

Systematic Digital Signing in Estonian e-Government Processes

Influencing Factors, Technologies, Change Management

Ingrid Pappel¹(✉), Ingmar Pappel², Jaak Tepandi¹, and Dirk Draheim¹

¹ Large-Scale Systems Group, Technical University of Tallinn, Tallinn, Estonia
{ingrid.pappel, jaak.tepandi, dirk.draheim}@ttu.ee

² Interinx Ltd., Tallinn, Estonia
ingmar@interinx.com

Abstract. In Estonia, digital signing started with the Digital Signatures Act already as early as in 2000. The aim to make digital signing and its use with various types of documents more convenient and efficient has had a high priority in the state's e-Governance initiative. In this article we provide a study of the systematic introduction and use of digital signatures with documents related to decision-making processes and analyze the factors which influence this. We look at local governments as a major use case and provide an overview of the digital signing statistics for local government document exchange. The article highlights the differences related to the size and administrative capacity of the local governments as well as their readiness to transition into the information society.

Keywords: Digital signing · Digital document exchange
Digital administration

1 Introduction

We live in an increasingly digitalized world. In addition to the different technological solutions in everyday life, document management and the related decision-making processes have also become digital. The Digital Agenda for Estonia 2020 aims for a “simpler state” [1], whereby in order to make the public sector more effective, it is important to achieve a 95% paperless official communication rate by 2020. This requires local government services to be as electronic as possible and that as an end result of the provided services, instead of printing out a paper to prove the fact of service provision, it is stored in digital form. In order to achieve this, various procedural systems are in use in Estonia, including document management systems (DMS) – which comprises of and manages documents as well as facilitates constant access to them. DMS has brought transparency to administration and allowed for including citizens in the decision-making processes of the organization. This, in turn, has made the implementation of digital signatures more efficient in Estonia.

In this paper the correlation between the use of digital signatures and specific document types is discussed based on usage of the DMS Amphora. Additionally, a

survey has been conducted that provides an overview of the factors influencing digital signing in local governments. Various research methods were used to carry out this survey, such as data obtained from databases on the basis of specified criteria, the observation of world practices, questionnaires and interviews. Generalizations have been made based on more than 50% of the Estonian local governments.

In order to make digital document exchange more efficient, several solutions have been developed in Estonia [2], e.g. the document exchange center (DEC) and e-services at the citizen portal eesti.ee environment, which enable the digital processing and management of a document life cycle from its birth to death. Over the years, the volume of paper documents exchanged between authorities has decreased significantly [3], which in turn has a positive effect on the budget of the institution. DMS Amphora is used in 127 Estonian local governments and this article presents the data from 117 Estonian local governments because their data was available in the database in the proper form. The data has been taken about the first quarter of 2016. The software solution enables to observe the reply deadline for the letters, and to digitally sign all documents and letters. The data used in this work have been obtained from the DMS database according to the following:

- How many incoming documents has the given local government registered in the Amphora document management system;
- How many outgoing documents has the given local government registered;
- How many of the outgoing documents has the given local government signed digitally;
- Total numbers of letters and documents;
- Capability index of the local government units [4];
- Number of residents in the given local government;
- How many documents per residents are there in the document management systems in the first quarter;
- Name of the local government;
- County in which the local government is located.

In Sect. 2 we explain the background, i.e., the current state of digital signing in Estonia and its motivation. Also we report on first insight concerning problems with digital signing and digital archiving. In Sect. 3 we give an overview of the technological infrastructure in Estonia relevant to digital signing. In Sect. 4 we provide the results of a survey concerning digital signing. In Sects. 5 and 6 we derive factors and draw recommendations for digital signing from the survey results. In Sect. 5 we delve further in issues of change management for the introduction of digital signatures in organizations. In Sect. 7 we discuss possible strands of future work. Related work is discussed in Sect. 8. We finish the paper with a conclusion in Sect. 9.

2 Digital Signing in Estonia

As aforementioned before, the digital signatures in Estonia is governed by the Digital Signatures Act (DAS), which was adopted on 7 March 2000 [5]. In the eyes of the law, a digital signature is equal to a handwritten signature. All Estonian authorities are

required to accept digitally signed documents. Estonian public authorities are required to accept digitally signed documents. Two certificates are issued along with an ID-card. One certificate is for identification and the other for digital signatures. It is important to ensure that these certificates have not expired when using digital signatures. In addition to signing by using the ID-card, Mobile-ID signatures are becoming increasingly popular. In 2015, the number of Mobile-ID users increased by 40%, exceeding the 75,000 user line this January. These users carried out over 25 million Mobile-ID transactions in the last year. In 2014, Mobile-ID was used for an average of 1.8 million transactions per month, where 2015 the monthly average was already 2.7 million [6]. Three types of formats are used in Estonia – BDOC, DDOC, and CDOC. The oldest one of these, the original is the DDOC. BDOC is a newer format meant for replacing the DDOC format, and it is certainly more consistent with international standards. CDOC is a file which in its encrypted form contains a data file (XML document or other binary file, e.g. MS Word, Excel, PDF, RTF, etc.), the certificate of the recipient, an encrypted key for data file decryption, and other optional metadata [6].

2.1 Reasons for Using Digital Signatures

A digital signature is the counterpart of an ordinary signature used to sign information in digital form. Digital signatures help identify the link between the document and the person who signed it. A digital signature along with a time stamp forms a combined dataset with the document, the components of which cannot be individually altered at a later time. Digital signatures replace ordinary signatures which helps to ensure the authenticity and security of electronic documents. Besides apply paperless administration to enable digital document exchange [7]. Ensuring security with a digital signature means that the document author is known and the document has not been altered by third parties between being sent and received [8]. The digital signature standard (DSS) was created by the US National Security Agency. DSS is based on the digital signature algorithm (DSA). DSS can only be used for digital signatures but the DSA can also be employed for encryption [9]. The simplicity of digital signing can be considered its biggest advantage. It is quick and convenient and lacks many of the risks that signing on paper entails. It is certain that a physical person is responsible for the signature. The signed document has not been subsequently edited by third parties, this option is eliminated by mathematical links. It is always possible to check the signing date because the time stamp is a part of digital signing.

- An endless number of legally equal copies can be made of a digitally signed document.
- Digital documents do not take up physical space.
- Digital documents do not require paper, a printer or other superfluous resources.
- Digital documents do not need to be delivered and communication is possible through electronic channels.
- With the use of DMS, digital documents can be found more quickly and archived on the basis of very different criteria.

When signing digitally, one must consider that the generated file can be singly read using convenient methods by all interested parties and that it can be opened without

issues in the future as well. If a file has been signed in one format, then it cannot be converted into another format without losing the signature. It is important to use to correct file formats for signing so that the file meets all the requirements. There are several possible purposes for using digital signatures, e.g. no need to specifically meet in person for a signature or to send documents with ordinary mail, thus significantly saving time. Digital signing allows for automating activities and to reduce spending time on regularly signing a large number of documents physically. If necessary, the document should be encrypted so strangers cannot read it.

