Macedonian Interoperability Building Block: **IOP-L**

(Legal Interoperability)

Peter Parycek, Olga Demian, Bettina Rinnerbauer, Ljubomir Mladenov, Jugoslav Gjorgjievski

Delivery: 15.07.2015
Version: V0.9 FINAL

This project is funded by the

1 Inhalt

1 INTRODUCTION 2

2 EXECUTIVE SUMMARY 3

2.1 Scenario I: recommendations deriving from IOP-O and from IOP-T 3

2.2 Scenario II: Additionally to the amendments proposed for Scenario I, there would be amendments in line with Regulation (EU) 910/2014 necessary 5

2.3 Scenario III: New e-Governance Law 5

3 ASSESSMENT OF THE CURRENT LEGAL FRAMEWORK AND RECOMMENDATIONS 6

3.1 GENERAL RECOMMENDATIONS 7

3.1.1 Legal Framework for E-Governance and the Macedonian Interoperability Framework 7

3.1.2 Law on Electronic management (LOEM) 8

3.1.3 Legislation on electronic identification and electronic signature 11

3.2 RECOMMENDATIONS BASED ON IOP-O 15

3.2.1 Proposed Interoperability structure of the IOP-O: 15

3.2.2 Legal grounds for creation of the IOP Committee: 16

3.2.3 Macedonian business process standard, and the engagement: 16

3.2.4 National competence center: 16

3.2.5 Catalogue on electronic services of the front office 17

3.3 RECOMMENDATIONS BASED ON IOP-T 17

3.3.1 Communication Server 17

3.3.2 Metadata Service Catalogue (MSC) 18

3.3.3 Communication Client 19

3.3.4 Storage of Messages 20

3.3.5 Internal communication between public administration authorities 20

3.3.6 Charging fees 21

3.3.7 Availability of Services 22

3.3.8 Security standards 23

4 ANNEX 24

4.1 THE LEGAL FRAMWORK OF THE FYROM PROVIDED FOR ANALYSIS 24

This project is funded by the

This project is funded by the

1 INTRODUCTION

The following Executive Summary provides an overview of IOP-L. The document in hand especially focuses on recommendations concerning adaptions of the current legal framework of FYROM which is listed as provided for analysis in the Annex of this document.

A key factor in the success of any interoperability, especially in the area of ICT, is to address it at the right legal level for maximum effect and legal amendments could be used for fundamental changes with high effects on efficiency and effectiveness.[1]

Legal aspects such as multiple and conflicting laws on the same matter can hinder interoperability and an assessment of the relevant legal and regulatory framework prior to implementation of the interoperability framework and other relevant initiatives is important.

Moreover, assessment of the ICT implications of proposed legal acts should be considered in due time to permit timely, efficient and effective ICT support for the implementation thereof. In cases when they are not considered during the drafting stage, there is a risk that it will lead to either sub-optimal or missing support through available technologies, resulting in unnecessary administrative burden and/or problems during the implementation phase with regards to the timeline foreseen, lacking interoperability with other systems, feasibility problems. Thus, an early consideration of ICT implications increases the chances for optimal support of the implementation of legislation through ICT technologies, with more guaranties of a timely implementation, cutting administrative burden and avoiding the creation of new e-barriers.[2]

[1] http://ec.europa.eu/isa/documents/isa_2_proposal_en.pdf
[2] http://ec.europa.eu/isa/documents/isa-wp-2014-detailed-description-of-the-actions-part-2_en.pdf


2 EXECUTIVE SUMMARY

In general, there are three action alternatives conceivable, which will be described below. In the end, it is the decision of the BC experts, which of the scenarios is seen as the most suitable option for FYROM respectively which of the proposed measures will be carried out.

- **Scenario I:** Minor amendments of the Law on Electronic Management with regard to the IOP-T and IOP-O could be made. In this case, it would be necessary to change the law especially with regard to the aspects mentioned in chapter 2.1.
- **Scenario II:** Minor amendments of the Law on Electronic Management in line with IOP-T and additionally with IOP-O could be made. Regulation No.910/2014 on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market could be taken into account, especially concerning electronic identification and electronic delivery. If this decision would be made, the measures described in chapter 2.2 would have to be put into effect.
- **Scenario III:** There could be adopted a new e-Governance Law as suggested in chapter 2.3.

Within the meeting on 7 July 2015, the Minister of Information Society and Administration has shown a recognizable tendency of a preference of Scenario II.

In order to enhance implementation of the amended legal framework, it is necessary to regulate its supervision. Considering the responsibilities and competences MISA has in the context of the interoperability framework, this authority shall be mandated with responsibilities in this regard.

2.1 Scenario I: recommendations deriving from IOP-O and from IOP-T

It is recommended to create a legal foundation to ensure successful cooperation between the public authorities, as well as for the decision making process, which is proposed in the IOP-O through an amendment of the LOEM/e-Governance Law. Through the establishment of a cross-governmental IOP Committee, through cooperation with other high-level decision makers, including representatives from the legislature and judiciary branches, especially the aim of commitment, increasing engagement and compliance, shall be pursued. The Committee shall be mandated to create working groups on specific topics and its work shall be administered and supported by an operative unit - the IOP clearing (secretariat). Through a national competence center, which will provide training to enhance the necessary skills, the transfer of knowledge and the international practice will be possible.

Communication Server: It is recommended to include a legal provision in the LOEM/e-Governance Law, which determines to appoint an “institution administrator”, who shall have access to the Communication Server, which contains the rights to access the application of the authority where

This project is funded by the

he/she is employed. The administrator shall assign the rights for access to their web service (database) to other state organisations.

Metadata Service Catalogue (MSC): The authorization assigned by the institution administrator shall be stored in the Metadata Service Catalogue. This Catalogue shall be designed to include information about e-services from the Macedonian Informatics Magistrale (MIM[3])/unique environment.

Communication Client: According to IOP-T the establishment of the role of a "user manager" is proposed. Therefore it shall be determined, who shall assign the rights to access web services (databases) of other organisations to specific natural persons within every organisation internally. It is recommended to include in the LOEM/e-Governance Law the requirement of having a user manager and to describe in further detail in a bylaw the aforementioned task. The requests conducted by natural persons shall be logged at the Communication Client.

Storage of Messages: Messages shall be kept at the Communication Server as well as at the Communication Client solely as long as necessary to deliver them in the shortest technical manner. It is recommended to regulate this in the Rulebook adopted according to Art.8 LOEM.

