Estonia
Latvia
Russia
ENPI cross border
cooperation programme
part-financed by
the European Union
united by borders

HANDBOOK

Implementation of E-Government in Cross-Border Regions

2015

This document has been produced with the financial assistance of the Estonia – Latvia – Russia Cross Border Cooperation Programme within European Neighbourhood and Partnership Instrument 2007 – 2013. The contents of this document are the sole responsibility of the e-Governance Academy and can under no circumstances be regarded as reflecting the position of the Programme, Programme participating countries, alongside with the European Union.

TABLE OF CONTENTS

1. INTRODUCTION 3

1.1 Aim and outline of Handbook 4

1.2 e-Government Concept 4

1.3 Key objectives and benefits of local e-government 5

2. E-SERVICES FOR CITIZENS AND BUSINESSES 8

2.1 Stages of online service development 9

2.2 Interoperability 10

2.3 Citizen inclusion and e-participation 10

2.4 Privacy and security matters 11

3. DELIVERING E-GOVERNMENT IN CROSS BORDER REGIONS 12

3.1 Boosting online cross border services 12

3.2 Key barriers of cross border services 13

3.3 Systems for authentication and authorization of citizens 13

3.3.1 Overview of the Estonian ID-card technology 14

3.3.2 Overview of the Russian Crypto Pro technology 15

3.3.3 Overview of the Latvian ID-card technology 17

3.3.4 Overview of the technology „Welcome without password – WWP" 17

3.4 Implementation of digital archiving in cross border areas – Practical example from the EstLatRus project 18

3.4.1 Introduction of electronic records and digital archiving 18

3.4.2 Background of the management of cross border records 19

3.4.3 Process analysis 20

3.4.4 Lessons learned and conclusions 22

1

INTRODUCTION

Information and communication technologies (ICTs), related telecommunication and other digital networks are considered to be a **major driving force** in building economies. These are increasingly recognized as a factor in improving existing governance practices, where up to 80% of citizen-to-government (C2G) transactions take place at the local level.

Local e-government means exploiting the power of ICTs for providing **quality public service** and to help renew the relationship between citizens and the public bodies who work on their benefit. At the local level e-governance and the appropriate use of ICT can enhance and support economic and social development, particularly in empowering officials and local authority representatives to ensure linkages, networking, and efficient, transparent, timely services.

Great benefits can be achieved by using ICT to enable digital public services (e-services) **across borders**. However, many public online services do not work across borders or involve cumbersome procedures to be accessible, reducing the mobility of businesses and citizens. Therefore **it is very** important to analyze the possibilities to develop and implement the quality services that decrease cross-border disparities and provide more balanced development.

The purpose of this Handbook **"Implementation of E-Government in Cross-Border Regions"** is to help local decision-makers to make informed policy choices and understand the practical challenges and opportunities that introducing e-government solutions imply in cross-border region. The Handbook provides good practices and recommendations in order guide local authorities to implement cross-border e-government solutions.

The Handbook was developed under the project ***"Increasing capacity of local authorities in providing e-services in Ida-Virumaa-Leningrad oblast cross-border areas"***. Overall objective of the project is to increase the administrative capacity and e-readiness of local and regional authorities in providing socially significant public e-services through cooperation and implementation of e-government solutions in cross-border region.

The project is supported by the ENPI Cross Border Cooperation Programme that is partly financed by European Union.

1.1 AIM AND OUTLINE OF HANDBOOK

There are no ready-made good or bad local e-governance models or strategies. A good model will be the one, which enjoys consensus among all stakeholders and has evolved from a transparent and consultative process. Nonetheless, there are some important benchmarking milestones that underpin the evolution of various e-government initiatives into e-governance as a comprehensive public service and government-to-citizen (G2C) communication system.

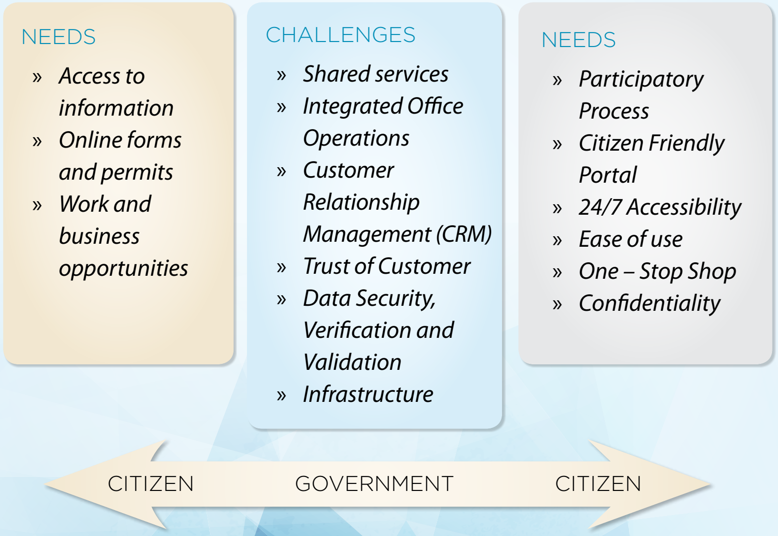
The Handbook gives a short overview of the three Est-Lat-Rus Programme Area countries´ experiences in digital world, identifies key challenges and impacts, and sets down possible strategies and guidelines for implementing cross-border e-government solutions, including digital archiving process.