2.2 Problems Related to Digital Signing

From a local government perspective, several issues have been highlighted that are related both to the organizational as well as technical aspects. Also, this is widely discussed elsewhere as well [10]. From a technical point of view, the digital signature format can be limited, as it is possible that different environments can show the document in different ways. The most important and serious risk with using digital signatures is that the signature rights can be stolen with a private key – the owner of the certificate must carefully monitor that the private key does not leave the possession of the signature owner. Nowadays, different methods have been devised to tackle this and the risk is diminishing.

The problems that may arise when using digital documents tend to differ between small- and large-scale uses. In both cases, one must bear in mind that not all clients and partners may have an ID-card or Mobile-ID and that parallel paper document use must be retained. The latter can only be avoided when an authority issues unilaterally signed documents. This could create duplication. For small-scale use, e.g. internal use of an organization and signing contracts with larger partners and clients, different issues occur and the use of a computer and ID-card and passwords is an extra effort, takes more time and is not suitable in outdoor conditions. In addition, a problem with digital documents may arise regarding the accompanying time stamp – the physical time of signing is visible to everyone who looks at the document. In local governments, this is linked to certain decisions and the granting of rights, where an important administrative act is formalized after the fact.

2.3 Problems Related to Archiving

Many local governments have brought out archiving as an issue for digital signing. Archiving digitally signed documents requires some extra effort [10–12]. With archiving, one must take into account that in addition to digital documents, paper documents also need to be managed. Thus, hybrid files are created. Inevitably, it is more difficult to use two separate management systems rather than only have one; it is reasonable to manage both digital and paper documents in the same information system. A solution is that the location, existence, and main information (what type of document, what parties, when, etc.) about the paper documents is registered in the same information system and in the same way as for digital documents, in the simplest case by using a small ordinary document file containing the main information. If an organization already employs a paper document registration system, adding digital

document management to the same system is likely to be the most effective – provided that this is technically possible.

Regarding potential software solutions, it is important to consider whether an existing software already in use could be suitable for archiving digital documents, or if the standard activities used in the organization already could not be employed for archiving the files. For instance, digital documents could simply be stored in a file system, grouping them chronologically into year- or month-based catalogues and coding the critical information (client name or code) into the file name. This can be used if there is a relatively small amount of digital documents. In addition, an existing specialized archiving software could be used and generally, a DMS already contains an archiving function. If it does not, a suitable archiving software could be created for the organization.

2.4 Digital Signatures and Digital Document Authenticity

Is a digital signature always a sufficient guarantee of the digital document authenticity for digital archiving? From the perspective of the Estonian national archive, it can be not sufficient [13–15]. A digital signature does protect the signed information (the content of the document) from unwanted changes but it is not enough to completely understand the document. A part of the information no less important than the content is hidden in the links between the documents – these allow us to understand the activities of the organization, during which the document was created. A digital signature does not release an organization from good and controlled management of the document, which is one of the guarantees of document authenticity. In the case of signed, but especially for digital documents with a permanent retention period, the organization must implement and ensure specific policies and procedures that enable verifying the creation, sending, forwarding, retention, and separation of documents [14].

In the future, it is possible to use archival time-stamping for ensuring the long-term preservation of documents in the BDOC format. This mechanism is based on the principle “fortify that, which could be weak” [13]. Consecutive time stamps protect the entire contents from weak hash algorithms and from breaching cryptographic material and algorithms. Certain costs are associated with this, as there is a need to enter into a contracts with an organization that offers certification and time stamping services (presently, in Estonia, this organization is Certification Centre). Monthly bills also need to be paid for the validity confirmation service, however, the costs are not that big.

3 Technological Infrastructure

In this section we give an overview of the Estonian technological infrastructure that enables digital signing of documents as represented in this article, compare also with [16]. Digital signing of documents is two-tiered. Each document is signed organizationally by Estonian’s streamlining data ex-change backbone, then, each document is signed by the person who is the accountable stakeholder in the respective organizational process. It is the latter, the individual signature, that we treat as digital signing, the first can then be coined e-Stamping.

In Estonia, e-Government is enabled and streamlined by a systematic distributed architecture and infrastructure, often coined X-Road, compare also with [17]. X-Road is called a data exchange layer, but is way more than just a data exchange layer protocol. It is the entirety of organizational and technological assets that enable a secure, tamper-proof and repudiation-proof data exchange over the public internet. Between parties involved in e-Governance processes, compare with Fig. 1. Basically, X-Roads consists of a data exchange layer protocol based on SOAP, the specification and implementation of an organizational security server, a PKI (public key infrastructure) that shows, in particular, in trust services for certificate validation and time stamping plus procedures for registration of X-Road members, organizational security servers and data services plus regulations for the establishment of organizational data bases in the X-Roads environment. The idea is that all e-Governance is streamlined by X-Road. Organizations that want to take part into Estonian's e-Governance need to become members of X-Road and must adhere to its standards and regulations. X-Roads follows a lightweight, distributed approach that aims at keeping centralization at a minimum. The key principle is that organization keep ownership and responsibility of exchanged data. Therefore, security servers are run by the single X-Road members.

Messages are sent directly from one organization to another via the organization's security servers. This means, that X-Road is not a value-added network, not an ESB (Enterprise Service Bus) no message-oriented middleware (MOM) or the like, compare also with [18–21]. The security servers take care for encrypting/decrypting, e-stamping, validating and time stamping outgoing and incoming messages. They exploit regulated trust services for that purpose that are provided by third party certification authorities. These trust services are a certificate validation service based on OCSP (Online Certificate Status Protocol) and a time-stamping service. The X-Road specified trust services adhere to the EU eIDAS regulation on electronic identification [22]. Each organization keeps full control over the data in its databases and connected information systems, in particular, it is the single organization that grants access rights for their data

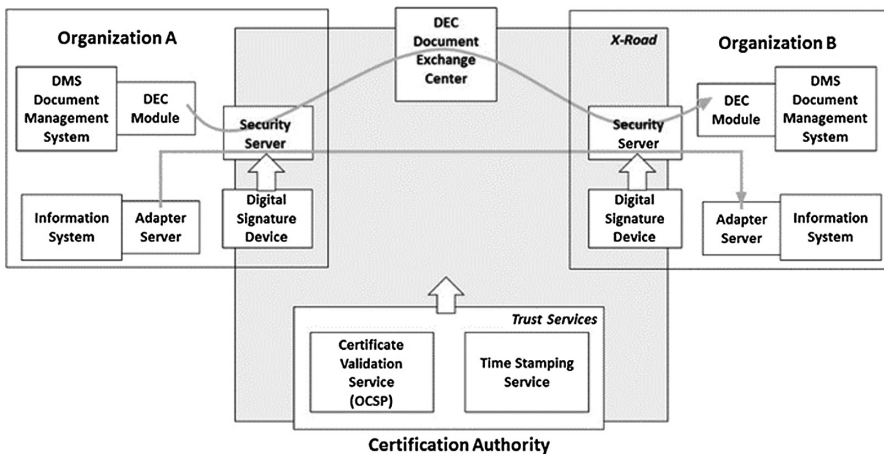


Fig. 1. Data exchange layer X-Road with trust services and document exchange center

to other organizations. Each organization maintains and controls these access rights in its own security server. Each message exchanged via X-Roads is digitally signed by the security server of the sending organization.