Communication between Ministries and other authorities: Apart from a few specific exceptions, which shall be clearly defined and listed in an exhaustive way within the LOEM, ministries and other authorities participating in the MIM/unique environment shall preferably use the latter instead of communicating directly with each other.

Charging fees: In order to facilitate electronic data exchange between authorities, it is a prerequisite to clarify models of covering the arising expenses. In particular transaction-based models can be distinguished from flat rate and such solutions, which require reallocation of budget because of refraining from charging fees. In the long term data exchange between authorities at zero cost pricing should be aimed at to enhance data quality and effectiveness of the public administration.
As a first step it is recommended to review the existing contracts for getting an overview about the current situation. New services should be developed on zero costs or flat rate cost models. For the existing transaction based services a migration plan has to be developed. Therefor budget relocations and substitutes have to be developed, so the respective authorities, who run the services, are able to sustain the services in the same or better quality.

Availability of Services: Further the requirement to keep information "generally available" leads to a large scope for interpretation. Therefore it is recommended to determine the manner of availability, which is required (Rules "Form of certification of information systems used by authorities communicate electronically, as well as form and content of certificates of functionality of information systems" adopted pursuant to Art.36 (2) LOEM).

[3] In previous approach it was called "Macedonian Interoperability Bus" (MIB)

Safety standards: Safety standards should be kept up-to-date and in case it is decided (e.g. by the IOP Committee) being suitable, standards should be replaced.

2.2 Scenario II: Additionally to the amendments proposed for Scenario I, there would be amendments in line with Regulation (EU) 910/2014 necessary

Within the IOP Committee there could be established a working group laying special emphasis on Regulation (EU) 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market, which will be repealing Directive 1999/93/EC and shall basically apply from 1 July 2016. The requirement for amendments in order to implement the aforementioned Regulation could be utilised to implement an eID-system, which is fully compatible with the named Regulation as well as the trust services for electronic signatures, timestamps, website certificates and electronic delivery.

2.3 Scenario III: New e-Governance Law

In the light of the further development of electronic services and communication between citizens, businesses and public institutions, it is recommended to broaden the scope of the current Law on Electronic Management (LOEM). In order to achieve this goal, it is proposed to restructure the law, to incorporate new sections in it and to entitle it as “e-Governance Law”.

The structure of the proposed law:

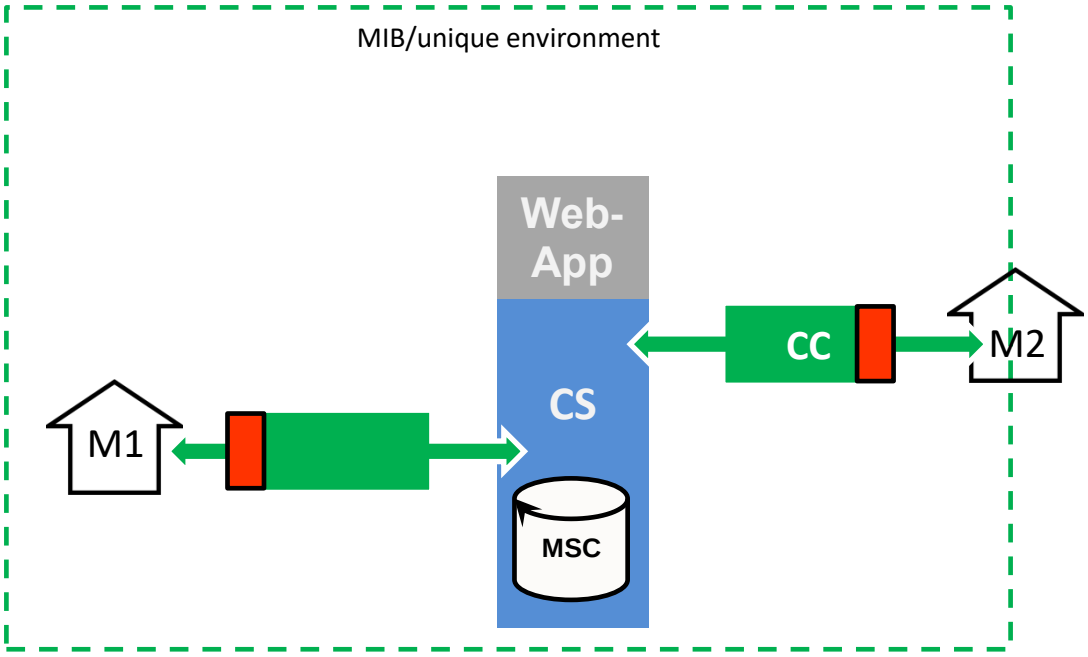
I. General Provisions
II. Legal Definitions
III. Citizen Rights in the Digital Age
IV. Establishment of e-Governance organisations
V. Electronic Data Exchange/Communication within the MIC
VI. Electronic Public Services and Websites
VII. eID - citizens - authorities and eIDAS trust services
VIII. Network and Information Security

This structure is described in detail in chapter 3.1.2.

3 ASSESSMENT OF THE CURRENT LEGAL FRAMEWORK AND RECOMMENDATIONS

Through analyses of the relevant current legal framework experts were provided with, recommendations with the aim to foster and embed internal communication of authorities in line with the interoperability framework into the legislation and avoid e-barriers are formulated.

In the following figure, communication of public institutions via the MIM/unique environment is depicted. As an example of how communication shall be conducted according to the interoperability framework, there are two ministries (M 1 and M 2) shown, who communicate via Communication Clients (CC) and the Communication Server (CS). At the Communication Server, the Meta-Service Catalogue is located. Through the Communication Server, Web-Applications can be accessed.



This project is funded by the

3.1 GENERAL RECOMMENDATIONS

3.1.1 Legal Framework for E-Governance and the Macedonian Interoperability Framework

E-Governance framework and e-Government projects should comprise all state branches - legislative, executive and judiciary. Therefore it is necessary to establish common standards and interoperability for all state organizations in the age of digital communication. Based on the expert's experience and knowledge of the proposed Macedonian Interoperability Framework (MIF) it does not interfere with the separation of power. Interoperability guarantees electronic communication between the organisations, which enables efficient and effective state processes, raises the efficiency and quality of public services and leads to trust of citizens in state institutions and their processes. Implementation of an E-Governance Policy and the MIF is only possible if all institutions closely cooperate, develop and implement policies and standards together.