1.2 E-GOVERNMENT CONCEPT

e-Government is about transforming the way government interacts. e-Government, in addition to service delivery, has also been used to enhance the coverage, increase transparency, improve response to citizens and lower administrative costs. It also facilitates citizens to have better access to services, equity and social empowerment.

The e-Government process requires a coherent strategy, beginning with an examination of the nation’s political will, resources, regulatory environment, and ability of the population to make use of planned technologies.

FIGURE 1: e-Government Model



NEEDS

- Access to information
- Online forms and permits
- Work and business opportunities

CHALLENGES

- Shared services
- Integrated Office Operations
- Customer Relationship Management (CRM)
- Trust of Customer
- Data Security, Verification and Validation
- Infrastructure

NEEDS

- Participatory Process
- Citizen Friendly Portal
- 24/7 Accessibility
- Ease of use
- One – Stop Shop
- Confidentiality

Source: United Nations e-Government Survey 2008 - From e-Government to Connected Governance

1.3 KEY OBJECTIVES AND BENEFITS OF LOCAL E-GOVERNMENT

Information Society development is in large extent issue of local governments (LG-s). As LG-s, compared to the central government, are more close to the citizens, e-government implementation on the local level and in cross-border regions can achieve the following objectives:

- **More 'joined up'** - common services in different organizations in the region, provided through linked information systems, improved access points and delivery methods. This includes **delivering services jointly** with central and local government agencies and departments.
- **More accessible** - from home, libraries, offices – from anywhere for the better convenience of the public rather than from LG offices in long queues. Equal ac-

cess for all and social inclusiveness are the key words. Services will be available for the citizens at any time – not constrained by normal office hours or specific technology to access the service (access channels).

- **Delivered or supported electronically** – creating more responsive, better valued and faster services, also offering 24/7 access to information. For example - simplifying access to services through web sites, such as changing school, setting up a business, or changing home address. Seamless delivery and the removal of unnecessary bureaucracy are the key aims.
- **Open and accountable** - providing more information about future activities, priorities and performance, encouraging public consultation and supporting local authority employees in keeping in touch with the people they represent.
- **Used by 'e-citizens'** – we need to support and encourage members of the public to adopt e-services where appropriate, especially if it reduces transaction costs and allows us to focus scarce resources on those in our communities who need it the most. Though it is hard to know what the public will expect from electronic public services in the future, and we recognize that not everyone will want or be able to access services electronically, careful design and continuing consultation will help avoid costly investment mistakes.

There are several benefits that implementation of the e-government provide:

- **The use of ICT helps to improve efficiency in the government**. ICTs are necessary enabler of reforms to the ways in which public administrations work. Improving internal operating systems like financial systems, internal communications and information sharing improve the efficiency of service provision in general.
- **Enhanced quality of service** has been a major component of public administration reform over the past two decades, and the use of ICTs to generate improvements in services has been a primary driver for e-government activity. Online services are increasingly seen as part of a broader services strategy, with important key-words like "customer focused" and "effective" (fast, simple and cost-effective).
- ICTs can support **more effective outcomes** in key policy areas such as health, welfare services, security and education. Ultimately, governments and public administrations exist to deliver policy outcomes, and ICT is just an enabler across all major policy areas.

- e-Government can help **forward the reform agenda**. When aligned with modernization goals, implementing e-government can help administrations focus on the additional changes needed to meet service delivery and good governance concerns. At the same time, it provides some valuable reform tools and builds support from high-level leaders and government employees for achieving those objectives.
- Through citizen engagement e-government can **improve the overall trust relationship** between the government and the public. e-Government, by improving information flows together with encouraging active participation by citizens is increasingly seen as a valuable tool and is also called as **e-governance** (e-government + e-participation/e-democracy).

2

E-SERVICES FOR CITIZENS AND BUSINESSES

LA-s have can increase citizens´ satisfaction on reaching for public services (e-services), as people appreciate the convenience of being able to book services, report faults or pay bills in the evenings and on weekends, through the internet (online).