For the exchange of documents an additional service, the document exchange center (DEC) has been established. The DEC slightly deviates from the X-Roads key principle of minimal centralization. It provides a store-and-forward mechanism therefore a kind of enterprise service bus component. Documents are sent to DEC where they are temporarily stored and preserved. Organizations that are entitled to, can then pick documents for the DEC. Organizations that want to participate in document exchange via DEC must be registered members of XROAD, in addition, they must become also registered users of the DEC.

4 Digital Signature Statistics Based on DMS Databases

The study presented in this article only reflects the digital signing of documents exchanged using the DMS, but many documents are processed outside of the document management system using other components [17]. For instance, if one were to change one's place of residence and make an application about this to the local government, this application is registered as an entry in the Population Register and may well not be reflected in the document management system. The same applies to construction permits, authorizations for use, and applications for design criteria, which are all registered in the Construction Register. The data that are registered in the social services and benefits data register (STAR) are also excluded from the document management system. In Estonia, information exchange with other systems is mainly carried out over the X-road for relational systems [16]. However, this is not always the case, and therefore it is necessary to also observe the situations where information with external systems is exchanged outside the X-road, in order to have adequate statistics about the public sector document exchange. Although X-road is the preferred communication channel, there are still information systems that communicate directly, i.e. exchange documents by other interfaces. Below, data is shown in various groups (local government totals, more successful local governments, less successful local governments, etc.), bringing out volume of digitally signed documents (Fig. 2, Tables 1, 2, 3, 4 and 5).

5 Factors Influencing Digital Signing

During the application of paperless management, there are several factors that determine its success. Same applies to digital signing as it is one important part of DMS-s. Although this paper discusses results based on survey in 2016, there have been other experiments before. The study was conducted in Rapla County during 2009–2011 [23, 24] also showed that local governments need a solution that would unify their services. After taking e-forms into use, an increase by leaps and bounds in digital signing was also evident (see Figs. 3 and 4) as the procedural steps of the respective applications were performed digitally and the answers to citizens were also transmitted digitally [24].

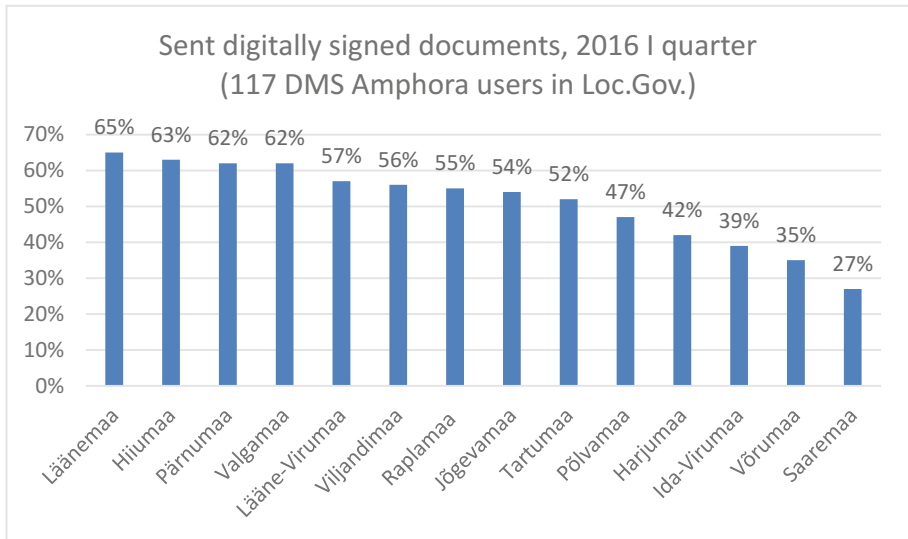


Fig. 2. Summarization according to counties

Table 1. Consolidated data

Consolidated data	
Total number of sent documents	24801
Total number of digitally signed sent documents	12245
Percentage of digital signing for sent documents	49%
Number of local governments in the sample	117
Average number of residents in local governments in the sample	3298

Table 2. Local governments that use digital signing the most

Local government	County	Sent signed	Number of residents	Capability index ranking
Tori parish	Pärnu	86%	2327	127
Elva town	Tartu	85%	5768	39
Värskä parish	Põlva	81%	1374	113
Tahkuranna parish	Pärnu	81%	2389	114
Audru parish	Pärnu	81%	5858	52
Karksi parish	Viljandi	80%	3400	88
Vigala parish	Raplamaa	79%	1267	66
Paikuse parish	Pärnumaa	75%	3899	74
Kehtna parish	Raplamaa	75%	4459	49
Vinni parish	Lääne-Viru	75%	4757	21

Table 3. Local governments that use digital signing the least

Local government	County	Sent signed	Number of residents	Capability index ranking
Pihla parish	Saare county	2%	1411	109
Ahja parish	Põlva county	0%	1011	191
Kihelkonna parish	Saare county	0%	773	86
Laimjala parish	Saare county	0%	711	183
Meeksi parish	Tartu county	0%	594	194
Mustjala parish	Saare county	0%	691	207
Sõmerpalu parish	Võru county	0%	1799	118
Torgu parish	Saare county	0%	350	208
Torma parish	Jõgeva county	0%	1991	137
Varstu parish	Võru county	0%	1075	180

Table 4. Most digitally signed letters per resident in local governments with up to 10,000 residents

Local government	County	Sent per resident	Number of residents	Capability index ranking
Lüganuse parish	Ida-Viru	0.235	3014	23
Vihula parish	Lääne-Viru	0.117	1955	36
Piirissaare parish	Tartu county	0.098	102	210
Vormsi parish	Lääne county	0.096	415	75
Misso parish	Võru county	0.096	645	126
Meremäe parish	Võru county	0.092	1093	181
Mõniste parish	Võru county	0.084	873	166
Kernu parish	Harju county	0.084	2040	27
Värskla parish	Põlva county	0.080	1374	113
Are parish	Pärnu county	0.069	1297	122

The implementation of e-services in the governing arrangement of local governments has a positive impact, because it facilitates solving the issues of the citizens more operatively and permits the better monitoring of the whole course of proceedings.

