ISSN 2029-7564 (online)
SOCIALINĖS TECHNOLOGIJOS
SOCIAL TECHNOLOGIES
2012, 2(2), p. 319–334

DEVELOPMENT OF ELECTRONIC IDENTIFICATION MEASURES IN THE PUBLIC SECTOR IN LITHUANIA: REALITY, DEMAND AND THE FUTURE

Rimantas Petrauskas

Mykolas Romeris University, Lithuania, rpetraus@mruni.eu

Paulius Vaina

Mykolas Romeris University, Lithuania, pavaina@stud.mruni.eu

Abstract

Purpose—*to analyze eIAS implementation reports and development peculiarities; to discuss measures that impede effective implementation of eIAS in Lithuania.*

Design/methodology/approach—*logical and systematic analysis, meta-analysis.*

Findings—*the article discusses the integration and use of eIAS solutions by the public sector in Lithuania. Main findings: 1) eIAS products and services are an integral part of a complex heterogeneous national platform consisting of regulatory, technical, organizational, social and even practical challenges; 2) National environment for eIAS remains underdeveloped for real life usage and promotion in order to reach critical mass applicability; 3) possibility to use different levels of eIAS for public e-Services is vital for the development of e-Government.*

Research limitations/implications—*the general overview reveals implementation challenges and particularities of the eIAS in the public sector of Lithuania. The article does not analyse the exploitation stages of eIAS.*

© Mykolo Romerio universitetas, 2012
© Mykolas Romeris University, 2012
ISSN 2029-7564 (online)
https://www.mruni.eu/lt/mokslo_darbai/st/apie_leidini/
https://www.mruni.eu/en/mokslo_darbai/st/apie_leidini/index.php

Practical implications—*the article evaluates regulatory, organizational, social and practical peculiarities of eIAS introduction and use in the public sector in Lithuania. The article forms a basis in order to exploit eIAS products and services more effectively.*

Originality/Value—*offers insight into the eIAS topic and fills the information void of implementation of eIAS solutions in the public sector, as it is not widely analysed in Lithuania.*

Keywords: *e-Identification, e-Authentication, e-Signature, Electronic identification, e-signatures and related ancillary trust services (eIAS), e-Services, e-Government.*

Research type: *general review, viewpoint.*

1. Introduction

During the last decade, on the European Union (EU) level and on national levels, strong political efforts have been declared on the willingness to exploit information and communications technologies (ICT) and move the activities of the public sector into the electronic environment. European policy documents like Digital Agenda, e-Government action plan 2011-2015, along with the national strategic documents set high priority for integration of ICTs to serve individuals and businesses. Emphasis is put on low carbon economy, productivity, social cohesion, innovative technologies, open specifications, innovative architectures and etc.

Not only electronic services (e-Services) should be provided using ICT, but also most communication with interested parties shall be undertaken *via* electronic means. Implementation of any ICT solution in the public sector should bring added value to e-Government platform as most of the e-Government development models introduce transaction levels, where the highest level of transaction allows completing a transaction without leaving the computer. Introduction of such ideas in real life should ensure that government to citizens (G2C), government to business (G2B) and government to government (G2G) interaction be carried out by empowered ICT solutions and promotion of paperless technology. In order to access and to receive e-Services, the user must be recognized by the service provider, especially in the cases where the user needs to express their commitment or the service provider must know that service is provided to the intended individual. Implementation of ICT brings new challenges in the areas of policy, regulation, supervision, technology, etc. That has an impact on social and organizational environment.

Therefore, today we can observe differences in implementation and use of electronic identification, authentication, signatures and related ancillary trust services (eIAS) solutions in various European Union (EU) countries as being influenced by regulatory, technologic, semantic, organizational and social issues. Implementation principles and approaches underline that eIAS is an integral part of the complex national systems. Currently, in the EU emphasis is placed on cross-border services as a future goal. In this

perspective it is necessary to assess practical implementation of eIAS solutions by the public sector in Lithuania.

The purpose of the article is to focus on assessment of legal, strategic, organizational and practical aspects of the eIAS that are undertaken by the public sector in Lithuania. Analysis is based on historical review and evaluation of the legal system and strategic actions carried.

The article discusses the steps taken, looks into historical aspects of eIAS implementation, summarizes them and gives insight on the future development of eIAS. Thus, eIAS technology integration requires a separate discussion and will not be touched on in this article.

2. Theoretical Background

After more than a decade since the introduction of eIAS services in the EU, its meaning and understanding of most eIAS definitions have found common ground. The difference between e-Identification/Authentication and e-Signature is that e-Signature allows making users' intent or commitment on content, where e-Identification is a process of using person identification data in electronic form unambiguously representing a natural or legal person; e-Authentication allows validating a person's e-Identification.

Figure 1 is presented to show functionality of e-Signature levels. E-Signature solutions are created for closed or open systems, using symmetric or asymmetric coding (one/two code system). E-Signature trustiness level is influenced by the investment required for its implementation. Also, investment has an influence on its functionality, risks and usability meaning that the developer of an e-Signature solution can choose an appropriate (intended/desired) functionality to make the e-Signature platform attractive to the service users.