Coordination and cooperation between the border area LA-s are needed to satisfy the following requirements of e-Government services:

- People are aware of available cross-border e-services and know how to use them
- e-Services are found easily from LA-s web-site, or from one access point in a separate web-site (one-stop-shop for e-services, etc) and are user-friendly
- e-Services must be accessible to all members of the intended target groups, including people with special needs and elderly persons
- e-Services should add value (save time, money and provide better communication with LA officials)
- Where applicable, a service should be integrated with other services.

Five objectives of the i2010 e-Government Action Plan - Accelerating e-Government in Europe for the Benefit of All should also be considered in developing cross-border e-services:

1. Access for all
2. Increased efficiency
3. High-impact e-Government services
4. Putting key enablers in place
5. Increased participation in decision-making

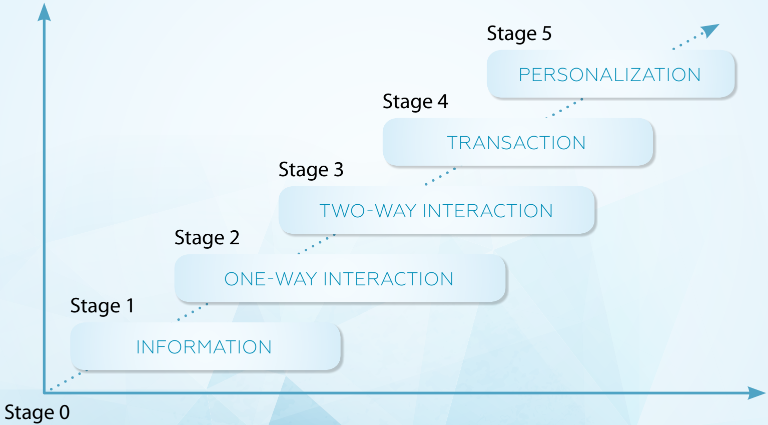
Following paragraphs are describing the **basic principles of e-services** and bring out the important enablers needed for the successful implementation.

2.1 STAGES OF ONLINE SERVICE DEVELOPMENT

In order to measure the “availability of public services online” five-stage framework has been defined and widely accepted by the European Union countries. This framework provides basic guidelines of how to proceed with the development of various services to the citizens and businesses. This kind of frameworks can be used also while developing and measuring **cross-border e-services**.

- **Stage 1 - Information:** Information how to use public service is available on-line.
- **Stage 2 - One-way Interaction:** The public website offers the possibility to download paper form for filling in and get specific service. Ordering a paper-form via electronic channel is also considered as stage 2.
- **Stage 3 - Two-way Interaction:** The public website provides electronic forms to fill in and to get certain public service. This implies that there must be additional step for authentication of the person (physical or juridical) requesting the services in order to reach stage 3.
- **Stage 4 - Transaction (full electronic case handling):** The public website offers the possibility to get the public service fully via the website, including decision and delivery. No other formal procedure is necessary for the applicant via “paperwork”.

FIGURE 5: The different stages of e-services



Source: Preparing the 9th eGovernment Benchmark Measurement- method paper, European Commission (2010).

- **Stage 5 – Personalization (pro-active and automated service delivery):** On this level fully integrated electronic procedures that help to improve data consistency is provided. No other physical action is required on behalf of the applicant. Online provision of the e-services is based on new models of front and back-offices integration, the reuse of available data, the idea of pro-active service delivery is embedded. For certain services this means that the applicant receives the service automatically based on a previous registration of an event.

2.2 INTEROPERABILITY

Interoperability of information systems (IS) has become an important topic for all countries in the world, as in the public sector it is defined as the ability of government organizations to share and integrate information by using common standards – shortly it is **"talk to one another"** without any technical problems that hinder the smooth operation of government. To provide interoperability, it requires political, legal, organizational, and technical activities.

Interoperability enables an **online tracking system** that permits citizens to check on the status of online transactions. As with an identity management feature, such a system implies that the citizen-facing system – the national website or portal – is able to communicate with the system that government officials are using to process the transaction.

The European Commission's *"Study on Analysis of the Needs for Cross-Border Services and Assessment of the Organisational, Legal, Technical and Semantic Barriers"* brings out that for the **successful** implementation of the **cross-border services**, the interoperability is a **key factor**.

2.3 CITIZEN INCLUSION AND E-PARTICIPATION

e-Participation is an area that is particularly relevant at the local level where individuals are most likely to come into contact with public agencies. It is important to consider to what degree are governments providing supporting information, actively consulting with citizens through online channels, and involving them in decision-making processes. Each of these aspects of citizen-centric governance must be defined in concrete, measurable terms, and corresponding data collected, in order to monitor the relationship between online services and citizen empowerment.