Table 5. Number of digitally signed letters per resident in local governments with more than 10,000 residents

Local government	County	Documents per resident	Number of residents	Capability index ranking
Viimsi parish	Harju county	0.010	18430	4
Viljandi town	Viljandi county	0.028	18111	32
Rae parish	Harju county	0.035	15966	1

(continued)

Table 5. (continued)

Local government	County	Documents per resident	Number of residents	Capability index ranking
Rakvere town	Lääne-Viru county	0.021	15942	40
Maardu town	Harju county	0.005	15676	29
Saue parish	Harju county	0.032	10451	7
Haapsalu town	Lääne county	0.037	10425	41

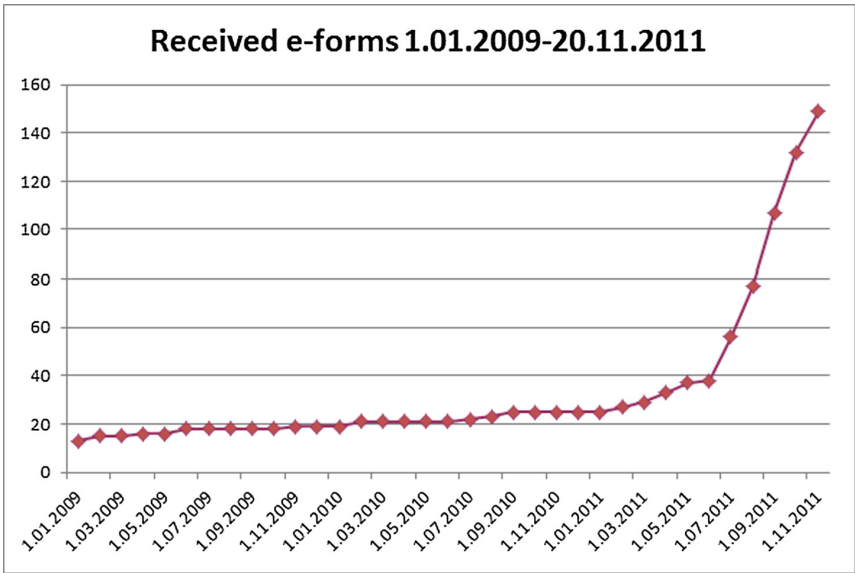


Fig. 3. The growth of e-forms received in EDRMS Amphora

5.1 Outcomes of the Survey

In this section we delve into the factors influencing digital signing by seeking for generalizations based on survey. This analysis is based on the survey conducted in spring 2016, which examined the various factors that influence the implementation of digital signing in local governments. The answers obtained from the survey illustrate the main factors which obstruct or advance digital signing in DMS. The answers reflects different criteria and measurements sets concerning the digital signing. For instance, answers to the questions “Do you sign government legislation digitally” the “yes” was answered 39,3%. Question “Do you sign outgoing documents digitally” got 58,2% “yes” and “partially” 40%. “Do you think preserving digital signatures is safe?” gave 46,4% “maybe” and 49,1 “yes”. Question “Do you think digital signatures can be used as evidence (e.g. in court)” got 79,8% “yes” answers. To the question “Is forwarding

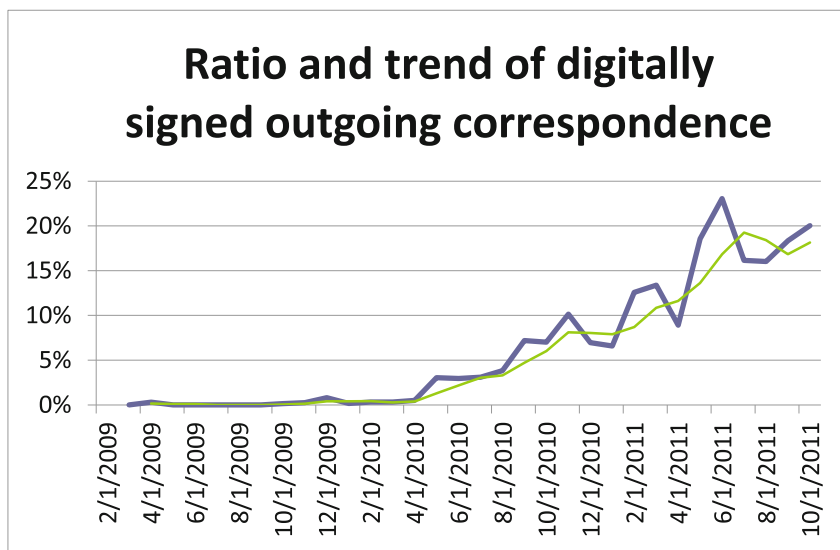


Fig. 4. The increase in digitally transmitted correspondence

digitally signed documents to citizens an issue” gave 57,4% of “Yes answers”. On the following figures are shown different criteria which were investigated such as variety of age and different factors influencing the digital signing (Figs. 5, 6, 7 and 8).

Also, in the inquiry, there was an open text question “What should be done to introduce the digital signing in depth”. The most used suggestions were brought out as follows:

- In order to raise elder people capability, the access to a computer, internet should be guaranteed more widely
- Digital signing should be introduced (forced) by rural municipality mayor within organisation (local government)
- Raise awareness regarding the digital archiving – explain long-term preservation methods
- It is necessary introduce and market digital signing for both - officials and citizens
- Develop more Public Internet Access points (for instance use county’s library), which gives the opportunity to consume public e-services (different application)

Allover, from the survey, we learned that the following are the delaminating factors for digital signing:

- *Digital Divide*
 - elder people vs. younger people
 - lack of ubiquitous internet access
- *Lack of sponsorship.* Lack of sponsorship by leaders in administrations.
- *Lack of awareness concerning digital archiving.*
- *Lack of iniquitousness towards population.* Barrier in the usage of digital signing between officials and citizens.