Current Situation:

There is no overall e-Government legislation in Macedonia.[4] Different laws, bylaws and guidelines have been adopted to enable electronic exchange of data but an overarching strategy and legal framework to ensure interoperability is missing. The law with the main impact is the LOEM. Art.1 LOEM for example stipulates the subject of the law over all as the work of mentioned administrational and other organisations solely concerning the exchange of data and documents in electronic format and concerning the realization of administrative services by electronic means. This limits the scope of the law.

Recommendations:

It is recommended to discuss the introduction of the term e-Governance, which covers digital policies, policy bodies and decision processes (e.g. recommended in IOP-O) and addresses the e-Government applications (e.g. recommended and described in IOP-T).

It is recommended to create a legal framework for implementation of the e-Governance initiatives and the MIF. Therefore, two possibilities seem to be relevant:

1 expanding the purpose of the LOEM, changing the name of the law to e-Governance Law and incorporating general and specific e-Governance aspects. The recommendations reflected in the IOP-O, IOP-T and IOP-L documents should be considered in the context of elaboration of the legal framework;

2 establishing a new law which would address the necessary e-Governance aspects considering that currently, according to the Fact Sheet on e-Government in the Former Yugoslav Republic of Macedonia[5], "there is no overall e-Government legislation in the Republic of Macedonia".

[4] The eGovernment in Former Yugoslav Republic of Macedonia, January 2015, Edition 9.0 https://joinup.ec.europa.eu/sites/default/files/egov_in_fyrom_-_january_2015_-_v.9.0_final_0.pdf

[5] https://joinup.ec.europa.eu/sites/default/files/egov_in_fyrom_-_january_2015_-_v.9.0_final_0.pdf

This project is funded by the

The structure of the proposed new e-Governance law or the subjects, which need to be reflected in the LOEM in force, is described in the chapter 2.3.

Examples of countries which have adopted laws on e-Government, are Austria[6], Greece[7] or Spain[8]. Greece for instance adopted the Law no.3979 on June 16th 2011 on e-Government and other provisions[9]. Spain adopted the Law on e-Government[10] in 2007 which created the National Interoperability Framework (NIF), together with the National Security Framework; the NIF was further developed in a secondary act - the Royal Decree 4/2010[11] of January 8th. Specifically the NIF is based on three key factors: namely the support of a sound legal basis, the role of common infrastructures and services and a strong cooperation effort between public bodies.[12]

3.1.2 Law on Electronic management (LOEM)

Interoperability is one of the essential prerequisite for open, flexible delivery of e-Government services and shall enable collaboration between administrations. Currently in Macedonia, the LOEM is the ground for data exchange; further details are regulated in numerous rules, rulebooks and guidelines.

Current Situation of interrelation of the legal acts:

It is important to identify the legal provision, which is the ground for elaboration of a legal act. Specifically it is necessary to include references to the relevant legal acts in the text of the act. Not all Macedonian legal acts (*translated*) received for analyses, include the legal bases to laws, bylaws and guidelines.

---

[6] Federal Act on Provisions Facilitating Electronic Communications with Public Bodies (E-Government-Act), published in Federal Gazette part I 2004/10, version Federal Gazette part I 2013/83 https://www.ris.bka.gv.at/Dokumente/Erv/ERV_2004_1_10/ERV_2004_1_10.pdf

[7] https://opengov.ellak.gr/?p=223

[8] Law 11/2007 of 22 June on electronic access to public services for members of the public. Available: http://administrLaw 11/2007 of 22 June on electronic access to public services for members of the public. Available: http://administracionelectronica.gob.es/pae_Home/dms/pae_Home/documentos/Documentacion/pae_NORMATIVA_ESTATAL_Leyes/LAW_11-2007_22Jun2007_eGov_Spain_NIPO_000-10-075-0.pdf acionelectronica.gob.es/pae_Home/dms/pae_Home/documentos/Documentacion/pae_NORMATIVA_ESTATAL_Leyes/LAW_11-2007_22Jun2007_eGov_Spain_NIPO_000-10-075-0.pdf

[9] https://opengov.ellak.gr/?p=223

[10] Law 11/2007 of 22 June on electronic access to public services for members of the public. Available: http://administracionelectronica.gob.es/pae_Home/dms/pae_Home/documentos/Documentacion/pae_NORMATIVA_ESTATAL_Leyes/LAW_11-2007_22Jun2007_eGov_Spain_NIPO_000-10-075-0.pdf

[11] https://joinup.ec.europa.eu/sites/default/files/files_epractice/sites/Royal%20Decree%204-2010,%20of%20January%208th,%20which%20regulates%20the%20National%20Interoperability%20Framework%20within%20the%20e-government%20scope.pdf

[12] Miguel A. Amutio "The National Interoperability Framework of Spain, a Global Approach to Interoperability Integrated in the eGovernment Legal Framework" https://joinup.ec.europa.eu/community/nifo/document/national-interoperability-framework-spain-global-approach-interoperability-i

Recommendations:

To foster transparency, it is recommended to include references to laws, bylaws in guidelines and to mention these guidelines in a uniquely identifiable way in bylaws
(e.g. the Rulebook according to Art.8(2) and Art.31(2) LOEM says in Art.7 "The manner of operation and functioning of the Communication Client shall be in compliance with the guidelines adopted by the Ministry", but is not clear which guidelines).

Current Situation of entire IOP/e-Governance overview:

It might be difficult for the state authorities and interested citizens to get an overview of the legislation related to the MIF.

Recommendations:

It is recommended to provide an overview about the relevant legal instruments (Laws, Bylaws, Rules, Rulebooks, Guidelines) and their link as it is for instance in Austria[13]. Additionally, an explanation in a general intelligible way with regard to the organizational structures and the meaning and purpose of interoperability and e-Government could be clarified in a way, which should be understood simply, similarly to the approach of Germany[14] and Austria[15]. This recommendation is crucial for the acceptance and implementation of the MIF.

Current situation with regard to legal definitions

Some important definitions (e.g. Communication Server, Communication Client) are only provided in the Rulebook adopted according to Art.8 (2) and Art.31 (2) LOEM.

Moreover the term "interoperability" is not defined although it is mentioned in the secondary legal acts, namely in two guidelines[16] adopted by the MISA. Furthermore this term is neither mentioned nor defined in the legislative acts provided for analyses.

Recommendations:

In order to avoid misleading interpretation it is recommended to define the main pillars of interoperability, the main terms, including the Meta-Service Catalogue, within the LOEM and to further use them in secondary acts and other relevant documents.

