecture governance is limited.

In the following, we present three challenges driving the need for a structured understanding of the technical aspects of e-governance.

Firstly, e-government is often defined as the use of electronic means for service and data delivery ([3], [4]). While accurate in many ways, such an approach seems to be focused on existing services and assume the government, as a system, to have a stable architecture. This is not necessarily true as architecture developed by accretion might exhibit deficiencies in behaviour [5] and a definitive innovation pressure exists driving functional and technical change of which the open data movement is an excellent example. Therefore, stability of system architecture and the service portfolio, can not be assumed. Clearly, an understanding of the underlying technical architecture is necessary so the functional architecture it supports can be systematically developed.

Secondly there is evidence for system architecture being related to, and therefore influencing, organisational architecture ([6], [7]). A similar relationship has been observed in the field of knowledge management [8]. In the field of system architecture and product design, the notion of architecture having an unintentional impact on system functionality is known as emergent behaviour [5] or incidental interactions [9]. The research also points out, that not all such unforeseen behaviour is desirable. In the context of e-government, this means that decisions concerning technical architecture could have a potentially unwanted impact on the governance models in use and democracy in general. Understanding, predicting and ultimately controlling such effects assumes understanding of the architecture of the technical architecture of the government.

Thirdly, the governments are funded by tax-payers and are thus under varying levels of pressure to reduce costs. One of the most accessible cost-reduction mechanisms is consolidation of IT organisations as it can be achieved by administrative measures only. This however can damage the ability of organisations to fully utilise IT, a concept known as IT-business alignment. According to Luftman, IT-business alignment can be assessed based on six criteria: communications, competency/value measurements, governance, partnership, scope & architecture and skills [10]. At least two of these - communications and partnership - are likely to be impacted as the organisational distance between IT and business is increased by centralising the former. Therefore, a need exists to identify more sophisticated means of consolidation which require a robust framework of thought around technical architecture.

3. Requirements

To be applicable and meet the challenges described above, the architecture framework to be developed should fulfil certain requirements.

1) It should provide a holistic view of the information system powering the governmental body in question in a way that is congruent with it in terms of scope, i.e. there should be one way of looking at the entire information system the said body is responsible for
2) Different governments have different approaches to performing their functions in terms of citizen involvement, centralisation, regulatory arrangements etc. A useful general framework should therefore fit a range of different forms of government while being flexible enough to accommodate for inevitable changes caused by democratic processes. It is also likely that the differences in approach (the concept part of the in the form-function-concept architecture model by Crawley [11]) can lead to significant differences between government architectures that should be possible to accommodate
3) The framework should have a level of abstraction that allows for conceptual discussion of the related topics. At the same time it needs to be specific enough to allow clearly define the related organisational architecture as a foundation for organisational change
4) As providers of e-government services vary in size and complexity from a small municipality to large confederations, the framework should allow for additional structure to be added to its elements in a way that does not affect the superstructure
5) All technical architectures are related to functional architectures, i.e. the way functional units are related to each other has an impact on how technical components interact. Thus, effective communication must exist between contributors to functional and technical architectures. In order to efficiently serve as a communication tool, the framework must, on a high level, be possible to describe in non-technical terms

4. The framework

Although the framework described is focused on technical architecture, technical architecture of any system is, as discussed, dependent on its functional architecture. Therefore, for each part of the framework, key question the functional architecture must answer are listed along with a brief description of their impact on architecture. These questions are centred around these three axis, each contributing to the complexity of the technical solution and the choices to be made:

- *Centralisation.* Generally a centralised solution offers more control but grows exponentially in terms of complexity for larger entities. A decentralised solution scales better but requires more complex coordination mechanisms to function
- *Privacy & security.* Any sharing of information or access to it causes privacy and security concerns. Thus, stricter policies in these fields drive up solution complexity while less restrictive policies require a framework for moving data between privacy domains
- *Diversity.* A more diverse solution space allows for a better match for potentially complex market needs and drives down complexity but requires robust coordination mechanisms. Stronger uniformity requires enforcement mechanisms to be in place and drives up complexity within a solution

The framework itself consists of four key layers uniting the information systems of various branches of the government and allowing interaction with the consumers of the services: citizens, officials and enterprises. Within each layer, the architecture of a particular government can be detailed using an enterprise architecture methodology of choice. The framework proposed intentionally does not cover the following aspects of e-government implementation:

- Implementation of the business logic of e-services themselves as the services are assumed to be implemented by the agencies and thus not to be subject to central governance
- Relationships between layers that, while undoubtedly existent, should be dealt with on a higher abstraction level

The framework is depicted on figure 1.