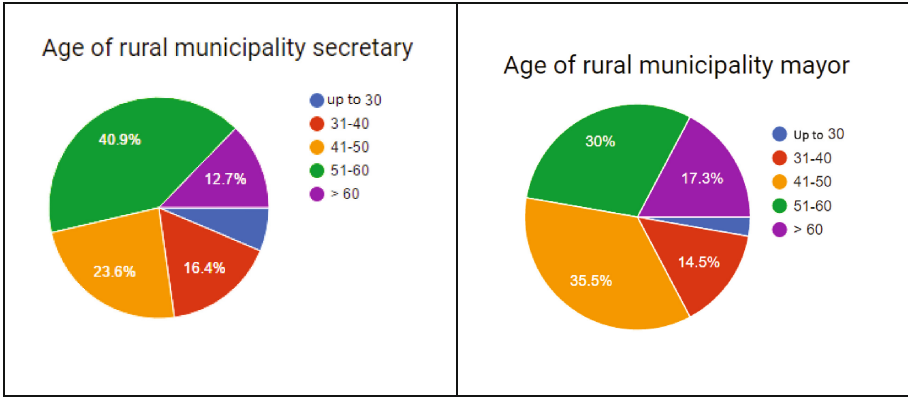


Fig. 5. Age difference

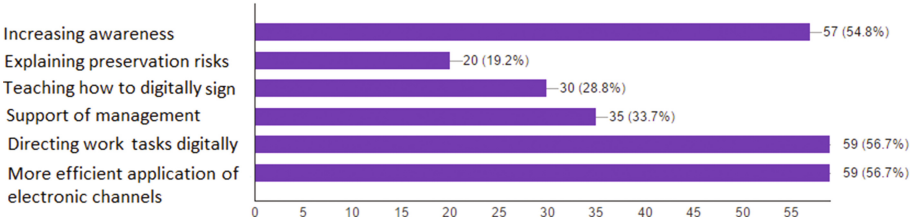


Fig. 6. How to raise digital signing?

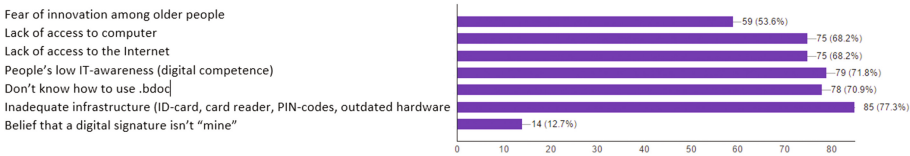


Fig. 7. Please mark the factors which could prevent forwarding digitally signed documents to citizens

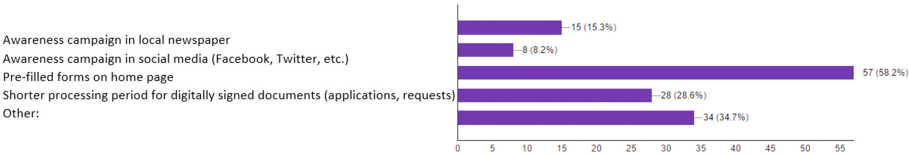


Fig. 8. How do you motivate your citizens to use digital signatures?

5.2 Organisational Development and Change

From the previous chapter it occurred that there are many factors influencing digital signing. The Digital Divide was stressed by drawing a gap between older and younger people habits, also lack of ubiquities internet access was pointed out. However, an important factor was brought out by not supportive management, and also awareness regarding the digital preservation. Also, implementation of digital signing faces controversies between the requirements arising from static legislation on the one hand, and the use of progressive ICT tools on the other hand. All these factors can be more or less related to the organizational development and change management in general. Organizational Development (OD) aims to expand the knowledge and effectiveness of people to accomplish more successful organizational change and performance [25].

OD is a process of continuous diagnosis, action planning, implementation and evaluation, with the goal of transferring knowledge and skills to organizations to improve their capacity for solving problems and managing future change. According to French and Bell (2011) organization development (OD) can be defined as “organization improvement through action research” [26]. During the 2003–2016 the developments of DMS Amphora as whole were mirroring the same logics where outcomes were constantly evaluated, improved and by that initiated a new cycle of investigations (see Fig. 9).

In addition to development activities of DMS Amphora the implementation process itself has been highly considered as a tool for managing organisational changes. Organisations have their own culture and specific ways do things. Especially in public sector government offices, there everything is strictly established based on legal environment and state functions. Alongside with the legal obligations many unwritten rules occurs that nobody is consciously aware of, still these dictate many decisions. All cultural habits have to change if digital transformation is going to take hold over the

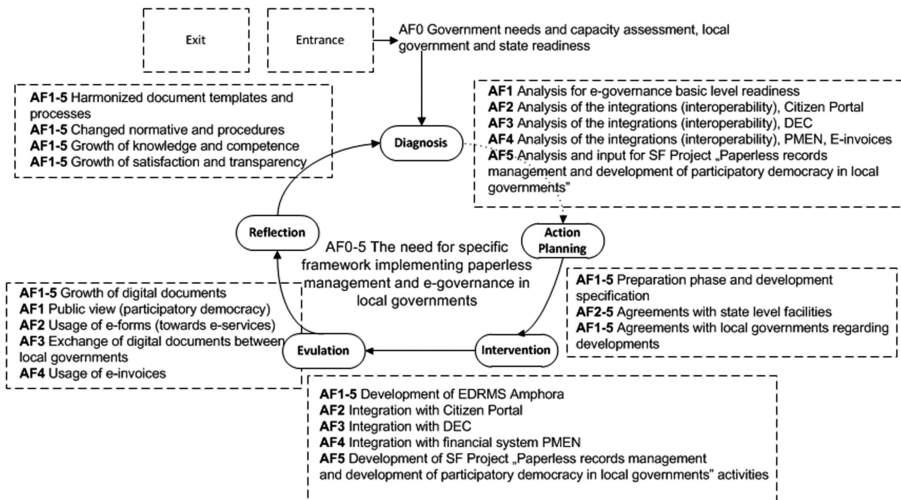


Fig. 9. Research and development activities of DMS Amphora

long term. But overcoming obstacles and new sometime unwritten rules is not easy. However, a fear can also hinder a progress as for someone digital signing is the unknown, and for many term digital is a big unknown. Many people afraid it will make their role redundant and people fear to learn new skills while analyzing their capacity to do that. From the survey it occurred that the factors which could prevent forwarding digitally signed documents to citizens were mostly related to people's low IT literacy (71,8%) and that people don't know how to use the format.bdoc (70,9%). Also the compatibility of the software-hardware was highly mentioned (85%) but it could be related to the IT literacy in general. It is impossible to overcome people's fears if there is a lack of communication. If people are struggling with the unknown, there is a need to make the unknown as known. Therefore a great deal of regular and consistent communication will helps to overcome this gap. During the years there have been conducted several implementation stages in local governments since 2009 [2, 23, 24].

Conducting changes is only possible by management exemplifying and communicating a new reality over the long term and doing it constantly. Set a new direction and step back does not work, management needs to remain engaged with the process. Another fact which may slow down change is related to novelty and obscurity in order to implement new way of thinking. According to Calista et al. [27] early adopters of the digital government often found it difficult to maintain their performance, while some late adopters have experienced dramatic performance improvements. Total implementation of the digital signing takes much effort and in many cases the business processes should be re-engineered. Development of the harmonised implementation methodology for local governments to use DMS Amphora has been an important goal for years. In the beginning of 2011, the objective was to partially develop the methodology for increasing and measuring the digital performance of local governments on the basis of nine local governments of Rapla County – the project was called “e-Raplamaa” and some results were presented at an e-Governance conference in Tallinn [23]. An important objective of this project was to create the methodology and criteria for measuring the changes in proportion and effectiveness of digital administration in local governments. One of the aims was to give an answer to whether and how much the training and application of DMS increases the proportion of digital administration in local governments. The statement was that the effectiveness increases at least 20% in a three-month period after the application and, thereafter, there will be no increase, i.e. the growth stops. In order to prove that two application/training days were organised in each local government. In conclusion the collected results did not give sufficiently adequate feedback to draw direct connection between trainings and efficiency growth in order to make correlation. Still, it helped to develop the Digital Performance Index [23]. Based on these results was generalized that local governments, who have had more training days and are using DMS functionality widely are also more effective users of the digital signing. In addition to every-day documents and records management, the head of the organizations have to understand the responsibilities which are related to digital preservation. As it was seen from the survey there is still lack of awareness concerning digital archiving.