Many governments have enhanced their national and ministerial websites to incorporate interactive tools to strengthen citizen e-participation. Citizens create a different relationship with their respective governments, characterized by enhanced effectiveness, as government are able to respond to the needs of citizens in a more direct manner.

Web 2.0 tools like Facebook, Twitter, blogs, wikis, have empowered citizens to become **more active**. They can make comments and suggestions to public institutions through these sites, despite of where they are located and whether it is their own LA, or LA across the border. The 24-7 reach of these tools provides a **cost effective mechanism** for citizen alerts as well as for views on how the well government is working.

2.4 PRIVACY AND SECURITY MATTERS

Citizens are unlikely to use e-government services without a guarantee of privacy and security. Governments also have a strong interest in maintaining citizens' trust (e.g. that information provided will not be misused). The difficulty of protecting individual privacy can be an important barrier to e-government implementation. Ensuring that e-government initiatives are in step with society's expectations in this area is a crucial means of building trust.

The challenge facing e-government coordinators and implementers is to respect accepted privacy principles while allowing the benefits of the Internet and other technologies to flow to citizens. This balance is of particular importance when considering seamless government services involving data sharing among agencies.

Government has a responsibility to provide leadership in developing a culture of privacy protection and security. ICT should provide this leadership through its roles in the development of public policy, as owner and operator of systems and networks, and as a user of such systems and networks. As a user of information systems and networks, government shares a role with businesses, other organisations and individuals for ensuring secure use of the system and network.

3

DELIVERING E-GOVERNMENT IN CROSS BORDER REGIONS

3.1 BOOSTING ONLINE CROSS BORDER SERVICES

According to the European Commission Analysis of the needs for cross-border services and assessment of the organisational, legal, technical and semantic barriers, in the context of the final conclusions on how to **boost online cross-border** services the following categories shall be used:

- **Economic:** demonstrating the cost savings for all the stakeholders (Citizens, Business, Administrations and Industry) in developing cross border services.
- **Governance:** Existing structure in terms of roles and responsibilities in coordination, overall sustainability and scalability aspects in use of cross-border services.
- **Organisational:** Cross-border model in setting requirements like handling of different languages, etc.
- **Legal:** Cross-cutting directives and regulations, etc, setting the frame for the legality of the policy, governance, technology, organisational aspects as well as the legality of the service provision.
- **Social and Communication:** raising awareness within the administration and towards users.
- **Technology:** technical architecture and functional requirements necessary for cross border services.

3.2 KEY BARRIERS OF CROSS BORDER SERVICES

In order to further deploy and enhance cross-border services, the analysis of the European Commission's *"Study on Analysis of the Needs for Cross-Border Services and Assessment of the Organisational, Legal, Technical and Semantic Barriers"* shows that there are a number of recurring barriers representing **similar challenges** in e-service provision:

1. Three major barriers are shared by all services, or indeed by any service requiring bilateral interaction: **eID**, **eSignatures** and **linguistic issues**.
2. Key challenge for many services is **the readiness of local infrastructures**, **stakeholders** and **legislation**.
3. All of the services above require **stable governance mechanisms** to ensure sustainability.

3.3 SYSTEMS FOR AUTHENTICATION AND AUTHORIZATION OF CITIZENS

Question about what mechanism for authentication is used for cross-border communication is widely connected to the relevant laws and regulations of the respected country. E-services, offered between cross-border LA-s should be analyzed, taking into account the required level for data security of the respective country and principles of personal data protection.

Most of EU countries already have some form of citizens' electronic authentication systems. In some cases the system is also integrated with an electronic ID card database and/or tied to the citizen's mobile phone.

When talking about the cross-border LA-s between EU and non EU country, the level of requirements differs, based on the information shared. Also software used for digital signing is different.

The digital trust aspect between cross-border institutions is extremely important for every electronic service. For this reason it is inevitable to include (electronic) information security requirements in every e-governance project. The benefit that an e-service or e-solution gives should be balanced with relevant security measures. The importance of security and privacy is growing along the number of e-services is being implemented. This is also very important while implementing the cross-border e-solutions that have equally accepted on both sides of the border.

Many online and corporate network services require strong user authentication. A traditional method of authentication is a combination "Login + Password". In order to increase the information systems security level, other authentication technologies have been developed – tokens and smart-cards, digital certificates and keys, biometric systems, etc.