Current Situation establishing nationwide Standards:

Safety standards are currently regulated by the Rules "Standards and rules for the safety of information systems that are used in bodies communicate electronically" adopted pursuant to Article 32 paragraph (3) and Article 33 paragraph (2) of the LOEM.

Recommendations:

It is recommended to establish a legal framework, which

[13] http://www.digitales.oesterreich.gv.at/site/5238/default.aspx
[14] http://www.it-planungsrat.de/DE/Organisation/Organisation_node.html
[15] http://digitales.oesterreich.gv.at/site/5234/default.aspx
[16] (1) Guideline on the manner of use, entry, access to and storage of records for the bases of administrative services by electronic means. (2) Guidelines on the technical requirements, manner of operation and functioning of the communication client, as well as recommendations on the usage of the interoperability system

This project is funded by the

- enables an effective standardization,
- goes beyond security and
- is legally binding for all state branches (central/local public administrations).

Proposed Structure of the new e-Governance law:

This chapter proposes the structure for the new e-Governance Law. The term "section" is used to describe various parts of the Law, but it shall be substituted with the relevant term in accordance with the Macedonian legal framework on elaboration of the legislative acts.

I. **General Provisions:** This section should include the subject, the objective, the purpose and the (broadened) scope of the law. Additionally it could include the general principles upon which the law is based (e.g. privacy by design, technological neutrality, legitimacy, good administration, citizen-centricity, transparency, standardisation and communication, cross-governmental cooperation).

II. **Legal Definitions:** This section should include legal definitions of terms used in the context of the law, including terms in regard to projects implemented in the context of the e-Governance Agenda (e.g. Electronic Identification, Communication Server, Communication Client).

III. **Citizen rights in the digital age:** This section could emphasise the rights exercised by citizens in the digital context (e.g. right of natural persons in connection with personal data processing for the purposes of e-Government, right to access to public sector agency information, right to electronic communication and ICT use, continuous participation in the improvement of functions and services).

IV. **Establishment of e-Governance organisations:** This section of the law should mandate organisations with competences and tasks for efficient and effective cooperation as recommended for example in IOP-O. In regard to the supervision of the implementation of the law, the legislator should delegate supervisory powers to a public authority. Having in mind MISA's leading role concerning the elaboration and implementation of the interoperability framework it is recommended to mandate this authority with supervision responsibilities.

V. **Electronic Data Exchange/Communication within the MIM/unique environment:** This section of the law should include provisions to regulate the electronic data exchange in the public sector. The relevant legal provisions already in force could be incorporated and further described in this section.

VI. **Electronic Public Services and Websites:** This section should include provisions to regulate creation, administration of websites, information obligation of the public administration, provision of electronic public services (e.g. compulsory requirement of bilingualism), etc. One-Stop-Shop could be established and maintained to facilitate access to public services and

information by citizens and business. Creation and maintenance of catalogue on electronic public services is another matter that could be considered.

VII. **eID - citizens - authorities:** In this section the Regulation No.910/2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC[17] could be transposed.

VIII. **Network and Information Security:** This part of the law should regulate network and information security.

3.1.3 Legislation on electronic identification and electronic signature

Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, OJ L 257, 28.8.2014, p. 73–114.

This Regulation determines requirements, the fulfilment of which shall lead to the recognition of identification means for natural and legal persons, who are falling under a notified electronic identification scheme of another member state.

Further, regulations for trust services, electronic signatures, electronic seals, electronic timestamps, electronic documents and electronic registered delivery service as well as certificate services for website authentication are contained. (cf. Art 1)

In contrast to the understanding of authentication in Directive 1999/93/EC, authentication is defined as both, an electronic process, which confirms the electronic identification of a natural or legal person and the confirmation of the originality and the integrity of data in electronic form (cf. Art 3 no. 5).

Trust service means an electronic service, which is provided in return for payment as e.g. issuing and verification of electronic signatures or electronic seals (Art.3 no. 16):

- "Signatory" is defined as a natural person, who issues an electronic signature (cf. Art 3 no. 9). Creator of a seal is defined as a legal person who creates an electronic seal (cf. Art 3 no. 24).
- An electronic timestamp is defined as data in electronic form, which link other electronic data with a specific point of time and hereby prove, that this data was available at this point of time (Art 3 no. 33).
- Electronic document is defined as content in electronic form, especially stored in the form of text, in audio, visual or audio-visual record (Art.3 n. 35).
- Electronic registered delivery service is a service, which enables the transfer or data from third and to third parties by electronic means and which provides a possibility to prove the dispatch and reception of the data and which protects the transferred data from loss, theft, damage and unauthorized change (cf. Art.3 no. 36).

[17] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0910&from=EN

- Certificate for authentication of a website is understood as a certificate, which enables an authentication of a website and which interlinks the website with the natural or legal person, for whom the certificate was issued (Art.3 no. 38).

The Regulation is divided in the following Chapters:

- Chapter I contains general provisions as the subject, scope and legal definitions as described above in extracts.
- Chapter II deals with electronic identification (e.g. requirements for notification of electronic identification systems, levels of security of the latter, notification).
- Chapter III regulates trust services (e.g. supervision, qualified trust services, electronic signatures, electronic seals, electronic timestamps and the electronic registered delivery as well as website authentication.
- Chapter IV contains legal effects of electronic documents, which shall not be denied legal effect and admissibility as evidence in legal proceedings only because of it is in electronic form.
- Chapters V and VI deal with delegation power, implementing provisions and final provisions.

Recommendations:

According to the timeline presented by Neil Clowes in February 2015, the implementing acts with regard to the aforementioned Regulation are now being established[18]. This is why it is now a good moment to launch new projects in Macedonia and to elaborate a comprehensive implementation.
In discussions with local experts it was referred to a project on electronic identification, which is in lead by the Ministry of Interior. It is recommended to create a legal basis for the electronic identification in accordance with the aforementioned Regulation. Additionally, the national legal basis for electronic delivery and electronic documents could be examined as further explained below.

3.1.3.1 Identification and authentication of the organ/authority/legal entity

Current situation

According to Art.7 of the LOEM, the organs, physical and legal entities shall be bound to identify themselves with a single identifier when exchanging documents by electronic means and when realizing administrative services by electronic means. This "single identifier" is needed on both sides according to Art.14 of the Rulebook, according to Article 8, paragraph (2) and Article 31, paragraph (2) LOEM: the user-sender as well as the user-receiver has to be identified by a unique identifier. According to chapter 3 of the Procedures for electronic data and documents exchange through the interoperability system, each authority may have a role of user and/or role of deliverer, which are further described.
The abovementioned provisions point out, that identification shall be ensured by identifying the organ/authority/legal entity, that is requesting or providing information and not the concrete natural person, who requests information.