5.3 Raising Awareness on Digital Preservation

The conducted survey demonstrates the necessity to raise awareness regarding the digital archiving by explaining long-term preservation methods. It is clear that the advantage of the electronic records is that they are reusable. Also, it is possible very quickly adapt a record or compile a new record on the basis of an existing one. It can be digital advantage or at the same time vulnerability because adaptations or changes are not always observable and retained. Still, the efficiency and time saving on the digital workflows is worth to implement. Thus, local governments can raise ICT capacity by raising the awareness of their officials. Besides, the growth of citizen satisfaction is tied to the growth of the digital performance of local governments [24]. The implementation of digital document work proceedings is facilitated by the rules and instructions described on the state level wherein several problems still require solutions in order to reach a wider assessment of the synergies and cooperation between local governments and the state. These rules and standards should be explained more thoroughly local governments officials. Also, more trainings are needed. These training can be conducted online based as well. One of the main focuses during the development of DMS Amphora has been a common implementation methodology for effortless organisational change [28]. It provides an efficient learning environment for the users for understanding the functions of local governments and actions with digital environments like DMS and integrated systems. One part of that is digital archive module. The developed implementation methodology has helped to increase the awareness of the users by providing a common ground for understanding the benefits. In addition to described methodology there has been developed common e-learning environment for local governments [29]. It contains information (instructions, training videos, etc.) about DMS interface and functions, putting it into use and managing various functions. Besides, e-learning environment enables users to measure the level of their knowledge, skills and user experience. And, users can exchange their experiences in e-learning environments. Therefore, the proposed approach focuses largely on the pre-generated environment and process-based tutorials in an e-learning environment in order to train users on DMS Amphora. With some minor adjustments, the same methodology could be implemented on other DMSs as well [29]. Which in turn helps to raise awareness concerning the digital preservation as well.

6 Recommendations for Implementing Digital Signatures

In order to implement the digital signing efficiently, it is necessary to consider the most suitable scenarios regarding saving/archiving documents. In most cases, there is no need to develop or implement some kind of special software, and using freely available standard software will suffice. Still, the use of DMS allows for digitalising the processes inside the institution and, thus, is one of the most popular inter-governmental services in e-Government projects [30, 31]. Implementing digital signatures in the DMS requires certain changes which can be divided into organizational and technological. On the information technology level, the work of users should be made convenient and where possible, automatic storage of deliveries and work task flows should

be introduced, as these support digital signing. On the organizational level, potential activities are mainly linked with training and increasing user awareness, both regarding simplifying work flows and digital archiving. If automatic work flow simplification is not possible, awareness campaigns are required and the users need to be taught how to a document is sent to be digitally signed when registered in the DMS or forwarded from the DMS. Digital signing is closely related to the implementation of digital records management. If the work processes are digital, digital signing is one logical step in the whole process. When discussing the digitalization of processes, it is important to note the complexity of business processes which in many cases are related to the size of the organization and the complexity of the offered services. For organizations with a rather large number of users, the complexity and large amount of business processes will be the deciding factors, nevertheless the people signing digitally tend to be the leaders of the organizations.

It is important to consider mapping, selecting, and analyzing the business processes suitable for the paperless alternative. The work load ranges from a few days to half a year, depending on the organization and the complexity of the task. Vitrally, the preparation and carrying out of archiving digital documents must be planned. If the organization already has the required software or experience of using ordinary software, developing the principles for digital archiving is going to be easier.

Transitioning to digital signing in Estonia is also supported by a European Commission directive eIDAS [22]. The standards listed in this directive also include the bdoc-format digital signature used in Estonia. European public authorities are required to recognize digital signatures that meet this standard, thus providing an Estonian citizen with the right to bring an action against someone in a court in Barcelona that is signed digitally. On the other hand, Estonian public authorities have to learn to receive other types of digital signatures received from Europe. Estonian digital signatures must start accepting digitally signed documents with an equal or “stronger” signature from other European Union countries. Estonian citizens in turn get the opportunity to turn to other European public authorities with their digitally signed documents.

7 Future Work

The implementation of digital signatures is a key enabler for e-Government initiatives, similarly it is at the core of the paperless office. A stable infrastructure for digital signatures consists at least of a convenient to use public key infrastructure. Convenient to use means that the public key infrastructure comes with well-defined, transparent and available routines for registration, certification as well as services for validation. If it is expanded to quasi-standardized automatic interfaces to information systems, even better. If it is further expanded to quasi-standardized features in end-user tools, once more, even better. Once a stable infrastructure for digital signing is established, it enables the transformation of e-governance processes into purely digital processes. This is so for the realm of e-Government as well as e-Commerce. Here comes the point: whenever an organizational process reaches a certain criticality, a certain level of compliance relevance, we can almost be sure that some signing of documents is involved.

Implementing digital signatures immediately increases efficiency. However, it does not guarantee at all an improvement of the effectiveness. The implementation of digital signatures can be done, and this is actually the most usual case, in a non-disruptive manner with respect to the existing processes. As a result, processes are completely digitalized, however, they are themselves not changed essentially. Here is where a next wave of enactment and enablement is possible, both inside organizations as well as cross-organizational, compare also with [32]. Here, digital signing is really just the basis, albeit an essential one. The real efforts are in the assessment and re-design of existing processes, a huge refactoring and change management endeavor, when it comes to the cross-organizational cases, which are actually the most interesting ones, i.e., the ones with the highest potential to increase effectiveness. We have started basic, use-case driven, research in this direction. The point is that we need to start from scratch, even in some basic cases, and need to conduct system analysis. Currently we investigate how to exploit best practices, techniques and tools from the realm of enterprise architecture (TOGAF, DODAF, Zachman framework) [33–35] in the analysis and refactoring of cross-organizational administrative processes. There is also potential for innovative supporting tools, like cross-organizational business activity monitoring. As a concrete next step, we investigate how to integrate a business rule engine into the document ex-change center DEC.