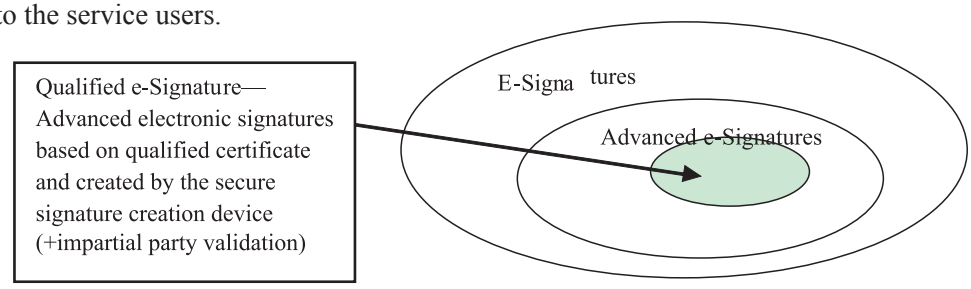

Fig. 1. Functionality levels of e-Signature (Dumortier, 2003)

In closed systems an identity of parties has been identified and parties trust each other in using the chosen e-Signature solutions. In open system (like public sector) parties do not know each other and trust level is low. Implementation of e-Signature based on qualified certificate (QeS) requires that a relation between the two parties must also involve registration, certification and validation authorities. Therefore, implementation of QeS differs in technology, functionality, security, risk and price involved. Practice shows that in implementation of any technology there is a need to justify its use. Any used technology should serve a purpose and offer functionality for money. But only

legal, technological, infrastructure, strategic changes are not enough for the development of the ICTs—organizational change is needed as well.

Lithuania's legal system focused on QeS for the public sector without questioning its necessity. The current situation shows that most e-Government services are not based on QeS. After the adoption of the Law on Electronic Signature (in August 2000) the Government of Lithuania did not ensure the necessary steps for the implementation of viable solutions that could ensure use of QeS by the government offices and constituency. That fact impeded the development of e-Government services.

In 2002, Information Society Development Committee under the Government[1] proposed new provisions[2] to the Law on Electronic Signature (which were adopted) that allowed using of any e-Signature solutions created by the private sector (like e-Banking, etc.) in closed systems. The private sector was eager to offer e-Solutions for their clients and have created viable eIAS systems that suited business needs, which were based on symmetric e-Signature solutions. Development of private e-Signature solutions that do not require QeS left public sector in a position where QeS remained underdeveloped.

Furthermore, Implementation Plan of the Concept of e-Government[3] had a provision indicating that until 2007 Ministry of Interior Affairs will implement national eID card system. National eID cards with QeS functionality were began to be distributed only in 2009. Another aspect of eIAS development in public sector in Lithuania is that national eID card is duplicated by the public servant card. Public servant eID should be used only for matters associated with public sector affairs. The number of national eID cards by 2012 reached 0,7[4] milliom, out of those 30. 210 (100% of public servants[5]) public servant eID cards issued by April 2011. Both eID cards offer a possibility to use QeS, but in national eID cards intended for citizens have wider possibilities for its use and functionality than public servant eID card. For example, in Estonia, single national eID card integrates all necessary functions all-in-one that citizen/servant needs. First eID card in Estonia was issued in 2002, first e-Signature was created in October 2002. In Estonia, national eID card roll-out was completed in 2006 (Martens, 2012).

Implementation of eIAS solutions requires testing its functionality on users. Thus, only in 2005 the Digital Certification Centre was registered as a Certification service provider, creating qualified certificates as a private initiative. That meant that public sector was lagging behind to implement the strategic information society development agenda. Until 2007 public sector was still in "empty field" position. To improve situation,

---

1 Currently Information Society Development Committee under the Ministry of Transport and Communications.

2 Changes to the Law on Electronic Signature adopted on 06-06-2002 (No. IX-934) (8.3 str. Elektroninis parašas visais atvejais turi šio straipsnio 1 dalyje įtvirtintą teisinę galią, jeigu parašų naudotojai tarpusavyje dėl to susitaria).

3 Lietuvos Respublikos 2003 m. lapkričio 25 d. nutarimas No.1468 "Dėl elektroninės valdžios koncepcijos įgyvendinimo priemonių plano patvirtinimo."

4 Report by the Communications Regulatory Authority (2012) on implementation of the Law on e-Signature during 2011.

5 Civil Service Department (2012) Report on Implementation of Law on Public Service and related legal acts 2011.

decision was made to accept private sector e-Signature solutions for provision of public e-Services (e.g. for declaration of taxes and other public e-Services).

Technology solutions may differ in reliability, price, ease of use and other characteristics. Lack of systematic approach in development of legal provisions, fragmented relations between eIAS and eID card developers along with different interest for eIAS of public and private sector lead to trust and confidence issues that disrupted implementation of eIAS solutions. eIAS solution for small number of consumers in social context without a take-up and use of e-Signature does not present the value for the large initial investment sums. Therefore, public sector should focus on management of e-Signature solutions that ensures implementation of viable solutions for critical mass of users.

3. Development of the EU and National Environments for e-Signature

eIAS is a service itself as eIAS solutions need to be created and deployed in order to be effective in use. Secure and trusted platform for e-Identification and e-Authentication should be functioning to create a possibility for a person to use any technology (e-Card, SIM card, or USB key) that allow to sign electronically (to prove intent or commitment on content). It should be mentioned that for the use of eIAS all supply chain from e-Service user to the provider should be capable of making electronic transactions, meaning that all necessary infrastructure and equipment should be in place. For eIAS products and services to be popular and gain critical mass they should be trusted, must have practical value and be comfortable to use. Stable regulatory environment along undue expense and trusted technology is necessary for the spread of e-Signature (Raymond, 2011).