Recommendations:

[18] http://www.trustindigitallife.eu/uploads/TDW%202015/Presentation-Neil_Clowes.pdf

A database for unique identification would be necessary for the identification process. Therefore the database of the unique identification should be regulated by law. These unique identifiers could also be used for other purposes than these, which are covered by the MIM/unique environment (e.g. Austria has regulated the usage of unique identification numbers within the Austrian e-Government Act)[19].

3.1.3.2 Identification and authentication of a citizen

Current situation

According to Art.17 LOEM, the user can submit requests in electronic format in accordance with the regulations on electronic data and electronic signature. Currently the requirements of Art. 64(2) and especially paragraph 3 Law on General Administrative Procedure and these of the Law on Electronic Data and Electronic Signature are to be met. This implies that submissions basically are to be signed personally while electronically submitted files are to be signed applying an electronic signature.

Currently, the issuer of a qualified certificate (Art.13 Law on Electronic Data and Electronic Signature) is – according to Art.28 Law on Electronic Data and Electronic Signature – required to determine the identity about the certificate holder on the basis of an identity card or passport and all other necessary documents. This process assures identification at the moment, the certificate is issued.

Recommendations

Abstaining from the mandatory prerequisite of an electronic signature whenever submitting requests electronically could contribute in providing a low-threshold electronic submission. This recommendation could already have been taken into consideration while amending the current version of the Law on General Administrative Procedure (clarification).

At the moment the qualified certificate and identification is issued. Afterwards there may arise mistakes e.g. from a change of names through marriage or simply through typing errors. Therefore qualified certificates without a link to the personal identification number cannot ensure the unique identification of a person continuously.

In general, there are for instance the following 3 models of e-ID-concepts, which could be taken into account:

- The identification of citizens may be performed using an identification number in combination of username password solutions.
- For higher security it could be stipulated to use second factor authentication systems (for example a mobile TAN). This way high user verification could be ensured whenever he/she

[19] cf. § 6 (3) Federal Act on Provisions Facilitating Electronic Communications with Public Bodies (E-Government-Act), published in Federal Gazette part I 2004/10, version Federal Gazette part I 2013/83; for companies and state bodies worldwide standardized numbers are use: http://www.gs1.org/id-keys

approaches state organizations and it could be used even for private services like online banking, e.g. Estonian and Austrian eID approach[20].

- The authentication of the citizen's will could be secured by electronic signatures as it is, for example, in Austria or Estonia. This could be done by combining the personal identification number with a qualified signature, which is an advanced signature based on a qualified certificate as is stipulated in Art.13(1) of the Law on Electronic Data and Electronic Signature, or it could also be solved without qualified signatures like in Germany[21].

For example in Macedonia legal amendments are proposed in accordance to EU-law it is pointed out in this context, that Regulation (EU) 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market, which will be repealing Directive 1999/93/EC, shall basically apply from 1 July 2016.
Particularly when initiating administrative penal procedures but also in general for authorities it is on the one hand crucial to know, they are facing the right party. Further administration shall work "customer orientated", therefore the access to electronic government shall be inclusive. According to the European e-Government Action Plan 2011-2015,
"Increasing effective e-Government means that services are designed around users' needs and provide flexible and personalised ways of interacting and performing transactions with public administrations."[22]
Within the above-mentioned document, practical e-identification and e-authentication solutions are called "Key Enabler" in the sense of a precondition for developing e-government. For this reason, we recommend the establishment of an easy-to-use e-identification.
Based on current insights, the personal identification number could be used to access services according to the Law on Personal Identification Number. If data protection concerns will be raised derived identification numbers could be established as it is in use in Austria.

3.1.3.3 Electronic Signatures

Current situation

Currently, electronic signatures are regulated by the Law on Data in Electronic Form and Electronic Signature. During the discussion with Ljubomir Mladenov and Jugoslav Gjorgjievski[23], Ljubomir Mladenov mentioned that the competency for regulating the Law on Data in Electronic Form and Electronic Signature has moved from Ministry from Finance to MISA and that MISA is going to make amendments. The Regulation (EU) 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market, which

[20] Estonian and Austrian eID System are also used for online banking; https://www.handy-signatur.at/ Estonia all banks work closely together with eID development and implementation. The eID card, according to the E-Government fact Sheet, fulfils the requirements of Estonia's Digital Signatures Act (https://www.riigiteataja.ee/en/eli/ee/Riigikogu/act/508072014007/consolide) https://joinup.ec.europa.eu/sites/default/files/egov_in_estonia_-_january_2015_-_v_17_final.pdf

[21] http://www.neuer-personalausweis.org/

[22] The European e-Government Action Plan 2011-2015, Harnessing ICT to promote smart, sustainable & innovative Government SEC(2010) 1539 final, 5.

[23] cf. Minutes of the Meeting of 14 May 2015

will be repealing Directive 1999/93/EC and shall basically apply from 1 July 2016, the Law on Data in Electronic Form and Electronic Signature could be considered and transposed in this regard.

Recommendations

Electronic signatures play a large role with regard to electronic identities, electronic delivery, and the unique environment. An amendment of the Law on Data in Electronic Form and Electronic Signature is recommended in accordance with the implementing provisions.

3.1.3.4 E-delivery

As proper delivery is crucial in administrative procedures, for instance concerning summons (Art.67 and the following of the Law on General Administrative Procedure) or decisions, electronic delivery is an important instrument for organs.

Current situation

Currently electronic delivery is regulated in Art.20 of the LOEM. Paragraph 1 of the aforementioned Article says "The user shall be bound to report his electronic mail address of receipt of administrative services by electronic means to the provider, in accordance with law." The requirements of Art.78 and the following Articles of Law on General Administrative Procedure have to be met. According to Art.84 Law on General Administrative Procedure, service shall be performed by mail, if the body fails to serve the parties by direct delivery.

Recommendations

It is recommended to regulate in more detail electronic delivery and to consider amending it according to the Regulation (EU) No 910/2014.

According to the feedback provided by BC experts, electronic delivery is regulated by the draft of the new Law on Administrative Procedure, which is currently in the parliamentary debate. It is recommended to align these provisions with the aforementioned Regulation (EU) No 910/2014.