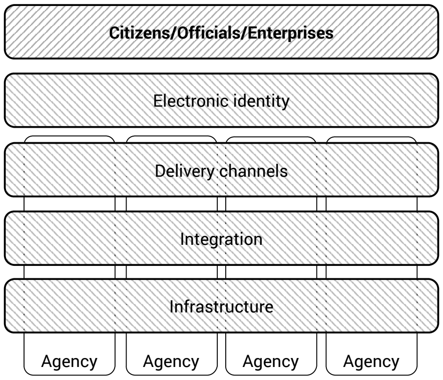

Fig. 1: Framework of e-government technical infrastructure.

4.1 Electronic identification

Without an efficient ubiquitous method of identifying a citizen and acquiring their legal consent, providing a full range of electronic governmental services is difficult. At the same time, many services can be provided with either limited or no identification depending on both the risk levels present and the level of risk aversion of the service provider. The main functional drivers of the electronic identity layer implementation are:

1) Who is the target customer of the e-services provided? The question of how to identify a user depends heavily on who the user actually is. In EU context, countries are increasingly providing services to EU citizens in general. There are also circumstances where large portions of the population are not citizens of the country but might be considered a target group for e-services. The answer here is the foundation to many assumptions the technical implementation can make about the user behind the keyboard.
2) What is the legal significance of electronic identification? Identification methods carrying more legal significance require a more robust technical implementation and might be more difficult to distribute widely. Also, if the legal gravity of electronic identification is low, the services implemented must be designed to fill in the gap by, for example, requiring physically signing and returning a hard copy of the forms filled.
3) What is the multiplicity relationship between legal and electronic identities? Again, identification methods that provide a more certain relationship between a legal and electronic identity are more complex. Also, if a physical person can have multiple legally equivalent digital identities, a need arises to link these to each other via a shared identity code or some other mechanism. In case multiple identities can have various levels of legal significance and/or the identities can not be related to each other in a definitive manner, the information system implementing the architecture must make provisions to cater for the possibility of overlapping digital identities of various certainty levels.

4.2 Delivery channels

E-services can be provided via a range of electronic channels from traditional IVR-based ones to sophisticated mobile platforms. It must be noted, that the boundary between electronic and non-electronic delivery channels is not definitive as both kinds of channels support the same set of business processes and the systems implementing them can at least on the logical level be considered as one entity. The main functional questions driving the architecture are:

1) What is the diversity of the electronic delivery channels across services? In case a small number of channels is offered, accessibility issues arise as no electronic channel is truly ubiquitous. As the number of channels grows, the architectural complexity of keeping the service consistent across them increases.
2) What is the diversity of the electronic delivery channels across the country? It is often described as desirable to implement a "single-window" approach for providing services to the citizens ([12], [13]). This approach implies a system that needs to meet stringent availability requirements under high-throughput conditions and requires complex orchestration of systems of various agencies. A fully decentralised system, on the other extreme, would require mechanisms of providing a consistent user experience as well as a shared robust security domain.

4.3 Integration

The integration layer joins the information systems of different agencies allowing for sharing of data and functionality. This layer embodies the classical concept of middleware [14, p. 14] providing a clean separation between consumers and producers of data and services. In addition, the integration layer might provide assistive services like caching, service discovery, audit logging etc. The main questions driving the architecture of the integration layer are:

1) To what extent are the functions centralised between the agencies? This level of centralisation determines the ratio between producers and consumers of data and services. This in turn drives the availability, deployment and flexibility requirements towards the middleware platform.
2) What are the integration paradigms used? Paper-based governmental processes rely on documents being passed around. In the context of e-services, however, documents transform to data that can be shared, transferred and fragmented. In case of cross-agency processes, sharing data is often not sufficient as the agencies must coordinate different functionally significant activities and sharing of services becomes necessary. The choice between the three communication paradigms - document, data or service - has a strong impact on the requirements towards the integration layer. For example, a document-based system would need to provide tracking facilities for the documents moved while the service-based integration layer would need to consider transactional integrity.
3) How are the questions of privacy and data ownership treated? Since the main function of the integration layer is to allow access to data that often concerns citizens, the approach taken towards privacy is an important requirement driver for the architecture chosen as it is the main point of data access implementation. For example, the middleware might provide a facility for citizens to track access to data concerning them or enforce regulations preventing access to data or services under certain conditions.

4.4 Infrastructure

All of the services making up the e-government portfolio need to be deployed in a manner that supports the strategic goals of the e-government including non-functional requirements of performance, availability and security. The layer consists of the digital infrastructure - servers, networks, hosting facilities, security equipment etc.- used to provide e-government services. Its main functional drivers are:

1) How tightly is the infrastructure consolidated? Although there are definitive benefits like cost, high level of control and ease of integration to be gained from consolidating infrastructure, excessive consolidation can lead to emergence of single points of failure. Also, the extent to which the organisational structure of IT services is consolidated in the country have a strong effect here.
2) To what extent are platforms offered centrally? Emergence of cloud computing has shown the viability of centralised platform offerings. While the consolidation question can be seen acting on the horizontal dimension of the infrastructure layer, platforms can be seen as vertical. On one extreme of the scale is a slim platform that is limited to a small number of commoditised services like network access while sophisticated platform-as-a-service offerings are on the other.
3) What restrictions exist for the physical location of data? Both EU and USA have passed legislation that governs privacy of personal data and its transfer outside of the respective jurisdictions. In addition to these, countries might adopt additional restrictions while governments on the municipal level could be subject to a looser set of constraints or be required to share data with central government.

5. Framework application in Estonia

In the following the framework covered above is applied to describing the e-government architecture of Estonia, a small North-European country. In Estonia, this framework is used for two main purposes. Firstly, it forms the basis of communication within the country and with our partners abroad allowing for rapid identification of contact points and clean separation of concerns. Secondly, it is used as a governance tool with the national architecture governance process being aligned to the layers of the model.

For the electronic identification layer, Estonia is using a smart card that is also a compulsory picture ID from the age 15 onwards and is carried by vast majority of the population [15], including the residents without Estonian citizenship that account for 15.7% of the population [16]. The card is tied to a unique ID-code of a person. Authentication and digital signing are carried out using the certificates stored on the card, the resulting digital signature is legally equivalent to a physical one [17]. The legal significance of the ID-card is further elevated by its singular use for electronic voting in the country since 2005 and the rapid expansion of this voting method across several demographic dimensions [18]. Although other means of authentication, mainly federated authentication schemes provided by banks, are used in service offerings, they do not hold an equivalent legal weight. Estonia has also participated in an international effort for cross-use of electronic identification [19].

In terms of service delivery channels, Estonia has mainly focused on web based portals. In 2011, 94% of tax returns were filed electronically [15] via a traditional web-based service. More specifically, an internal unpublished analysis found 93,2% of the visitors to the main government portal in the first quarter of 2014 using a desktop computer with the rest using a mobile platform. This indicates a strong focus on traditional as opposed to mobile channels. Although a central government service portal exists, there are still more than 128 individual web-based service points as identified by an internal unpublished study. Thus it must be concluded the channels used in Estonia are not very centralised across the agencies.

For the integration layer, Estonia has chosen a relatively unconventional route and implemented a state-wide distributed integration bus called x-road [17]. X-road consists of a network of dispersedly deployed access points that mediate between agencies and the rest of the government infrastructure while performing support functions like service discovery and access control. This approach means all the data and services are distributed and all integration points are established peer to peer. Although x-road does not enforce a specific integration paradigm, majority of the APIs provided are data-based with service- and document based integration points being a clear minority. One of the main features of the platform is access control allowing fine-grained permissions to be set for data access. X-road also provides control points for data access monitoring.