3.1. Regulatory development, policy and supervision

3.1.1. Regulatory development

The history of e-Signature development began after the introduction of computers and electronic commerce in the late 90's. In the EU, legal act dedicated to e-Signature entered into force in 1999 (Directive 1999/93). Member States were obliged to transpose provisions of the directive on establishes a legal framework for electronic signatures in order to ensure the proper functioning of e-Signature on national level. E-Signature directive aim was to stimulate secure cross-border electronic communications, legal recognition of e-Signatures and to avoid divergent national regulation.

Laws on Electronic Signature were adopted around 1999–2002 in most European countries—Spain, Ireland, UK, Poland, Check Republic, and in Lithuania. Germany introduced e-Signature provisions in 1997. This fact shows that most of EU countries started e-Signature platform development on equal footing with equal opportunities.

EU legal documents should create a positive impact on the development of any internal market issues, including eIAS. Transposition process of any EU directive is

based on the rule that directives specify only a result to be achieved by the EU country, but it can choose the measures (Cairns, 1999). In case of implementation of the e-Signature directive, its aim is not achieved as e-Signature use is not widely spread for a provision of public e-Services. To analyse e-Signature implementation case there is a need to look at the eIAS issues as a complex and detailed regulatory system that is based on strategic decisions to create a functional platform. E-Signature directive (Annex I) commands QeS for public sector, but that does not mean that it is the only legally valid e-Signature. For example, Sweden and Denmark still do not use qualified e-Signature for the provision of public e-Services (Ekenberg, 2012; Jacoby, 2012).

A study by Dumortier et al. (2003) shows that most EU countries faithfully transposed e-Signature directive into the national legal systems. Directive influenced legal and technical activities concerned with the implementation of e-Signature solutions. Countries had to establish schemes for supervision, validation, certification of e-Signatures. Such schemes were based on individual interpretation of e-Signature directive by the implementing authority. Directive was adopted in 1999, but European standards followed only in 2003. That led into large investment and complex implementation experience. Such facts led to the creation of "isolated islands" in the European Union and on the national levels. Study by Dumortier (et al. 2003) assessed transposition aspects of the e-Signature directive. It analysed whether supervision, notification, accreditation, secure signature-creation device assessment schemes are in place. Lithuania was amongst those EU countries that faithfully transposed e-Signature directive and made decisions to use some European and national standards for e-Signatures implementation, but that was not enough for creation of viable e-Signature platform for provision of public e-Services.

E-Signature directive has no clear focus on international dimension and limited practical guidance. In the area of trust e-Signature directive framework lacks detailed rules on supervision of certified signature providers (CSP), offers only voluntary accreditation and trusted status lists (Lacroix, 2012). As regulatory, standardization and trust factors are approached differently in EU countries it creates even wider gap in creation of cross-border interoperable solutions.

More legal certainty on the EU level might be ensured after adoption of a currently introduced proposal for a regulation—a legal act directly applicable in the Member States (Cairns, 1999)—which will enter into force after scrutiny by the EU institutions. Also, strengthening of the EU rules might have a positive impact on interoperability of cross-border e-Services. Nonetheless, regulation will be followed by the delegated acts (indicative date 2014-2015) that will ensure the evolution of the framework (Lacroix, 2012).

Transposition of the e-Signature directive did not stop after adoption of the Law on e-Signature in Lithuania. Thus, legal base and technical solutions offer only limited range of public e-Services that can be provided using eIAS. Most important legal acts adopted since 2000 that create a legal national base for the development of eIAS:

- Requirements for certified service providers (CSPs) creating qualified certificates, procedure of registration of CSPs that issue qualified certificates and requirements for e-Signature equipment (2002);
- Appointment of the e-Signature supervisory institution (2002);
- Supervision of the trusted list of providers (2009);
- Requirements for minimal insurance sum for the e-Signature providers (2011);

Aspects that still needs regulatory attention on national and on the EU levels:

- Coordination of relations between development of eIAS and responsible party for introduction and promotion of electronic national eID cards for eIAS use;
- Transparency in security and risk guarantees;
- Requirements for eIAS verification procedures;
- Promotion, management and supervision of interoperable eIAS platform to be used by all public institutions. ·

The subject of eIAS is analysed in time when proposal of the European Commission for a Regulation on electronic identification and trust services for electronic transactions in the internal market[6] is placed for Member State scrutiny.

3.1.2. Policy and supervision

Research undertaken shows that transposition of the e-Signature directive and real life practice differ. For example, Estonian, Scandinavian public sector did not adopt e-Signature directive to the full extent, but rather focused on practical aspects of it use.

First of all, policy creation starts in the European Union rule making. Second, eIAS implementation depends on national policy decisions that influence development of the information society sector and its strategic priorities (Garuckas and Kaziliūnas, 2008). Third, political decisions are vital not only for legal system, but also for the financing of the solutions to be implemented and used in the public sector. Fourth, political decisions ensure institutional set-up for supervision of the eIAS. Clear responsibilities are vital in any complex subject matter, which is even more important is interaction between institutions. Fifth, standards are an important issue. Use of eIAS is based on standards that are usually created by the international standardization bodies that are voluntary or national specification that not necessarily correspond to international standards. Sixth, management and supervision of the process should be a catalyst for the spread of eIAS.