3.2 RECOMMENDATIONS BASED ON IOP-O

3.2.1 Proposed Interoperability structure of the IOP-O:

A strong cooperation effort among public administrations and a centralized regular monitoring of interoperability initiatives are considered to be the basis for an effective implementation of the national interoperability framework.

In order to strengthen interoperable services and systems at the governance and organisational levels in Macedonia, the IOP-O proposes a number of recommendations, namely (a) to establish a cross-governmental IOP committee, (b) to create an IOP Clearing, (c) to implement a Common Assessment Method for Standards and Specification (CAMSS), (d) to establish a Macedonian business process standard, (e) to establish a national competence center, etc.


3.2.2 Legal grounds for creation of the IOP Committee:

Specifically, the IOP-O recommends creation of the high level-IOP Committee. It shall be mandated to maintain, decide on adjustments and changes to the MIC and MIF. Currently, there is no legal base for creation and functioning of this high-level IOP committee.

Recommendations

It is recommended to adapt the current legal framework by either extending the scope of the existing LOEM or by introducing specific provisions in the new law on e-Governance.

With regard to members of the IOP committee, the IOP-O suggests that members shall be high-level decision makers from both the central and local administrations. Nevertheless in order to encourage cooperation, to increase the efficiency and effectiveness delivery of public sector and cooperation between authorities through the use of information technologies, representatives from both the legislative and the judiciary could become members of the same committee.

New legal provisions shall also detail the procedure for appointment of members and the chairperson of this committee. With regard to the last, the MISA's role, which is the authority de facto responsible for the IOP portfolio, could be considered.

The main tasks of the IOP Committee, which are summarised in the IOP-O, shall be included and detailed in the legal framework (e.g. in the new law on e-Governance).

Additionally, for the purpose of supporting the maintenance, development and compliance with the MIC and MIF and other related standards, schemes and use of infrastructure, which are proposed by the IOP-O, the legal framework shall regulate creation of permanent or temporary working groups.

The IOP-O proposes to establish a clearing (administrative) body, which would have an administrative role, namely to support the activity of the high-level cross-governmental IOP committee and to organize the relevant processes. At present, no legal acts establish this kind of body.

Amend the legal framework to regulate the establishment of the IOP clearing body (secretariat). New provisions shall detail responsibilities of the clearing body.

3.2.3 Macedonian business process standard, and the engagement:

A legal base is necessary to implement the recommendation made in the IOP-O concerning the business process standard in line with the EIF V2 and to document them.

Recommendations

It is suggested to regulate the establishment of a business process standard in the secondary legal acts, which would create a legal base in this regard.

3.2.4 National competence center:

The IOP-O includes a recommendation about creating a new competence center, which has the objective to ensure, establish and maintain the responsible authority as a source of expertise and knowledge transfer and thus supporting compliance.

This project is funded by the

Recommendations

It is recommended to regulate this aspect, for example, in bylaws or in contract, like it is done in Austria and Germany[24].

3.2.5 Catalogue on electronic services for the front office

The LOEM regulates the right to interact electronically with the public authorities. Specifically it provides that public administrations are obliged to provide public services by electronic means within their scope of work, unless the law envisages another procedure for providing those services.[25]

Access to electronic public services is allowed through the portal for the administrative services by electronic means. The MISA is responsible to maintain this portal and to prescribe the "form and content of the basic elements of the request for delivery of administrative services by electronic means" (Art.13, LOEM).

The legal acts provided for analyses do not stipulate expressly the obligation to create, approve and maintain the Central National Catalogue of Electronic Services.

Recommendation

It is recommended to amend the legal framework to address the underlying principles of public services through the service lifecycle - planning, design, acquisition, implementation, deployment, exploitation, publication, preservation.
Moreover, it is recommended to mandate an authority to develop, maintain the catalogue of electronic services for the front office and to obligate the relevant authorities to provide information, which is necessary for maintaining and updating the content of this catalogue.

3.3 RECOMMENDATIONS BASED ON IOP-T

3.3.1 Communication Server

The IOP-T proposes that the systems should rely on a centralized architecture having a central communication server acting as mediator for various communication clients.
According to IOP-T, a user manager (institution administrator) responsible for setting up the user rights for the Macedonian Interoperability Bus (MIM)/unique environment has to be appointed.

Current legal situation

The "Guidelines on the manner of use, entry, access to and storage of records for the bases of administrative services by electronic means" regulate (2.) that "only persons authorized by the Minister of Information Society and Administration shall have access to the records, shall use them and enter information, and shall undertake activities with regard to their storage".

[24] https://www.egiz.gv.at/ or https://www.fokus.fraunhofer.de/go/elan

[25] Article 10 of the Law no.07-3641/1 of 21.08.2009 on Electronic Management

The legal basis of the guideline is not clear. A reference to the bylaw according to which it was adopted (see general recommendations above) could be made.

The Guidelines on certification of information systems contain the requirement to have appointed persons to the position of "network administrator" and "system administrator". These terms are neither defined, nor could there be identified a description of tasks of these administrators.

Recommendations

It is recommended to include a provision in the LOEM/e-Governance law to oblige every participating authority/organisation to appoint an "institution administrator". The administrator shall have access to the Communication Server, which contains rights to access the application of the authority where he/she is employed. The administrator shall assign rights to access their web service (database) to other state organisations; this authorization claim is stored in the Meta-Service Catalogue. Responsibilities of the institution administrator should be regulated.

Moreover, it is recommended to define the phrase MIM in a bylaw of the LOEM.

3.3.2 Metadata Service Catalogue (MSC)

The central interoperability model is based on two different enterprise service buses. In this model, the MIM/unique environment relies on two instances for managing metadata of services or authorization information. These so-called Metadata Service Catalogues (MSC) include e-service information from the MIM/unique environment. Every e-service should be registered at the Communication Server concerned and stored in the MSC.

Current situation

The "Rulebook on the manner of recognizing the unique environment and electronic communication between authorities via the unique environment for electronic documents and data exchange", adopted to Art.8 LOEM, defines Communication Client and Communication Server, but it does not define the Metadata Service Catalogue, which is one of the crucial parts of the MIM/unique environment.

Recommendations

Over all to avoid misinterpretation, the term "Service Catalogue" shall not be used in this context. This catalogue addresses the services of the back office, for this reason the term "Metadata Service Catalogue" should be used preferably. The use of "Service Catalogue" could be misleading, because, in the European context, the Catalogue of Public Services also means an overview of the public services for customers - "ISA Action 1.3: Catalogue of Services"[26]. MSC, as is used in the IOP-T, would be a recommended phrase.