Also with respect to supporting business process technologies [36], there are still many opportunities. To see this, we start with identifying two different kinds of qualities of digitally signed documents. The first kind is, what we would like to call asset-related, the second is what we would like to call process related. Asset-related documents serve as proof of ownership or right. They are independent of particular organizational processes, albeit they play crucial roles in organizational processes over and over again. Process-oriented signatures stem from the organizational processes themselves. Organizational processes emerge and are shaped over the years; many of are built around some RACI principle (responsibility, accountability, consulted, informed). Then digitally signed documents have the purpose to allow for next activities. Traditionally, they serve as a message, a trigger so to speak, but also have the purpose of documentation and proof, two facets that are important with respect to compliance issues. At least, with respect to the kind of process-related documents we should think about their transformation into digitally signed workflow steps and work-flow triggers. Which leads us to a vision of signature-integrated workflow management system. A similar vision is currently developed by the smart contract community, starting from a particular cross-organizational perspective, compare with [37, 38].

8 Related Works

Digital signing Problems related to digital signing are widely discussed from the perspective of the integrity and authenticity [10], and digitally signed documents requires extra effort for digital archiving [11, 12, 39]. In order to guarantee the organization in Estonia must implement and ensure specific policies and procedures [14], besides the initiative comes from the EU level as well. However, investigating other

countries experiences several circumstances indicates the rise of the digital signing. Levy [40] recognizes that *“to benefit from its massive advantages, digital signatures still have challenges to overcome”*.

According to [40] the financial services industry has been the pioneer in the adoption and development of digital signature solutions, and he expects other industries, such as telecommunications, commerce, utilities, notaries and healthcare, to follow suit. Estonian case shows that besides the financial service industries the public sector has been adopted digital signatures quite well as well. However, based on the report [40] the findings are claiming that *“challenges include the integration and alignment of the technology with existing processes, together with a transparent analysis of the related regulatory situation and its legal consequences when implementing digital signatures”*. On this basis, it should be admitted that same matter must be considered in Estonian case. Although, the digital signatures are more efficient way to work, still the different obstacles should be resolved first. Besides the legal framework, the problems related to digital signing are tight to technology issues and people’s resistance. This is discussed in the study conducted in USA where survey [41] shows that *“digital signatures have emerged as one of the technology priorities for local and state governments for the purpose of gaining both operational efficiencies and legal assurances”*. Like to this paper, the aforementioned survey was conducted among the local and state authorities and shows many similarities in findings to this work here as well. Still, the main advantages of this presented work are presenting besides the qualitative research results based on statistics from the DMS databases. This in turn gives real-live numbers of the actual signing of the local governments and qualitative research helps to understand the difference of the curve within local governments. To conclude, the international studies are indicating that digital signing is an important future trend and its development should be considered, while making local governments work routines more efficient along with the cost savings on paper products.

In [42] we report on the implementation of e-Invoicing in Estonia, again based on a document management systems approach. The described approach follows stepwise enterprise application via workflow modules and interfacing with enterprise resource planning (ERP) systems.

In [43], the authors demonstrate how to integrate digital signature workflow management into enterprise content management systems, based on secure digital tokens via smart cards. Documents can be signed each smart card having digital signatures capabilities with the citizen card as a particularly important case. In [44] the authors report on intrinsic barriers of the implementation of digital signatures. The Russian e-Government initiative is used as a case study for this purpose.

9 Conclusion

Digital signing has already claimed a significant place in today’s society but signs are showing that the importance of digital signing is bound to increase even more in the near future. Firstly, the simplicity and security of the signature make it a preferred choice ahead of signing on paper. Secondly, digital document exchange also translates into savings in the budget. It can also help increase the security of the documents: a

digital signature is tamper-proof and creates the option of creating an unlimited number of authentic verifiable copies of the document. This in turn enables to reduce the work load and increase the efficiency of local governments. Although the survey revealed that many of the smaller local governments do not have such administrative capabilities, the proportion of digital signatures is still notable. The main findings of the survey can be summarized as limiting factors concerning digital signing, which are digital divide, lack of sponsorship, lack of awareness concerning digital archiving and lack of iniquitousness towards population. For more efficient implementation, in addition to technological adaptations, the awareness of officials about issues related to digital archiving as well as software capabilities and interoperability for reading documents should be increased. Thus, in order to improve the implementation of digital signing in an organisational setup, there is a need to increase the IT-literacy of local government officials. The latter leads to the better management of the organisational changes and helps beside the digital signing more efficient digital workflow.

References

1. Ministry of Economic Affairs and Communication: Estonian Digital Agenda 2020, Tallinn (2013)
2. Pappel, I., Ingmar, P.: Implementation of service-based e-government and establishment of state IT components interoperability at local authorities. In: The 3rd IEEE International Conference on Advanced Computer Control (ICACC 2011), Harbin, China (2011)
3. Ministry of Economic Affairs and Communication: Outcome of the 2014 Estonian document exchange classification Project DECS, Tallinn (2015)
4. Ministry of Interior of Estonia: Classification of Estonian administrative units and settlements 2015v1, Tallinn (2015)
5. Estonian Digital Signature Act, Tallinn (2000)
6. Estonian Certification Center: Usage of ID in Estonia, Tallinn (2016)
7. Pappel, I., Pappel, I., Saarmann, M.: Digital records keeping to information governance in Estonian local governments. In: Shoniregun, C.A., Akmayeva, G.A. (eds.) *i-Society 2012 Proceedings: i-Society 2012*, 25–28 June 2012, London (2012)
8. Merkle, R.C.: A certified digital signature. In: Brassard, G. (ed.) *CRYPTO 1989*. LNCS, vol. 435, pp. 218–238. Springer, New York (1990). https://doi.org/10.1007/0-387-34805-0_21
9. Naccache, D., M'Raihi, D., Vaudenay, S., Raphaelli, D.: Can D.S.A. be improved? — Complexity trade-offs with the digital signature standard —. In: De Santis, A. (ed.) *EUROCRYPT 1994*. LNCS, vol. 950, pp. 77–85. Springer, Heidelberg (1995). <https://doi.org/10.1007/BFb0053426>
10. Vigila, M., Buchmanna, J., Cabarcasb, D., Weinerta, C., Wiesmaier, A.: Integrity, authenticity, non-repudiation, and proof of existence for long-term archiving: a survey. *Comput. Secur.* **50**, 16–32 (2015). Elsevier
11. Lekkasa, D., Gritzalisb, D.: Long-term verifiability of the electronic healthcare records' authenticity. *Int. J. Med. Informatics* **76**, 442–448 (2007)
12. Lynch, C.: The future of personal digital archiving: defining the research agendas. In: *From Personal Archiving: Preserving Our Digital Heritage, Information Today*, vol. 50, May 2015
13. Estonian National Archive: The 2005–2010 National Archives' digital archives strategy, Tartu (2003)
14. Estonian National Archive: Digital archives vision, Tallinn (2005)