The following three solutions describe the digital identity management, used in different EU and non-EU countries:

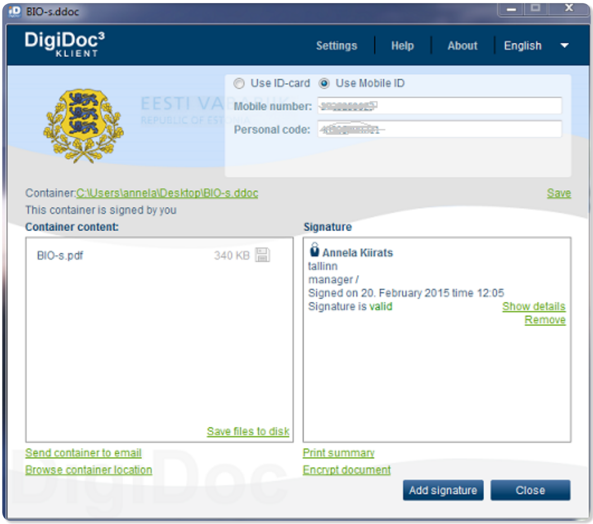
In Estonia, citizens are using their national ID-card or mobile phone to electronically sign documents when digital signature is equally binding with physical signature. In Russian Federation Crypto Pro solution is used for digital document exchange and the software is used within the country. In Latvia there are still three different possibilities to give e-signature: virtual eSignature, eSignature on smart card and eSignature on eID.

3.3.1 OVERVIEW OF THE ESTONIAN ID-CARD TECHNOLOGY

Estonian ID-card technology is based on the national ID-card, provided by the Police and Border Guard Board. ID-card provides both, physical and digital use of the card. Each person who recieved the card, also gets 2 PIN codes where first is (4 digits) for digital athentication and second one (5 digits) for digital signing. Validity confirmation service is provided by the Estonian Certification Center. Most of government services are available online (www.eesti.ee), through digital authentication.

In order to sign and view digitally signed documents, free software, called DigiDoc can be downloaded (www.id.ee) by anyone who want to use it, despite of the geographical location. Digital signatures are free of charge for ordinary citizen and signature is binded with time stamp.

Digitally signed documents are stored in a „container" where all signed files are listed on the left side and signature together with time stamp is stored on the right. The solution allows to add as many signatures as needed.



○ Use ID-card ● Use Mobile ID

Mobile number: [redacted]

Personal code: [redacted]

Container: C:\Users\annela\Desktop\BIO-s.ddoc

This container is signed by you

Container content:

BIO-s.pdf 340 KB

Signature

Annela Kiirats
tallinn
manager /
Signed on 20. February 2015 time 12:05
Signature is valid

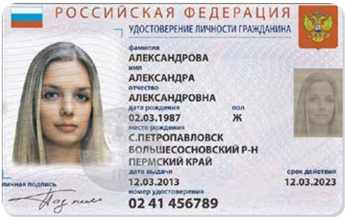
Digital signature is used since 2002 and by the year 2015 already 202 million digital sigatures have been given (there are 1,3 million people in Estonia). ID-card is also a physical identification and travelling document within the European Union (EU) and mandatory identity document. Compulsory from the age of 15.

3.3.2 OVERVIEW OF THE RUSSIAN CRYPTO PRO TECHNOLOGY

On the national level, the principles of ID-cards use (Universal Electronic Card - UEC) have been described in the Federal Law of July 27, 2010 №210-FZ "On the organization of state and municipal services".

Universal Electronic Card (UEC) is a separate type of plastic card which allows the user to perform legal actions, including receiving state, municipal and commercial services in electronic form.

The UEC pilot was launched in 2012 in nine major regions of the country. Starting from 2013 all citizens could apply for UEC. By February 2015 over 500 000 cards had been given out (0.34% of RF citizens).



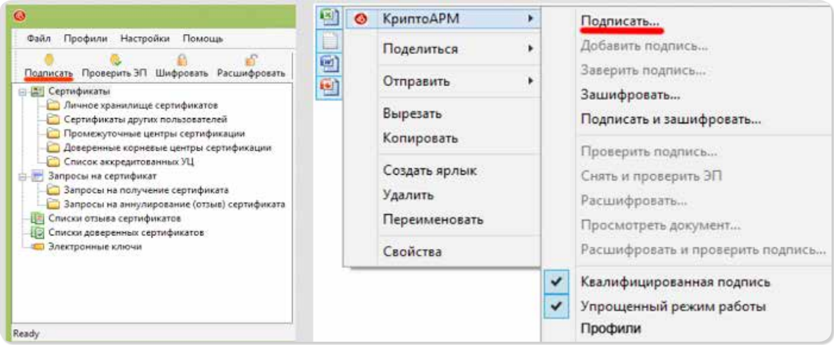
РОССИЙСКАЯ ФЕДЕРАЦИЯ
УДОСТОВЕРЕНИЕ ЛИЧНОСТИ ГРАЖДАНИНА

фамилия
АЛЕКСАНДРОВА
имя
АЛЕКСАНДРА
отчество
АЛЕКСАНДРОВНА
дата рождения 02.03.1987
пол Ж
место рождения
С.ПЕТРОПАВЛОВСК
БОЛЬШЕСОСНОВСКИЙ Р-Н
ПЕРМСКИЙ КРАЙ
дата выдачи 12.03.2013
срок действия 12.03.2023
номер удостоверения
02 41 456789
личная подпись

In September 2013 the Government of the Russian Federation proposed the concept of introducing a new identity card (Electronic Passport) and the issuing process should start from January 1, 2016.