Policy decisions should be aimed at creating a functional e-Signature implementation platform on the national level for provision and use of e-Services. Therefore, combination of standards, policy decisions and regulatory issues create a basis for playing field for business companies that develop and offer viable e-Solutions for the governments to achieve their policy goals (Figure 2). Recent changes of national strategic provisions[7] excluded e-Government understanding and also it excluded clear provisions on the use of

6 Proposal of the European Commission of 7 June 2012 for a Regulation on electronic identification and trust services for electronic transactions in the internal market (No. 10977/12), Brussels.

7 Public administration development strategy until 2010 in 2012 was changed by the Public management improvement program for 2012–2020.

e-Signature solutions. Exclusion of such provision leaves integration of eIAS solutions as voluntary for public sector institutions. Latest national strategic provisions do not improve management, supervision, but rather loosens the possibility for systematic development of e-Government platform.

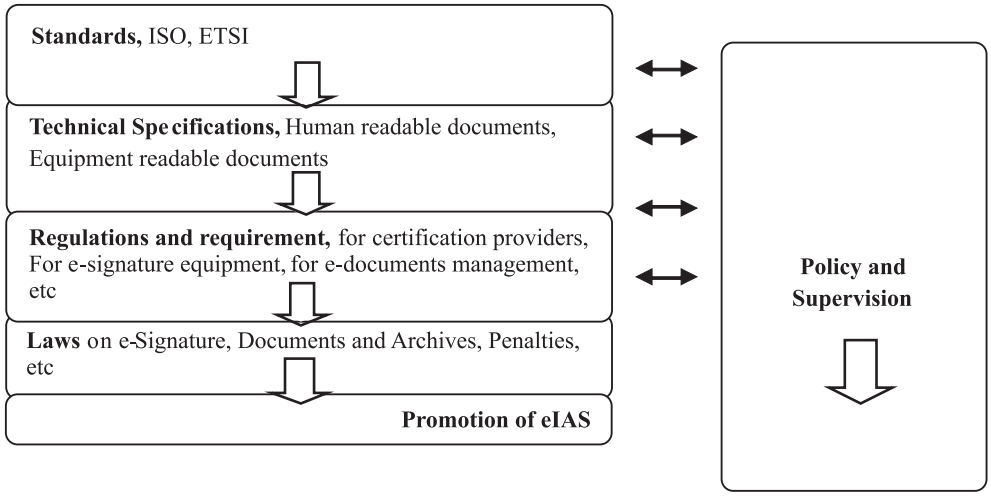

Fig. 2. Interlaced relations between standards, legal provisions, policy and supervision

3.2. Organizational set-up features

Organizational set-up in Lithuania is touched on for two reasons: 1) to show the complexity of organizational set-up and 2) to look how it ensures the goals for development and promotion of eIAS.

Responsibilities for e-Signature development are spread among wide number of institutions. Such system lacks coordinated approach towards development and promotion of the eIAS and other e-Government solutions. In 2012, Ministry of Transport and Communications was named[8] as a main policy institution for e-Signature development. The scope of policy making in the area of e-Signature is without a possibility to ensure vertical coordination and integration of the policy on national level. In 2011, Communications regulatory authority was appointed[9] as supervisory authority for the e-Signature. It supervises certified service providers that offer e-Signatures based on qualified certificates, but not the overall process of e-Signature promotion on national level. Ministry of Interior Affairs is responsible for eID cards that are provided to the citizens since 2009, but since 2011 legal acts do not oblige citizen to get national eID card

8 Lietuvos Respublikos Vyriausybės 2012 m. liepos 4 d. Nr. 830 nutarimas „Dėl Lietuvos Respublikos Vyriausybės 2010 m. spalio 13 d. nutarimo nr. 1480 "Dėl Lietuvos Respublikos susisiekimo ministerijos nuostatų patvirtinimo 'pakeitimo'."

9 Lietuvos Respublikos Vyriausybės 2011 m. sausio 17 d. nutarimas Nr. 32 "Dėl elektroninio parašo priežiūros institucijos."

that is the main source, which offers eIAS solution in Lithuania. Only 644.465 national eID cards were issued since 2009 (Communications Regulatory Authority report, 2012). In 2011, Office of the Chief Archivist of Lithuania has introduced specification for e-Documents, e-Document management rules and rules for submission and storage of e-Documents. E-Document dimension is added in Figure 3 because documents play an important part in the e-Government sector.

