Ministry of Economic Affairs and Communications

Interoperability of the State Information System

Endorsed with the Directive of the Minister of Economic Affairs and Communications 11-0377, 22.12.2011

Framework

Version 3.0

2011


BY
SA

Ministry of Economic Affairs and Communications

Interoperability Framework of the State Information System

Version 3.0
2011

The present document is a part of the interoperability framework of the state information system. The document is open for suggestions from public, private and third sector institutions and all the interested parties. We ask you to send your suggestions to the e-mail address koosvoime@riso.ee.

The documents of the framework are constantly updated and the current state of the document is published in the wiki of the state information systems[1]. After updating, the official version of the document is endorsed, which is coordinated with the institutions of the public sector and published on the website of the framework of interoperability[2].

[1] http://www.riso.ee/wiki/
[2] http://www.riso.ee/et/koosvoime/
[3] http://www.creativecommons.ee

Contents

1. Introduction

21-st century key words – citizen centred state and service oriented information system necessitate linking information systems into an integrated logical whole, supporting citizens and organizations. To make it come true, different organizations and information systems must be interoperable, or in other words, they must be able to work together.

Interoperability is the ability of disparate and diverse organisations to interact towards mutually beneficial and agreed common goals, involving the sharing of information and knowledge between the organizations, through the business processes they support, by means of the exchange of data between their respective ICT systems4.

Interoperability, based on standards and open platforms[5] is the precondition of achieving the objectives of the European Digital Agenda[6], which was a leading initiative of "Europe 2020". Hence, interoperability is not merely an IT issue, but includes very many facets of information society.

Interoperability framework is an interorganizational agreement and instrument to achieve interoperability. The framework is a collection of requirements, standards and instructions, handling the interoperability of information systems and services of the Estonian public sector, which ensures serving public sector institutions, enterprises and citizens[7] both in Estonia and all over Europe.

Interoperability framework is a guideline for preparing public sector IT legal acts, designing IT solutions and organizing IT related public procurements.

The objective of the interoperability framework is to make the operation of the Estonian public sector more effective, improving the services offered to Estonian and EU citizens. The more concrete objectives of the framework are:

- To contribute to the development of a service oriented society, where people can communicate with the state without knowing anything about the hierarchic structure of the public sector or the division of roles in it.
- To bring more transparency into information related political decisions of the information system.
- To support co-development of the state information system.
- To create conditions for free competition, following the agreed framework.
- To reduce public sector IT costs.

The target group of the interoperability framework is chief executive officers (CEO), chief financial officers (CFO), chief information security officers (CISO), chief information officers (CIO) and chief technical officers (CTO)[8]. The present document is also a guideline for private sector managers and project leaders who offer development and administrative services to the public sector.

The Ministry of Economic Affairs and Communications **(**MKM**),** as the ministry responsible for developing the state information system, is responsible for designing the **Interoperability framework and the related documents.** At MKM, there was created an interagency state information systems interoperability working group, whose duty is to advise the ministry on designing interoperability documents. For the sub-topics of the interoperability framework, there have been created official and unofficial working groups.

Legal status of the framework

[4] http://ec.europa.eu/isa/documents/isa_annex_ii_eif_en.pdf

[5] European Parliament and Council's September 16, 2009 decision No 922/2009/EÜ on ISA http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:260:0020:0027:ET:PDF.

[6] KOM(2010)245 European Digital Agenda, http://ec.europa.eu/information_society/digital-agenda/index_en.htm.

[7] In interoperability documents the word "citizen" is used in a broader sense, meaning not only Estonian citizens.

[8] Internationally recognized abbreviations: CEO (*Chief Executive Officer*), CFO (*Chief Financial Officer*), CIO (*Chief Information Officer*), CISO (*Chief Information Security Officer*), CTO (*Chief Technical Officer*).

Pursuant to the Government of the Republic Act § 63, subsection 1 and the Government of the Republic's resolution on 23.10,2002, No 323 § 12, subsection 5, the Ministry of Economic Affairs and Communications (MKM) organizes designing and implementing development plans relating to IT and telecommunications, as well as coordinates the development of the state information system. The interoperability framework is a strategic document, which MKM is guided by when it makes political decisions with regard to information, assesses projects financed from structural funds, prepares legal acts with regard to the state information system, coordinates IT and communications related legal acts of ministries and coordinates information systems in the management System of State Information System (RIHA). Interoperability documents are enforced with a directive of the minister coordinating the state information system and compliance with them is obligatory for those who organize communication of the information systems of the state and local governments.
In addition, the framework is obligatory as an agreement between different parties. The framework and related with it documents, go through a consultation period, during which state and local government institutions, the private sector, third sector institutions and private persons can make amendment and improvement suggestions. The suggestions and comments are discussed by the executive group of the interoperability framework and its final version is considered as an agreement between different parties.