At the moment, in Russia there is no single recommended solution for electronic signature – different software is used: Crypto CSP (Crypto-Pro), CryptoARM (Digital technology), KARMA (EOS), Blokhost-EDS (Gazinformservice), Kriptoserver (Validata) and many others. In government institutions CryptoARM is most often used - a program for encryption and signing of files of any format and size. This program meets all the requirements of Russian legislation in the part of legally significant status and is used to sign documents in the system of e-government services, departmental workflow, various contracts and other documents.

Correctly installed and configured CryptoARM allows the user to sign, encrypt, verify signature and decrypt any file types using its menu as well as using the File Manager context menu.



To use it also across the border (cross-border signing solution), export license is required.

3.3.3 OVERVIEW OF THE LATVIAN ID-CARD TECHNOLOGY

Latvia started issuing electronic identity cards (**eID**), provided by Office of Citizenship and Migration Affairs in 2012, thus joining the group of the EU Member States that have already introduced their national eID. Apart from being a physical identification and travelling document **within the European Union** (**EU**), eID ensures secure authentication for services online and the creation of a legally binding digital signature. This is provided by the appropriate authentication certificate, a means for creating and signing electronic documents, and 120 free-of charge time stamps included in the eID card. Electronic signing service is provided by SJSC "State Radio and Television Centre". As ID-card is not compulsory in Latvia, there are not many users of digital services, nor ID-card based signed documents. Most of the e-services are used by the e-Signature cloud solution (eParaksts) where authentication is made through the bank, or using 3-level mobile-based log-in (mob. No + password + secret question). **Most of the services are available when logging into the bank**.

Third digital signing solutions was created for entrepreneurs and public servants in 2013, as ID-card, not being compulsory document, was not in everybody´s pocket and therefore no good solution for officials to sign documents by not using personal banking for authentication.

3.3.4 OVERVIEW OF THE TECHNOLOGY „WELCOME WITHOUT PASSWORD – WWP"

Several digital identity systems bind a user to a workstation or a particular PC where all the components necessary for work with the authentication tools are installed. Therefore, certain limits in use and inconvenience for users appear.

The technology «Welcome Without Password» (WWP) is newly worked out by the company "e-Signature Without Borders" and is based on complex use of cryptography and electronic signature technology. In order to use the technology, a person needs a smartphone to be able to read a QR code.

WWP technology uses software-based security solutions (tokens and smart-cards use hardware-based security solutions).

Every new client should pay a small fee for the certificate and its maintenance. User identification for the first time is through the bank. The solution has been implemented on the portal of the International system of protection against forgery and counterfeit *"Crypto Contra Counterfeit"* (CCC) http://fbc24.com/. Detailed description of the WWP technology is described in Russian on the following link in YouTube: https://www.youtube.com/watch?v=tHFvfTWet7c

3.4 IMPLEMENTATION OF DIGITAL ARCHIVING IN CROSS BORDER AREAS – *PRACTICAL EXAMPLE FROM THE ESTLATRUS PROJECT*

3.4.1 INTRODUCTION OF ELECTRONIC RECORDS AND DIGITAL ARCHIVING

Digital records are not a new topic – they have been around since the personal computers became prevalent at workplace in the 1990's and provisions have been made for the creation, exchange and archiving of electronic records in legislation by all countries. In Estonia, the main legal acts that the use of electronic records in administrative process relies on, include the:

- Digital signature Act[1]
- Public Information Act[2]
- Archives Act[3]
- Administrative Procedure Act[4]

and several decrees (administrative and records management procedures, archiving procedures, etc.). Majority of existing regulations cover the active stages of the life-cycle of electronic records while the archiving, storage and preservation aspects have usually received less attention. Archiving in paper environment has carried the notion that records are transferred to the custody of an archive once they are no longer needed for current business. In digital environment the archiving may need

[1] https://www.riigiteataja.ee/en/eli/ee/Riigikogu/act/508072014007/
[2] https://www.riigiteataja.ee/en/eli/ee/Riigikogu/act/522122014002/
[3] https://www.riigiteataja.ee/en/eli/530102013053/
[4] https://www.riigiteataja.ee/en/eli/ee/Riigikogu/act/530102013037/consolide

to happen before the records have reached the inactive stage in their life-cycle but the physical custody of digital files can be shared between an archive and the agency, without compromising the accessibility of records.