15. Estonian National Archive: Archives management requirements for digital records, Tallinn (2008)
16. Draheim, D., Koosapoeg, K., Lauk, M., Pappel, I., Pappel, I., Tepandi, J.: The design of the Estonian governmental document exchange classification framework. In: Kõ, A., Francesconi, E. (eds.) EGOVIS 2016. LNCS, vol. 9831, pp. 33–47. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-44159-7_3
17. Kalja, A., Robal, T., Vallner, U.: New generations of Estonian eGovernment components. In: Proceedings of PICMET 2015 – Portland International Conference on Management of the Technology Age, Portland (2015)
18. Atkinson, C., Draheim, D.: Cloud-aided software engineering: evolving viable software systems through a web of views. In: Mahmood, Z., Saeed, S. (eds.) Software Engineering Frameworks for the Cloud Computing Paradigm. CCN, pp. 255–281. Springer, London (2013). https://doi.org/10.1007/978-1-4471-5031-2_12
19. Draheim, D.: The service-oriented metaphor deciphered. *J. Comput. Sci. Eng.* **4**, 253–275 (2010)
20. Bordbar, B., Draheim, D., Horn, M., Schulz, I., Weber, G.: Integrated model-based software development, data access, and data migration. In: Briand, L., Williams, C. (eds.) MODELS 2005. LNCS, vol. 3713, pp. 382–396. Springer, Heidelberg (2005). https://doi.org/10.1007/11557432_28
21. Draheim, D., Nathschläger, C.: A context-oriented synchronization approach. In: Electronic Proceedings of the 2nd International Workshop in Personalized Access, Profile Management, and Context Awareness: Databases (PersDB 2008) in Conjunction with the 34th VLDB Conference (2008)
22. European Parliament and Council: Regulation (EU) No 910/2014 on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market and Repealing Directive 1999/93/EC (eIDAS Regulation), European Union (2014)
23. Pappel, I., Pappel, I.: Methodology for measuring the digital capability of local governments. In: Proceedings of the 5th International Conference on Theory and Practice of Electronic Governance, Tallinn (2011)
24. Pappel, I., Pappel, I., Saarmann, M.: Development of information society and e-government by improving electronic records management solutions at Estonian local authorities. In: Kommers, P., Isaias, P. (eds.) Proceedings of the IADIS International Conference e-Society 2012, Berlin (2012)
25. Margulies, N.: Organizational Development: Values, Process, and Technology, p. 3. McGraw-Hill Book Co., New York (1972)
26. French, W.L., Bell, C.H.: Organization Development: Behavioral Science Interventions for Organization Improvement. Prentice-Hall, Englewood Cliffs (1998)
27. Calista, D.J., Melitski, J., Holzer, M., Manoharan, A.: Digitized government in worldwide municipalities between 2003 and 2007, pp. 588–600 (2010)
28. Pappel, I., Pappel, I., Saarmann, M.: Conception and activity directions for training and science centre supporting development of Estonian e-state technologies. In: Proceedings of the 5th International Conference on Theory and Practice of Electronic Governance, Tallinn (2011)
29. Pappel, I.: Paperless Management as a Foundation for the Application of e-Governance in Local Governments. Tallinn University of Technology, Tallinn (2014)
30. Hung, S.Y., Tang, K.Z., Chang, C.M., Ke, C.D.: User acceptance of intergovernmental services: an example of electronic document management system. *Gov. Inf. Q.* **26**(2), 387–397 (2009)

31. Yaacob, R.A., Mapong Sabai, R.: Electronic records management in Malaysia: a case study in one government agency. In: Asia-Pacific Conference on Library & Information Education & Practice 2011 (A-LIEP2011): Issues, Challenges and Opportunities, Malaysia (2011)
32. Sellen, A., Harper, R.: *The Myth of the Paperless Office*, pp. 17–18. MIT Press, Cambridge (2001)
33. Zachman, J.A.: Business systems planning and business information control study - a comparison. *IBM Syst. J.* **21**(3), 31–53 (1982)
34. Winter, K., Buckl, S., Matthes, F., Schweda, C.M.: Investigating the state-of-the-art in enterprise architecture management methods in literature and practice. In: Sansonetti, A. (ed.) *Proceedings of the 4th Mediterranean Conference on Information Systems*, Tel Aviv (2010)
35. Taveter, K., Wagner, G.: A multi-perspective methodology for modelling inter-enterprise business processes. In: Arisawa, H., Kambayashi, Y., Kumar, V., Mayr, H.C., Hunt, I. (eds.) *ER 2001. LNCS*, vol. 2465, pp. 403–416. Springer, Heidelberg (2002). https://doi.org/10.1007/3-540-46140-X_31
36. Draheim, D.: Smart business process management. In: *2011 BPM and Workflow Handbook, Digital Edition. Future Strategies*, Workflow Management Coalition (2012)
37. Milani, F., García-Bañuelos, M., Dumas, M.: Blockchain and Business Process Improvement. *BPTrends Newsletter* (2016)
38. Norta, A., Ma, L., Duan, Y., Rull, A., Kõlvart, M., Taveter, K.: eContractual choreography-language properties towards cross-organizational business collaboration. *J. Internet Serv. Appl.* **6**, 1–23 (2015)
39. Wallace, C., Pordesch, U., Brandner, R.: Long-term archive service requirements (2007)
40. Levy, D., Schaettgen, N., Duvaud-Schelnast, J., Socol, S.: Digital signatures - paving the way to a digital Europe. Arthur D. Little (2014)
41. American City & Council: Benchmark Survey: Digital Signatures. ARX (2014)
42. Pappel, I., Pappel, I., Tampere, T., Draheim, D.: Implementation of e-invoicing principles in Estonian local governments. In: *Proceedings of ECDG 2017 – the 17th European Conference on Digital Government*, Lissabon (2017)
43. Sousa, P.R., Faria, P., Correia, M.E., Resende, J.S., Antunes, L.: Digital signatures workflows in alfresco. In: Kõ, A., Francesconi, E. (eds.) *EGOVIS 2016. LNCS*, vol. 9831, pp. 304–318. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-44159-7_22
44. Gorelik, S., Lyaper, V., Bershadskaya, L., Buccafurri, F.: Breaking the barriers of e-Participation: the experience of Russian digital office development. In: Kõ, A., Francesconi, E. (eds.) *EGOVIS 2014. LNCS*, vol. 8650, pp. 173–186. Springer, Cham (2014). https://doi.org/10.1007/978-3-319-10178-1_14

Transactions on Large-Scale Data- and

Knowledge-Centered Systems XXXVI

Special Issue on Data and Security Engineering

Hameurlain, A.; Küng, J.; Wagner, R.; Khanh, D.T.; Thoai,

N. (Eds.)

2017, XI, 193 p. 60 illus., Softcover

ISBN: 978-3-662-56265-9