Several requirements of the interoperability framework cannot be fulfilled by all institutions at once, it may take several years. Although, every institution should have an action plan to reach the results.

European interoperability framework

From the point of view of the development of the common market of the EU, in addition to domestic interoperability, it is also important to have interoperability of IT systems and services of the EU countries. In the EU, interoperability is handled, first of all, in European Interoperability Strategy[9] European Interoperability Framework[10], whose principles and terminology are also followed by the present framework.

The Estonian framework makes use of the European one as a metaframework. The Estonian framework gives answers to the question how Estonia ensures fulfillment of European requirements, although the focus of the framework is requirements for Estonian administrative institutions, to ensure domestic interoperability.

The Government session on 17.02, 2011, supported the positions of the European interoperability framework. At the same session, the Government also approved the objectives of the European e-Government action plan, according to which, the member states must harmonize their frameworks with the European ones.

History of the interoperability framework

The first document of the interoperability framework of the state information system “State IT Interoperability Framework” was published in 2004. Its size and relevance has grown over the years and the third version differs somewhat from the previous ones. On the one hand, the new interoperability framework reflects the principles of the EU interoperability strategy and framework. On the other hand, interoperability here is interoperability of services, information systems and administrative processes. That is why the framework has been given a more general title now.

Framework content

The framework contains common agreed elements like a list of documents, dictionary, understandings, principles, policy, guidelines, recommendations and practice.The documents of the framework have been divided into four groups:

I. General documents

[9] http://ec.europa.eu/isa/documents/isa_annex_i_eis_en.pdf
[10] http://ec.europa.eu/isa/documents/isa_annex_ii_eif_en.pdf

- Framework (the present document)
- Interoperability dictionary[11]
- Questionnaire on assessment of compliance with interoperability requirements[12]

II. Frameworks of interoperability dimensions and spheres

- Interoperability documents of specific/different spheres (for example, semantic interoperability, security, software, websites, management of documents, open standards, development framework)

III. Infrastructure

- Architecture of joint services of infrastructure (e.g backbone network Peatee, electronic identity infrastructure, secure data exchange layer X-Road)

IV. Guidelines

- Guidelines and procedures (documents which support and specify documents of level II and III).

It is recommended to start one's acquaintance with the framework from this document and then continue in accordance with one's interests.

The key words of the document “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY” and “OPTIONAL” should be interpreted as specified by Internet Engineering Task Force (IETF)[13]. To highlight the relevance of these words, they have been provided in block capitals and their meaning is as follows:

Meaning	**Words expressing the meaning**
Required/obligatory (absolute requirement or prohibition)	*MUST, REQUIRED, SHALL*
Recommendation (full implications must be understood and carefully weighed before choosing a different course)	*SHOULD, RECOMMENDED*
Acceptable/allowed	*MAY, OPTIONAL*
Not recommended (acceptable only under particular reasons or circumstances)	*SHOULD NOT, NOT RECOMMENDED*
Prohibited (absolute prohibition)	*MUST NOT, SHALL NOT*

The framework uses the style of open standards and European decisions, in which requirements provided in the conditional mood do not imply condition, but such an obligation, with regard to which there may be exceptions, as a certain requirement cannot be fulfilled completely. In that case, making an exception must be carefully considered and justified.

The most relevant conclusions and requirements have been provided in boxes with a green background. The requirements are numbered within a chapter throughout.

2. Underlying principles of interoperability

Interoperability framework is an information related political document of the Republic of Estonia and is guided by the European Interoperability Framework and its 12 principles:

1) subsidiarity and proportionality
2) user-centricity
3) inclusion and accessibility

[11] http://www.riso.ee/wiki/Sonastik
[12] http://www.riso.ee/et/files/Kooskolastamise_protseduur.pdf
[13] Internet Engineering Task Force (IETF) RFC 2119: „Key words for use in RFCs to indicate requirements levels“

4) security and privacy
5) multilingualism
6) administrative simplification
7) transparency
8) preservation of information
9) openness
10) reuse
11) technological neutrality and adaptability
12) effectiveness and efficiency

The most relevant and general principle is that of subsidiarity. Principles 2-8 handle end users' needs and expectations. Principles 9–12 are oriented at common activity of public sector institutions.