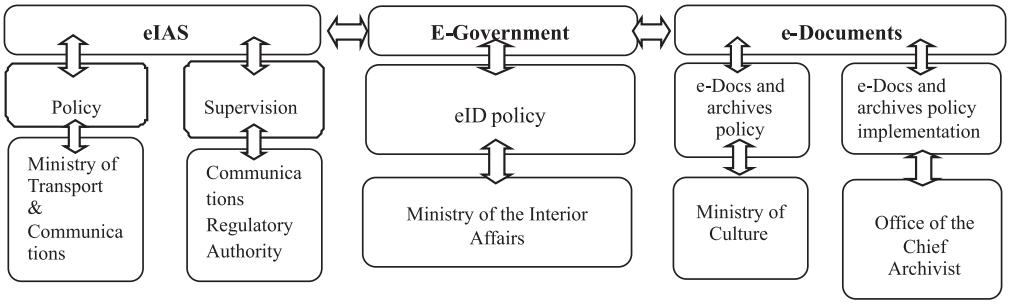

Fig. 3. Responsibilities of institutions in Lithuania.

eIAS, e-Government and e-Document solutions cannot offer effective interoperability without closer interaction between institutions showed in the Figure 3. Organizational set-up reveals that take up of eIAS solutions can be better coordinated, legal provisions should ensure smooth structure for its effective functioning. Only in such case it could be expected less interoperability problems and possibility to move towards practical and usable national eIAS platform that allows integration of cross-border services in the EU.

National supervision scheme for e-Government projects was not created in Lithuania. Chief Information Officer or responsible institution was not appointed. ICT implementation structure is based on horizontal scheme where every institution mostly ran their own ICT/e-Signature projects. From 2000 until 2011 new functions for ICT and eIAS development were changed or added to institutions mentioned in the figure 3.

3.3. Spread of eIAS

Main idea of the public services is that citizens could access public e-Services via any technology (eID card, SIM card or USB keys). Currently, there is a notion that public sector services exist in parallel reality from eIAS. Public sector should have developed a strategy for eIAS integration. Only in that case it would be a possibility for private sector to offer missing solutions, which are not free (Krawczyk 2010). Implementation of any solutions in public sector is ensured by the finances from the national budget. eIAS has a stimulus to be a solution that is close to the user because eIAS offers tangible benefit when deployed in the real life.

There are three entities that issue certificates in Lithuania: 1) Digital Certification Center (DSC); 2) Centre of Registers (CR); 3) Residents' Register Service under Ministry of Interior Affairs (RRS under MIA) (Table 1). Mentioned providers have

started activities in 2005, 2008 and 2009 respectively. Residents' Register Service under Ministry and Interior Affairs issue (since 2009) offers two type of certificates: 1) national eID cards and ii) public servant eID cards, both enabling to use QeS. Centre of Registers (public institution) offers certificates (since 2008) that are not based on national eID card, but as a separate commercial service.

Table 1. Number of certificates issued in Lithuania.[10]

Year	DSC (Number of certificates issued)	CR (Number of certificates issued)	RRS under MIA (Number of certificates issued)
2009	4311	20158	219000
2010	11530	35156	451000
2011	15057	61590	644465

On the positive side currently there are 0,7 milion certificates and most of them are issued by the Residents' Register Centre that means that the e-Cards are integrated with qualified certificates. On the negative side national eID cards are duplicated—national eID card and civil servant card are issued. Moreover, since 2011 Law on Identity Card does not make obligation for citizens to get eID cards, citizen can get a passport instead.

Table 2. Use of valid electronic certificates and transactions.[11]

Country (Total population)	No. of valid certificates	No. of transactions
Lithuania (3.0 mln)	0.7 mln	No Data
Denmark (5.5 mln)	3.7 mln	Around 45 mln transactions (eIAS) per month
Estonia (1.3 mln)	1.1 mln	Around 3 mln e-Signatures per month
Sweden (9.5 mln)	4.5 mln	In 2011, around 1,25 mln e-Signatures per month
Latvia (2.7 mln)	0.1 mln*	Around 0,7 mln e-Signatures per month (5.8 mln signatures (from 2012-01 until 2012-08)
Norway (5 mln)	4 mln	No data

Despite the differences in Member States policy, technical solutions and use of eIAS, promotion of eIAS and its use are reflected in Table 2.

* 250 per cent increase in number of valid certificates compared to 2011(Bokta, 2012).

10 Data taken from Communications Regulatory Authority's Report on Implementation of the Law on Electronic Signature in 2011.

11 Data taken from the presentations presented on 18th September 2012 during the Nordic-Baltic seminar "Practical Aspects of e-Signature and e-Documents Use in the Framework of Digital Single Market" that took place in Vilnius.

4. Demand for eIAS and its value

Any use of ICT solutions are attributed to e-Government and considered to be related to organizational changes, new skills, advanced public service that contributes to the democracy processes and enhanced relations between government and constituency. eIAS ensures the possibility to use less paper, e-Invoices, allows to use time more effectively, save on postal charges, etc. As public sector gets more experience in eIAS use it can better formulate future needs.

4.1. Social and practical aspects of eIAS usage

There are some success stories in public sector for the use of eIAS (Table 3). State Social Insurance Fund Board received about 0.5 million signed documents per month. 82 per cent of proposals for procurement of public sector are submitted electronically. Also, 90 per cent of annual tax declarations are submitted electronically. Public sector understands necessity for e-Signature. Therefore, experience of eIAS use for access and use of e-Government services is rather promising.