Furthermore the phrase "Metadata Service Catalogue" should be defined within the LOEM and it should include a minimum set of information concerning how a service should be described (metadata e.g. what kind of data).

[26] http://ec.europa.eu/isa/actions/documents/catalogue-of-services.pdf

One centralized Metadata Service Catalogue would – especially with regard to the resources of public administration – for the long-term perspective also be a possible approach.

3.3.3 Communication Client

Current situation

The Communication Server and the Communication Client have been established by the Rulebook, which was adopted according to Art.8(2) and Art.31(2) of the LOEM, of which Art.7 assigns the establishment and maintenance of the Communication Clients to the authorities and the undisturbed functionality of the Communication Server (Art.15 Rulebook) to the MISA.

According to the IOP-T, the responsibility for the Communication Client shall lie with the participating ministry and the responsibility concerning the Communication Server, which belongs to the unique environment, shall lie with MISA. The current legal framework already assigns responsibilities this way.

The messages between communication client and e-service shall be encrypted based on IOP-T, which is regulated in Art 9 Rulebook adopted according to Art.8 LOEM ("cryptic form"). Within the "Guidelines on the technical requirements, manner of operation and functioning of the communication client, as well as recommendations on the usage of the interoperability system (6.2)", encryption is regulated in more detail.

The Communication Server shall only link the message from Communication Client to electronic service (Art.7 Rulebook adopted according to Art.8 LOEM) and the electronic service shall only record that an organization (unique identifier of the user-sender and user-receiver) has sent a message. This does not mean to protocol the message body (content), but the fact, that the message was invoked/delivered. According to Art.14 Rulebook adopted according to Art.8 LOEM, there is an obligation to record each transfer of electronic documents "in the database of the information system of the unique environment". Currently, there is no legal obligation to log the requests conducted by individual natural persons in the Communication Client System.

Recommendations

According to IOP-T, the establishment of the role of a "user manager" is proposed. Therefore it shall be determined, who shall assign the rights to access web services (databases) of other organisations to specific natural persons within every organisation internally. It is recommended to include in the LOEM/e-Governance Law the requirement of having a user manager and to describe in further detail in a bylaw the aforementioned task.
The request conducted by natural persons shall be logged at the Communication Client, for there, the user-management shall be implemented.

It is recommended to clarify, which database is meant by the term "the database of the information system of the unique environment" and to enforce a legal obligation to store the information about which natural person accessed what information internally at the Communication Client within each of the respective participating organisations. A relevant authority, for instance, the Directorate for

Personal Data Protection could inspect on a random basis if the access is conducted in accordance with the access authorizations.

In Estonia, for example, a separate chapter (5), which is incorporated in the Public Information Act[27], regulates the establishment and administration of databases, including establishment of the support systems to state information system (§43), the role and responsibilities of the chief and the processor (administrator) of a database (§43), conditions for access to database (§43), statutes of databases. Moreover, establishment of separate databases for the collection of the same data is prohibited pursuant to the §43(2) of the same act.

3.3.4 Storage of Messages

Current situation

According to IOP-T, the to-be-delivered messages shouldn't be stored at the Communication Server or at the Communication Client longer than it is technically absolutely necessary. No provisions could be identified, which would regulate these aspects.

Recommendations

If the participating ministries communicate with each other (request - reply) via the Communication Server, the latter and the Communication Client shall not be allowed to store/keep messages. They shall be kept solely as long as necessary to provide them in the system in the shortest technical manner. The actual content must not be inspect able by the MIM/unique environment as message encryption is a legal obligation. It is recommended to regulate these matters in the Rulebook adopted according to Art.8 LOEM.

With regard to electronic logging in other jurisdictions, the Law no.3979 on e-Government of the Hellenic Republic of 16 June 2011 could be mentioned as it includes provisions which regulate electronic logging.[28] Specifically, it provides that "every public sector agency shall maintain an electronic log, where it will record acts such as the issue, delivery, notification, transmission of documents, which are either issued by that agency, held by it or come into its possession in the framework of the exercise of its authority"(Article 16).

The International Organisation for Standardisation provides guidance and requirements on logging and monitoring in the 27000 family standards. The ISO/IEC 27002:2013, for example, includes requirements and advice to satisfy the control objective - to record events and generate evidence - with regard to logging and monitoring (chapter 12.4), which could be consulted.

3.3.5 Internal communication between public administration authorities

There are two possibilities to regulate communication between authorities, namely via bilateral agreements and via the MIM/unique environment. According to IOP-O, authorities, which communicate through the MIM/unique environment, shall communicate directly with each other

[27] https://www.riigiteataja.ee/en/eli/ee/Riigikogu/act/522122014002/consolide

[28] https://opengov.ellak.gr/?p=223

solely in exceptional cases. Public administration shall communicate via the MIM/unique environment, which is operated by the MISA (Art.31 LOEM).

Current legal situation

The communication through the MIB/unique environment is regulated by Art.4 of the Rulebook "On the Manner of Recognizing the Unique Environment and Electronic Communication between Authorities via the unique Environment for electronic documents and data exchange", adopted according to Art.8 (2) and Art.31 (2) LOEM and stipulates that the MIB/unique environment shall be used for data exchange from authorities certified information systems.

Recommendation

It is recommended to define exceptions in detail in the LOEM. It is recommended, that the IOP Committee elaborates the necessary exceptions and lists them in a complete manner (in the sense that there are no other reasons possible for not participating in the MIM/unique environment than the ones mentioned). The IOP Committee is especially appropriate for this task because of the possible consideration of the perspectives of its members.

3.3.6 Charging fees

Current Situation

The legal framework in force allows authorities to charge fees for accessing services. Discussions with BC experts indicated, that in practice, there are mostly contracts in force, which regulate transaction-based payment.

Recommendations

In general, three models to deal with the costs produced by data exchange between authorities can be observed:

- Transaction-based payment
- Flat rate
- No payment

Out of experience there is a high risk that transaction-based payment may lead to a decreased use of registers/databases and data may be stored numerous times. This may result in inconsistencies of data as authorities may – driven by economic considerations – store data they have bought and tend to re-use them. To avoid that risk public administration authorities could be encouraged to provide access to registers to other authorities for free or based on a flat rate model.

Nevertheless experts are aware of the fact that there are authorities which depend on generating income through making their data available to other authorities to finance themselves. In these cases a reallocation of budget is necessary for successful implementation of the interoperability framework. To reach long term objectives as improved services for citizens and businesses and increased transparency the requirement of budget reallocation would have to be met in these cases.