Although the fundamental principles have been taken from the European framework, what follows is not a repetition of the European angle, but peculiarities and specifications of the application of these principles in the Estonian context.

2.1. Subsidiarity and proportionality

Subsidiarity principle has its origins in the European Union Treaty. In that document, subsidiarity principle means that all information related political decisions in Estonia are made on a low, closer to user level. Interoperability related decisions are made on a state level only if they are more efficient than the ones made in public sector institutions.

In Estonia, application of subsidiarity principles means that centralized solutions are used as little as possible. Centrally it is worhtwhile to realize only joint infrastructure services (e.g public key infrastructure, X-Road, state information system's management system), and the systems providing joint services for citizens from public sector institutions (e.g information portal eesti.ee). Ministries do not force central solutions in their areas of government, where an institution may lose control of business processes. Neither does the central government prescribe technical solutions for local governments. At the same time, subsidiarity principle does not restrict public sector institutions' cooperation in working out joint standard solutions.

Information systems should support the existing organizational structures and their objectives, that is why mechanical merging of the information systems of different organizations should be avoided, if possible. Instead, creation of independent information systems, linked through services, should be preferred.

2.1. National information related political decisions SHOULD be enforced only if they are more efficient than the ones made in public sector institutions.
2.2. Instead of centralizing information systems, they SHOULD be mutually linked through services.
2.3. Before a decision is made to merge the systems that support the operation of institutions with different objectives, a risk and profitability analysis MUST be conducted. Corresponding decisions must be harmonized with the institution coordinating state information systems.

2.2. User-centricity

Public sector services are adapted in accordance with the needs of citizens and businesses. The expectations of the users are as follows:

- User-centred services are secure, flexible, personal and they respect invioalability of private life.
- Citizens and enterprises give information to the public sector only once, in order to avoid repeated asking for data.
- Public services are, apart from service providers' channels, also available through information portal eesti.ee. Services that necessitate cooperation of several institutions are

available for a citizen as an integrated whole.

- Access to services is guaranteed through many different channels in any way, at any time and in any place, but within reason, taking into account security, economic feasibility and the size of the target group.

2.4. Institution based approach MUST be replaced with a user based approach. Institutions MUST provide information at their own initiative.
2.5. To make services more comfortable for citizens to use, public sector institutions create a network of portals, the connecting link of which is information portal eesti.ee.
. Evidential value and private information MUST be provided through personalized portals.

2.3. Inclusion and accessibility

IT must create for citizens and businesses equal opportunities with the help of open and inclusive services that are available without restrictions. The aim of inclusion is to use IT possibilities to get over social inequality and exclusion. The aim of availability is to guarantee for the elderly and people with special needs access to services on the same level with other population groups. To increase inclusion and improve availability of services, new service channels are combined with traditional ones. At the same time, opportunities must be guaranteed for authorized third parties, who act on behalf of people who, either temporarily or permanently, cannot use services directly.

2.7. The user SHOULD be able to choose an agreeable duty type of a service: service bureau, post, telephone, e-mail (including the use of @eesti.ee mail address), and other Internet channels.
2.8. A person identified with an ID card MUST be able to apply for any electronic public service.
2.2.9. Citizens MUST have the right and opportunity to participate in making decisions, concerning them and society, through electronic environments.
2.10. Information MUST be available and e-services uasable through most widespread, supported by the private sector or communities, software systems (operation systems, browsers).
2.11. Public sector institutions MUST provide information in open formats. Citizens do not have to make extra expenses to use information (for example, obtain own software).
2.12. People with special needs and the elderly SHOULD be guaranteed access to services on the same level with other population groups.

2.4. Security and privacy

Citizens and businesses, when they communicate with the public sector, MUST be guaranteed reliability of the communication environment and compliance with the regulations of privacy and data protection.

Personal data processing in the private sector MUST be transparent. Private sector must guarantee safe processing of personal data and reliable storage of e-documents. The logs with inquiries into registers containing personal data are preserved. All inquiries made into such registers must be justified.