Table 3. Use eIAS while accessing most popular e-government service in Lithuania.[12]

Institution	e-Service	Usage/Period
State Social Insurance Fund Board (SODRA)	Submission of documents	Around 0.5 million. e-signed documents per month
Centre of Registers	Registration of enterprise/ reservation of names	Every second registered enterprise was registered electronically (total number of registered 1384 units); 1736 names were reserved using electronic means, during 2012-01-01/04-30
Public Procurement Office	Documents for public procurement	7189 (82 per cent) public procurements by the public sectors carried electronically, during 2012 I and II quarters
State Tax Inspectorate	Tax declarations	Out of 820.000 tax declarations (for the year 2011) 90 per cent submitted electronically

There is a need to mention factors that influence popularity of e-solutions:

- Price of equipment. At the moment, readers cost are minimal, free software can be downloaded.
- Competition between certificate providers reduces the price of certificates and increase user interest in eIAS solutions.

12 Data taken from presentation by Strumskis (2012) "SODRA's Experience of Application of e-Signature Solutions and Sustaining it in the Future"; Center of Register (2012, e-news "Companies that are willing to register on-line will save"—Public Procurement Office, Reports 2012 I and II Q; E-news (2012) "Preliminary results on tax declaration by the citizens."

Another important issue is how e-Services (like tax declaration, social services, e-Government gates) that are offered in Lithuania can be accessed by the citizens. At the moment, some public e-Services are accessed and used through private e-Signature system, which is not public sector product. Existing e-Banking system in Lithuania does not ensure two way transactions in order to have highest level of interaction according to e-Government models. The question is whether this practice will still be viable for the provision of eIAS intended for public e-Services in the near future.

There is a need to mention an issue with security level and liability for risks. It is an important to set certain insurance level on the EU or national level in order to tie technology to risk management where monetary loss is involved.

Aspects mentioned in this section should also be addressed and balanced between member states if EU really wants to have cross-border services.

4.2 Risk of failure and value for investment

The worst outcome for the investment is failure. Failures can be total, partial or project is implemented successfully. Analysis by Heeks (2005) shows that 35 per cent are total failures, 50 per cent is partial failures (show subjectivity of failure) and 15 per cent of ICT projects are implemented successfully. Heeks (2005) makes a division between "objective technology" and "enacted technology." E-Government systems should be viewed in systematic manner as group of related dimensions (invention, design, deployment context, culture, soft transformational aspects). Furthermore, failure of a single project does not necessarily terminate life of the system. There might be other attempts to introduce a solution. For that matter, failures need to be tolerated and learned from.

Juell-Skielse (2011) argues that use of technology or solution is based on needs of a subject that is going to deploy it. Deployment should be based on added value of the solution. Use, promotion and popularity of any technology depends on value, which is something that is interpreted by the user as beneficial and is caused by transfer or conversion of a resource. The value of changes in organizational effectiveness is often related to income increases or cost reductions enabled by changes in business processes.

In public sector eIAS solution can be effectively used in the front and back offices. eIAS helps to access certain application upon identification and authentication, also to sign. Value of eIAS in public e-Services provision is in its integration in e-Government model (Juell-Skielse, 2011).

5. Findings

The general findings of the research. eIAS must be functional and simple to use in order to reach critical mass and become a part of everyday life. People must understand what digitally signed file is. Cross-border dimension shows that citizens must be able to travel abroad and use it for any sector services (e.g. Courts of other EU member states, etc.). Figure 4 illustrates that any national system is influenced by international dimension, integration of all public sector institutions and constituency. That fact

ensures stimulation of demand for a single acceptable trusted and secure e-Signature solution for all sectors for any service, anywhere and at any time.

In creation of e-Signature solutions private sector relies on the idea that technological solutions' price must be proportional to its functionality and risks. Public sector solutions cannot be based on that notion because an accident can create risks and loses (data, information, financial) that are not foreseen by the basic insurance. That's why public sector needs higher level of safeguard for the secure risk-proof solutions. In Lithuania, insurance[13] sum for the e-Signature providers that issues qualified certificates is not less than 100 000 LTL (1 EUR = 3 4528 LTL).

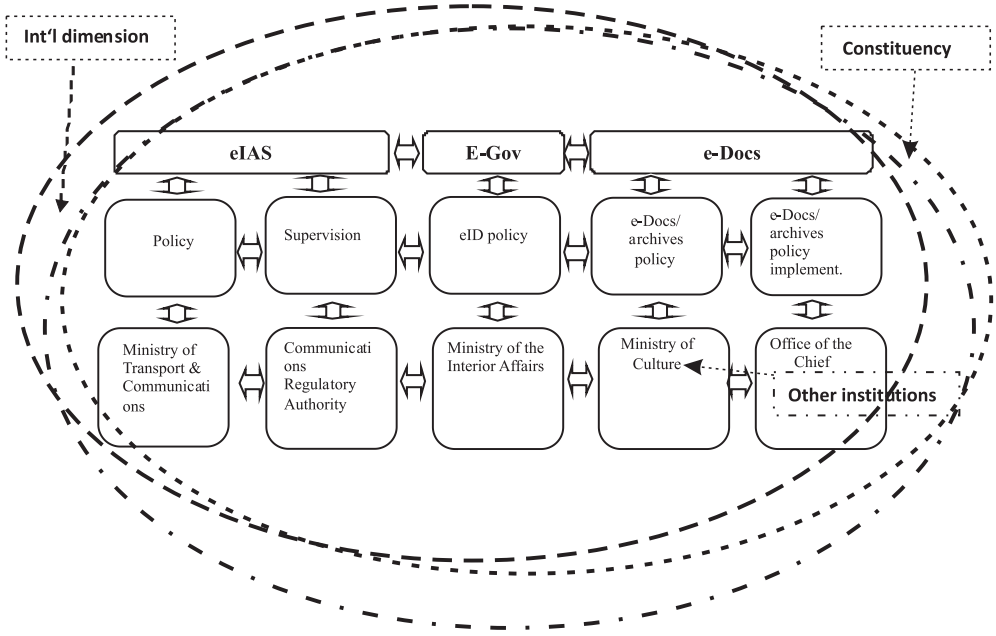

Fig. 4. Implementation of eIAS solutions on the national level with international dimension.