The practice of digital archiving is varying from agency to agency and often depends on the availability of know-how, tools and skills. The type of electronic records (e.g., textual documents, databases, audio or video recordings, websites, etc.) also appears to determine the level of control that organisations have taken over their assets – the more static data types (images, text) are often under better archival control than the more dynamic object types.

Exercising planned control over life-cycle of electronic records facilitates their archiving towards the end of their life-cycle – adequate metadata, regard for authenticity requirements, integrity control and continuous audit trail options are preconditions for automating the archiving process. Using automated tools to actively manage the electronic records throughout their life-cycle also enables further efficiency in the administrative processes of managing records, responding to customers and creating a knowledge-base for improving user support.

This section of the Handbook will use an **example** from the EstLatRus project – **automating the workflow of archival certificates** – as an example of controlling the life-cycle of electronic records that facilitates digital archiving and provides efficiency gains for the owning organisation.

3.4.2 BACKGROUND OF THE MANAGEMENT OF CROSS BORDER RECORDS

The EstLatRus project set out to facilitate cross-border e-services by developing the enabling legislation, administrative procedures, ICT infrastructure and staff skills. Narva, Kingissep and Slantsy local archives issue certificates to citizens on both sides of the Estonian-Russian border but the current paper-based process is slow. In addition to cross-border acceptance of digital signatures, an obstacle was also the difficulty with managing efficiently and archiving of electronic records. The archival institutions are issuing a broad range of certified document copies to a large number of applicants, a third of which are cross-border. **Efficiency effect** of introducing **cross-border electronic document exchange** and **archiving** would, therefore, be substantial. The process was analysed to determine ways to re-engineer the current business process for efficiency and speed, and to enable digital archiving of created records.

3.4.3 PROCESS ANALYSIS

The process of issuing a certificate usually commences with the receipt of an application via post as a paper document, application handed over in person and often composed on location at the archives, sent by e-mail or fax, or a request made by phone. The processing of an application can take anywhere between one day and one month, depending on the nature of the application and information requested. The average processing time in the archival institution is 1 week. The certified document issued by the archive is final after it has been signed by the responsible official and registered in the archives' records registry. The documents are sent to the applicant by mail, handed over the counter (the person is requested to produce an ID) or sometimes also to a third party person who acts as a courier (a written authorisation is requested).

The **easy-wins in efficiency** during this simple correspondence-based process would be to use alternative tools or techniques, such as the following:

- Using standardised electronic application forms that will ensure that applicants provide sufficient information for fulfilling the request and for archiving the request later as an electronic records. This can reduce the need for asking additional information either from the applicant or other agencies at a later stage of processing the request.

- Scanning and OCRing the incoming paper applications to enable copying of text from them both for searching the information in archives and when compiling the archival certificate. When scanning happens in controlled environment, the scanned versions of applications can be archived instead of the paper documents.

- Using or introducing electronic finding aids for archival collections since search in a database is more efficient than browsing paper-based finding aids. Dedicated archives management software solutions are available on the market. Electronic records management systems (ERMS) can also be configured to act as archival finding aids.

- Defining a shared metadata set for describing the document types that are received and issued by the organisation, as well as shared vocabularies, keywords and thesauri facilitate the search and retrieval process in both electronic records management as well as archives management systems.

- Using organisation's ERMS to assign tasks (e.g. finding the relevant records and compiling the archive's certificate) to members of staff and to track the progress of work. This helps avoiding the situation where some applications are processed for a long time or „forgotten" because an employee's absence, illness or other reasons.

- Digitising the archival records that were found and are used as the basis for archival certificates. The scanned images can be stored in the organisation's ERMS or archival database for checking and future use, for example when a repeated request or application for additional certificates is received.

- Using ready-made document templates for archives' certificates that are linked with the registration system (e.g., ERMS) for incoming applications. Through linking it is possible to automatically fill some fields in the document template and thus speed up the certificate-creation in the archives.

- Using an electronic document or records management system (ERMS) for registration, document approval and digitally signing it within the archives to speed up the review and approval process. For example:

    - Every time a new application is registered, a query should be run in the ERMS to check whether same application already exists or has been dealt with previously so as to speed up the answering process.

    - Possibility for searching for received application in electronic database by various keywords (person's name, geographical area, date range, document type, etc.).