6. Summary

We have outlined a framework that is designed to solve a number of challenges modern governments face. The framework is comprised of four layers - identification, channels, integration and infrastructure - providing a lattice uniting individual agency information systems into an unified system. This framework has been applied to a country of Estonia with two key positive outcomes:

1) The key aspects of the technical architecture of the country can be communicated both within the country and in the context of international cooperation
2) A holistic governance can be (and indeed is) applied to the technical aspect of the country allowing for systematic development of the services provided

References

[1] S. Sharma and J. N. Gupta, "Transforming to e-government: a framework," in *Proceedings of the 2nd European Conference on eGovernment-2002*. Academic Conferences Limited, 2002, p. 383.

[2] Z. Ebrahim and Z. Irani, "E-government adoption: architecture and barriers," *Business Process Management Journal*, vol. 11, no. 5, pp. 589–611, 2005.

[3] K. Layne and J. Lee, "Developing fully functional e-government: A four stage model," *Government information quarterly*, vol. 18, no. 2, pp. 122–136, 2001.

[4] Z. Fang, "E-government in digital era: concept, practice, and development," *International journal of the Computer, the Internet and management*, vol. 10, no. 2, pp. 1–22, 2002.

[5] E. Crawley, O. de Weck, S. Eppinger, C. Magee, J. Moses, W. Seering, J. Schindall, D. Wallace, and D. Whitney, "The influence of architecture in engineering systems," *Engineering Systems Monograph*, vol. 2006, 2004.

[6] A. MacCormack, C. Baldwin, and J. Rusnak, "Exploring the duality between product and organizational architectures: A test of the "mirroring" hypothesis," *Research Policy*, vol. 41, no. 8, pp. 1309–1324, 2012.

[7] J. E. Fountain, *Building the virtual state: Information technology and institutional change*. Brookings Institution Press, 2001.

[8] P. H. Hendriks and D. J. Vriens, "Knowledge-based systems and knowledge management: friends or foes?" *Information & Management*, vol. 35, no. 2, pp. 113–125, 1999.

[9] K. T. Ulrich, S. D. Eppinger, *et al.*, *Product design and development*. McGraw-Hill New York, 1995, vol. 384.

[10] J. Luftman, "Assessing business-it alignment maturity," *Strategies for information technology governance*, vol. 4, p. 99, 2004.

[11] E. Crawley. (2007, January) Introduction to System Architecture. Architecture to value. [Online]. Available: http://www.mitocw.espol.edu.ec/courses/engineering-systems-division/esd-34-system-architecture-january-iap-2007/lecture-notes/lec1.pdf

[12] A. Tat-Kei Ho, "Reinventing local governments and the e-government initiative," *Public administration review*, vol. 62, no. 4, pp. 434–444, 2002.

[13] J. Gant and D. Gant, "Web portals and their role in e-government," in *AMCIS 2001 proceedings*, 2001.

[14] P. Naur, B. Randell, F. L. Bauer, N. S. Committee, *et al.*, *Software Engineering: Report on a conference sponsored by the NATO SCIENCE COMMITTEE, Garmisch, Germany, 7th to 11th October 1968*. Scientific Affairs Division, NATO, 1969.

[15] Estonian ICT Export Cluster, "e-Estonia. The digital society," 2012.

[16] Ministry of Economic Affairs and Communications. (2014, March) About Estonia. Society. Citizenship http://estonia.eu/about-estonia/society/citizenship.html. [Online]. Available: http://estonia.eu/about-estonia/society/citizenship.html

[17] A. Kalja, A. Reitsakas, and N. Saard, "eGovernment in Estonia: Best practices," *Technology Management: A Unifying Discipline for Melting the Boundaries*, pp. 500–506, 2005.

[18] A. H. Trechsel, K. Vassil, *et al.*, "Internet voting in estonia-a comparative analysis of four elections since 2005. report for the council of europe," Council of Europe, Tech. Rep., 2010.

[19] A. Piñuela, S. Palomares, and A. Crespo, "D1.3.1 publishable summary report d1.3.1 publishable summary report d1.3.1 publishable summary report stork 2.0. publishable summary report," STORK 2.0 Consortium, Tech. Rep., 2013.