6. Conclusions

This research offers insight into the eIAS topic and fills the information void of implementation of eIAS solutions in Lithuania. Article assesses legal, strategic, organizational and practical aspects of the eIAS that offers a possibility to use eIAS solutions by the constituency in Lithuania. Also, article models a possible solution for effective eIAS implementation by the public sector of Lithuania. Article concludes that:

a) Public sector focused only on the development of the qualified e-Signature, which is its most advanced form, requires focused strategy and management ability.

13 Lietuvos Respublikos ryšių reguliavimo tarnybos direktoriaus 2011 m. balandžio 19 d. Įsakymas Nr. 1V-408 "Dėl minimalios draudiminės sumos kvalifikuotus sertifikatus sudarantiems sertifikavimo paslaugų teikėjams nustatymo."

Such strategy and implementation scheme was a barrier for the development of public e-Services;

b) Until the end of the first decade of the XXI century public sector in Lithuania was focused on qualified e-Signature, but analysis shows that relatively small private or public (number of public servants in Lithuania around 29 000) systems can rely on simpler e-Signature solutions than e-Signature based on qualified certificates. Practice and examples of other countries shows that such advanced solution did not prove viable for e-Government sector;

c) Policy and strategy adopted by the government precluded private sector from creating viable solutions that could have been use for public sector as well;

d) In Lithuania, the value chain for the provision of public e-Services was created rather slowly. In 2007, in order to meet political agenda public sector started using private eIAS solutions (e-Banking system) for public e-Service provision to constituency. Also, eID cards were developed and distributed in 2009 when provision of public e-Services was already based on private eIAS solutions;

e) Practice shows that closed systems could rely on simpler closed system e-Signature solutions without qualified certificates even for public sector. As it was shown in the figure 4 e-Signature based on qualified certificate becomes a viable solution that fits emerging (not fictional) conditions for open systems and provision of cross-border services. Implementation of new eIAS solutions requires input on organizational side.

Conclusions lead to the possibility and need to further analyse eAIS topic in the light of optimal scheme for eIAS implementation and its management in Lithuania. That is why it is necessary to further analyse how it is possible effectively change current eIAS system and adopt it to the emerging and future needs.

Literature

Cairns, W. (1999). *Introduction to EU Law*. Eugrimas.

Dumortier, J.; Kelm, S.; Nilsson, H.; Skouma, G.; Eecke, P. (2003). Study for European Commission, "The legal and market aspects of electronic signatures."

Garuckas, R.; Kaziliūnas, A. (2008). "Regulation of electronic signature and particularities of its implemenation in Lithuania" (Elektroninio parašo teisinis reglamentavimas ir jo įgyvendinimo ypatumai Lietuvoje). *Viešoji politika ir administravimas*, Vol. 24, p. 114–123.

Heeks, R. (2005). "E-Government as a Carrier of Context." *Int'l Public Policy*, Vol. 25(1), p. 51–74.

Juell-Skielse, G. (2011). "Improving Organizational Effectiveness through Standard Application Packages and IT Services." <http://www.dissertations.se/dissertation/79ec0a69a2/>.

Krawczyk, P. (2012). "When the EU qualified electronic signature becomes an information services preventer." *Digital Evidence and Electronic Signature Law Review*, 2010, Vol. 7, p. 7–18.

Raymond, A. H. (2011). "Improving Confidence in Cross Border Electronic Commerce: Communication, Signature, and Authentication Devices." *Journal of Internet Law*, 2011 January, p. 24–34.

AE sprendimai (2012). "Preliminary results on tax declaration by the citizens" (Preliminarūs gyventojų pajamų ir turto deklaravimo rezultatai). 2012-05-07, <http://aesprendimai.eu/preliminarus-gyventoju-pajamu-ir-turto-deklaravimo-rezultatai/>.

Bokta, J. (2012). presentation: "Cardless e-Signature Solution in Latvia—Virtual eParaksts." <http://www.rrt.lt/lt/pranesimai_296/2012.html>.

Centre of Registers, 2012-04-30. "Enterprises registering data online will save" (Internetu duomenis registruojančios įmonės pastebimai sutaupys). <http://www.registrucentras.lt/naujienos/index.php?mod= news&act=view&id=8615>.

Communications Regulatory Authority (2012). Report on implementation of the Law on e-signature during 2011. <http://www.rrt.lt/lt/apzvalgos-ir-ataskaitos/elektroninio-paraso-istatymo-1b73.html>.

Dumortier, J. (2003). presentation: "Legal Status of Electronic Signatures: The transposition of the EU Directive in the Member States."