    - Using pre-defined workflows in ERMS for document approval and signing process within the organisation to speed up the review and approval process, and to allow tracking of the process.

    - The resulting digital archive of current, digitally signed records complete with all necessary metadata, can easily be archived electronically either locally or handed over to an archives service provider.

- Using electronic signatures instead of handwritten signatures and organisations' stamps will save time, facilitate electronic document exchange and provide for archiving the documents digitally in the future.

- Sending the finished archival certificates to applicants via electronic channels in order to speed up the forwarding process and to save on postage costs. When files are large or require secure channels of communication file-sharing environments similar to Dropbox can be used that have controlled access and user authentication mechanisms. Export and import with such tools should be integrated into the ERMS solutions.

- To avoid difficulties with using digitally signed documents, institutions should agree on file formats and types of (e.g. very old or very new file formats or their versions; file formats created with software that does not exist at one partner involved in the exchange).

Implementing some or all of these features will automate the workflow associated with handling the requests and issuing certificates in response to them. It will provide the participating organisations in **significant gains** in speed of responding to customer requests, avoiding duplication of effort and build a digital collection over time that can be searched with automated tools and archived as a whole.

3.4.4 LESSONS LEARNED AND CONCLUSIONS

- Digital archiving starts by taking the electronic records under active management control at as early a stage as possible, preferably at their creation phase.

- Digitising paper-based documents will speed up their subsequent processing and will avoid having to create a hybrid collection of both paper and digital records that is more difficult to archive and use.

- Digital archive relies not only on records but also on their metadata – for search and retrieval, but also for verifying the authenticity of records. Standards exist for records management metadata and / or archival description in all countries and these should be used.

- Digital signatures are a primary means for creating, exchanging, archiving and storing authentic electronic records.

- EDMS provide most of the desired features for taking the life-cycle of electronic records under control and also for automating the archiving of records.

- Mutual agreements with key partners in correspondence and reliance on existing standards makes the task of archiving considerably easier.

- Digital archiving does not require significant resources – it can be started using standard office software and tools used for processing documents. The key component is the analysis of records processes and life-cycle with the archiving requirements in mind. The records creation and management processes can be reviewed and re-designed to ensure the creation of a complete digital records' archive. The archive can be maintained in the ERMS until its retention period is over, periodically transferred to a dedicated digital archive management software system, or transferred to an archives service provider / public archive. In the latter case, the regulations and standards established by the archive must be followed.

» Digital archiving will never be fully regulated by legal acts - legislation and regulations only provide the necessary enabling foundation for the use and archiving of electronic records. But the level of granularity required for implementing these processes in practice will always require initiative, planning and management from organisation itself. Useful guidance and best practice exists for the implementation phase (see Appendix 1 – Useful Resources).

APPENDIX 1: USEFUL RESOURCES

Archiving

- Estonian National Archives http://www.arhiiv.ee/en

Digital signature

- Estonian ID-card and digital identity: http://id.ee/index.php?id=30500

Electronic Records Management Systems

- https://www.mkm.ee/en/objectives-activities/information-society/records-management-information-governance
- http://www.nationalarchives.gov.uk/documents/information-management/managing-electronic-records-without-an-erms-publication-edition.pdf

Metadata

- http://community.aiim.org/browse/blogs/blogviewer/?BlogKey=da202182-575a-4ce5-87f5-0c3c1ddf3802&tab=recentcommunityblogsdashboard

Scanning paper documents

- http://www.naa.gov.au/records-management/digital-transition-policy/scanning-incoming-paper.aspx
- http://www.archives.gov/frc/scanning/why-scan.html
- http://www.aiim.org/Research-and-Publications/Research/AIIM-White-Papers/Archived-Content

Other resources

- Digitizing Public Services in Europe: Putting ambition into action - 9th Benchmark Measurement, European Commission (2010)
- Global Information Technology Report 2012, World Economic Forum (2012)
- Study on Analysis of the Needs for Cross-Border Services and Assessment of the Organisational, Legal, Technical and Semantic Barriers, European Commission (2011)
- United Nations e-Government Survey 2012 – *e-Government for the People*, United Nations New York (2012)
- United Nations e-Government Survey 2014 – *e-Government for the Future We Want* (2014)

Estonia – Latvia – Russia Cross Border Cooperation Programme within the European Neighbourhood and Partnership Instrument 2007-2013 financially supports joint cross border development activities for the improvement of the region's competitiveness by utilising its potential and beneficial location on the crossroads between the EU and Russian Federation.

The Programme web-site is www.estlatrus.eu.

e-Governance Academy

e-Governance Academy Foundation
Tõnismägi 2
10122 Tallinn
Estonia

+ 372 641 1313
info@ega.ee