Whenever creating new services existing contracts should be reconsidered and there should be taken into consideration to regulate charging a flat rate if out of economic considerations abstaining from charging fees cannot be regarded as an action alternative.

With regard to existing services and related contracts, it is a political decision, whether reallocation of budget is regarded as a suitable option and as a result, these contracts could be amended and a flat rate could be introduced. Those charges nevertheless should be set according to objective, transparent and verifiable criteria.

In the long term perspective abstaining from charging fees concerning data exchange between authorities should be targeted.

3.3.7 Availability of Services

Current situation

According to the Guidelines on certification of information systems which refer in a very general way to "the rulebooks deriving from the Law on Electronic Management" (see general recommendations) a requirement for certification of functionality of an information system (4.1) is that the information is public and "generally available".

Recommendations

For clarification it is recommended to make references to the respective legal provisions or legal acts generally more precise. For example §3 of the Guidelines on certification of information systems could be amended to specify the legal act that it refers to rather than stating that "according to the rulebooks deriving from the Law on Electronic Management".
Further the requirement to keep information "generally available" leads to a large scope for interpretation and it would be recommended to determine the manner of availability. Availability of classifications and the manner of the answer of a back-end-system should be detailed in a bylaw. If services meet the requirement of a bylaw, the requirement of bilateral agreements containing an obligation to keep information of base registers available, which shall be the foundation of services, will not be necessary. This is how the objective to have all authorities obliged to keep their information available could be reached. The participating authorities are highly interested in being able to rely on the availability of the information/services.

The Estonian Public Information Act[29] stipulates that before the introduction of a database it shall be registered in the administration system of the state information system - one of the support systems established according to §43 of the same act (§43). Moreover it stipulates that "before a database belonging to the state information system is registered, an official or employee of the Estonian Information System's Authority which has appropriate competence shall check and harmonise the technical conformity of the database and the conformity of the data to be collected and the sources thereof with the requirements established by law or legislation issued on the basis thereof" (§43).

[29] https://www.riigiteataja.ee/en/eli/522122014002/consolide

This project is funded by the

3.3.8 Security standards

Current situation

According to the Rules "Standards and rules for the safety of information systems that are used in bodies communicate electronically" adopted pursuant to Art.32 (3) and Art.33 (2) LOEM, the use of EN ISO/IEC 27000 family standards is regulated.

Except the Law of Personal Data Protection (Art.5) laws provided for consultation do not include an obligation of public authorities in regard to quality of data which, thus, needs to be exchanged within the public sector.

Recommendations

Having in mind that in 2013 the International Organisation for Standardisation adopted a new edition of ISO/IEC27001 and ISO/IEC27002, it is recommended to align the Macedonian rules on information security to the latest version of these standards.

Moreover, once adopted the Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union[30] will be relevant.

With regard to personal data protection in the EU, the new draft Regulation on personal data protection could be consulted. The key changes concern: (a) a right to be forgotten; (b) the right of data portability, i.e. easier transfer of personal data from one service provider to another; (c) increased responsibility and accountability for those processing personal data including the obligation to inform the relevant authority in case the personal data has been hacked within 24h; essential principles 'Data protection by design' and 'Data protection by default' – this means that data protection safeguards should be built into products and services from the earliest stage of development, and that privacy-friendly default settings should be the norm; (e) explicitly given consent whenever is required; etc.[31]

[30] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52013PC0048

[31] http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm

4 ANNEX

4.1 THE LEGAL FRAMWORK OF THE FYROM PROVIDED FOR ANALYSIS

The STEs thank the BC experts for presenting the following legal acts for analyses. Detailed information can be inferred from the assessment of the current legal framework and recommendations above.

1. Legislative acts:
   - 1.1. Law No.07-3641/1 on Electronic Management
   - 1.2. Law No. on Classified Information
   - 1.3. Law on Data in Electronic Form and Electronic Signature
   - 1.4. Law on Free Access to Public Information
   - 1.5. Law on Personal Data Protection
   - 1.6. Law on Personal Identification Number
   - 1.7. Law on Records of Births Deaths and Marriages
   - 1.8. Law on the General Administrative Procedure
   - 1.9. Law on ex officio collection and exchange of data

2. Bylaws
   - 2.1. Bylaw pursuant to Article 13 paragraph (2) and Article 19 paragraph (2) of the Law on electronic governance (Rules The format and content of the basic elements Request for submission of administrative services electronically and format of documents in electronic form)
   - 2.2. Bylaw pursuant to Article 36 paragraph (2) of the Law on Electronic Governance (Rules Form of certification of information systems used by authorities communicate electronically, as well as form and content of certificates of functionality of information systems)
   - 2.3. Bylaw Pursuant to Article 34 paragraphs (2) and (4) and Article 35 paragraph (2) of the Law on Electronic Governance (Rules The format and content of the records of databases of bodies Mutual communicate electronically, the manner of its guidance, format and content of the form of notice to establish the base for its Maintenance and storage, as well as changes that apply to its status, the manner of notification, and the way the use, registration, access and preservation of the records of the Database and services electronically)
   - 2.4. Bylaw pursuant to Article 32 paragraph (3) and Article 33 paragraph (2) of the Law on Electronic Governance (Rules Standards and rules for the safety of information systems that are used in bodies communicate electronically)
   - 2.5. Bylaw pursuant to Article 16 paragraph (1) of Electronic Governance (Rules For technical requirements for providing access to administrative services by electronic means the provider and policy of use of graphics and Other Information Portal System)


2.6. Bylaw according to Article 32, paragraph (2) from the Law on Electronic Management (Rulebook on the standards and rules and unified numerations in the mutual communication by electronic means)
2.7. Bylaw according to Article 8, paragraph (2) and Article 31, paragraph (2) from the Law on Electronic Management (Rulebook on the manner of recognising the unique environment and electronic communication between authorities, Rulebook on the manner of recognising the unique environment and electronic communication between authorities via the unique for electronic document and data exchange)

3. Guidelines
3.1. Guidelines on the technical requirements, manner of operation and functioning of the communication client as well as recommendations on the usage of the interoperability system
3.2. Guidelines on the levels of classified information and on access levels
3.3. Guidelines on monitoring and management of information security incidents
3.4. Guidelines on the manner of use, entry, access to and storage of records for the bases of administrative services by electronic means
3.5. Guidelines on activities undertaken according to risk assessment and management
3.6. Procedures for electronic data and documents exchange through the interoperability system

This project is funded by the