Ekenberg E. (2012), presentation: "Challenges in Changing the Existing Infrastructure in Sweden to New Conditions." <http://www.rrt.lt/lt/pranesimai_296/2012.html>.

Kumetaitienė, A.; Jakimavičius, T. (2012), presentation: "Legal Framework for e-Signature in Lithuania and Envisaged Changes." <http://www.rrt.lt/lt/pranesimai_296/2012.html>.

Lacroix, S. (2012), presentation: "Overview on e-Signature Standards Evolution as Supporting the New European Legal Framework." <http://www.rrt.lt/lt/pranesimai_296/2012.html>.

Martens, T. (2012). presentation "10 Years and 100 Million Digital Signatures Later—from National Standards to International Standards and Cooperation." <http://www.rrt.lt/lt/pranesimai_296/2012.html>.

Public Procurement Office, Information on Public Procurement during 2012 I Q and II Q, <http://www.vpt.lt/rtmp8/dtd/index.php?pid=121189211065&lan=LT>.

Rongmo, K. (2012). presentation: "Electronic Signature in Norway - Supervision and Legal Aspects." <http://www.rrt.lt/lt/pranesimai_296/2012.html>.

Strumskis, M. (2012). presentation: "SODRA's Experience of Application of e-Signature Solutions and Sustaining it in the Future." <http://www.rrt.lt/lt/pranesimai_296/2012.html>.

ELEKTRONINIŲ ATPAŽINTIES PRIEMONIŲ PLĖTRA VIEŠAJAME LIETUVOS SEKTORIUJE: REALYBĖ, PAKLAUSA IR ATEITIS

Rimantas Petrauskas

Mykolo Romerio universitetas, Lietuva, rpetrausk@mruni.eu

Paulius Vaina

Mykolo Romerio universitetas, Lietuva, pavaina@stud.mruni.eu

Santrauka*. Straipsnyje nagrinėjamas elektroninės atpažinties, elektroninio tapatumo nustatymo, elektroninio parašo ir su tuo susijusios patikimumo užtikrinimo paslaugos (EANPP) diegimas, kurį vykdo viešasis Lietuvos sektorius. Šių sprendimų diegimas turi būti siejamas su pridėtine verte, kuri suteikiama viešųjų e. paslaugų teikimo platformai, nes dauguma elektroninės valdžios plėtros modelių yra susiję su paslaugos perdavimo galimybe nau-*

dojant IRT technologijas. Svarbu yra įvardinti silpniausias grandis, kurios sudaro kliūtis tolesnei elektroninės atpažinties bei elektroninio tapatumo nustatymo plėtrai Lietuvos viešajame sektoriuje.

Apžvelgiamas elektroninio parašo naudojimas uždarose ir atvirose sistemose, taip pat akcentuojami simetrinio ir asimetrinio kodavimo sprendimai, kurie lemia elektroninio parašo technologinį, funkcionalumo, saugos, rizikos ir kaštų lygį. Vertinama elektroninio parašo plėtra, susijusi su teisiniais, strateginiais, organizaciniais ir praktiniais diegimo aspektais, už kuriuos yra atsakingas viešasis sektorius. Lietuvoje elektroninio parašo diegimą neigiamai veikia horizontalus informacinės visuomenės politikos diegimo pobūdis, kai nebuvo numatyta institucija, prižiūrinti šios srities projektų vertikalų diegimą.

Straipsnyje aptariami sėkmingai panaudoti elektroninio parašo sprendimai, kuriuos įgyvendinus teikiamos aukščiausio brandos lygio viešosios elektroninės paslaugos (*SODRA, Registrų centras, Viešųjų pirkimų tarnyba, Valstybinė mokesčių inspekcija ir kt.*). *IRT panaudojimo elektroninei atpažinčiai vertė suvokiama kaip sprendimo pridėtinė vertė, kurią interpretuoja technologijos naudotojas, atsižvelgdamas į technologijos suteikiamą naudą – efektyvesnę organizacijos veiklą.*

Atsižvelgiant į Europos Sąjungos tarpvalstybinių paslaugų perspektyvą, taip pat pristatomas elektroninio parašo ir su tuo susijusios patikimumo užtikrinimo paslaugos įgyvendinimo modelis, kuris galėtų užtikrinti efektyvesnį šių sprendimų diegimą Lietuvoje.

Išvados: a) *Lietuvos viešasis sektorius koncentravosi ties sudėtingiausio lygio elektroninio parašo su kvalifikuotu sertifikatu diegimu, o tai reikalauja papildomų strateginių ir vadybinių sprendimų; b*) *Analizė parodė, kad sudėtingiausio lygio elektroninio parašo sprendimų diegimas Lietuvoje kol kas ne iki galo pasiteisino; c*) *Atsižvelgiant į tarpvalstybinių viešųjų elektroninių paslaugų kontekstą tikėtina, kad tik elektroninis parašas su kvalifikuotu sertifikatu užtikrins atvirų sistemų ateities poreikius, tačiau tokių technologinių sprendimų diegimas reikalaus ir organizacinių pokyčių.*

Raktiniai žodžiai: *e. atpažintis, elektroninio tapatumo nustatymas, elektroninis parašas, elektroninės atpažinties nustatymas, elektroninio parašo ir su tuo susijusios patikimumo užtikrinimo paslaugos, elektroninės paslaugos, elektroninė valdžia.*