Citizens have the right to know which data the public sector has collected about him/her. Personal data are collected and used only for purposes and to the extent established in legal acts. Citizens must be guaranteed a right and opportunity to correct inaccurate and misleading data.

2.13. The solutions used in the state information system MUST be secure, in other words, they MUST guarantee confidentiality, authenticity, availability and provability of data and services.
2.14. Citizens MUST be guaranteed services through which can check and, if necessary, correct the data, collected about them by the public sector.
2.2.15. Citizens MUST be guaranteed services, through which they find out who, and for what purposes, has used the data collected about them in the public sector.

2.5. Multilingualism

Developing public pan-European services, the creators of the user interface must carefully consider requirements of multilingualism. Expectations of citizens and businesses that they are served in languages that suit them, must be balanced with the ability of the user interfaces of information systems to provide services in all the EU official and most widely used languages.

With regard to the principle of multilingualism, the present framework, unlike the EU framework, has brought out, first of all, the aspects of Estonian and liguistic neutrality.

2.16. In the user interfaces of information systems created for residents of Estonia, the default language MUST be Estonian.
2.17. The interfaces of information systems MUST comply with WCAG (Web Content Accessibility Guidelines)[14] standards, which guarantees their usability through Estonian language speech synthesisers[15] .
2.18. The user interfaces of pan-European services and relevant information on services SHOULD be provided besides Estonian, also in English, and if necessary, in Russian, or in any other languages relevant for the users. The user interfaces of information systems and content must be usable with the help of translation services (e.g. Google Translate, Yahoo Babelfish) .
2.19. The user interfaces of information systems MUST be easily adaptable to other languages with the help of translation files.

Multilingualism of information systems is not only an issue of user interface, it also cocerns services, metadata of services, documentation, code comments, data structures and data representation. Information system reuse in another language room should be easy.

2.20. The architecture, data structures and software of information systems SHOULD be linguistically neutral: functionality of an information system should ensure its easy realization in another language.
2.21. Information systems SHOULD support multilingual and international semantic assets.

Public sector must also take care of estoniazation of the IT environment of citizens. Estoniazation of commercial software is the duty of the producer of the corresponding product. To ensure estoniazation of free widespread software, public sector should participate in the initiatives of corresponding communities.

2.22. The state supports estoniazation of free widespread software relevant to citizens.
2.23. Information systems and sortware products meant for the public SHOULD contain the support of language technological means of the Estonian language.

2.6. Administrative simplification

Public sector gathers, in their line of duty, a considerable amount of information, which sometimes comes down to the fact that law requires it, not the direct objectives of the institution. Such behaviour raises the cost of the operation of the public sector and causes administrative hindrances. Public Information Act prohibits to use different databases for collecting the same data.

2.24. When the documentation of databases is coordinated in the Management System of state Information System (RIHA), the purposefulness of data collection and compliance with the principle of single request for data are checked.
2.25. Everybody has the right to use public services simply and comfortably. Public services are provided so that service users do not get held up by technical details. Public sector institutions do not burden citizens and businesses with unjustified claims.

[14] http://www.w3.org/TR/WCAG/
[15] In Estonia, apart from Estonian language speech synthesisers (eg. http://meelis.eki.ee/) Finnish language synthesisers are used.

2.7. Transparency

Public sector activities MUST be comprehensible for citizens and businesses. Citizens and businesses are entitled to receive information on the state of affairs concerning them. When a person starts applying for a public service s/he receives an accurate overview of the progress of the service provision and the deadline. S/he can find out easily how far the processing of his/her request is.

Public sector institutions are constantly engaged in monitoring the quality of public services, by including public services' consumers in the assessment process. Information on the quality of services is made public on the website of the institution.

2.26. Every person SHOULD have an easy opportunity to find out how far the processing of his/her request is.
2.27. Public information on the management of affairs of the the public sector is published in the document register of the institution.
2.28. Procedure of requests related to private life SHOULD be sent to a citizen's personal portal or his/her @eesti.ee e-mail address.
2.29. Public sector SHOULD create mechanisms for each service, where a user can express his/her opinion about the quality of the service. Information on the quality of the services is made public.

2.8. Preservation of information

Public sector MUST guarantee readability, reliability and integrity of the digital documents, which were created as part of its activities.

With regard to archiving digital documents, institutions must be guided by the guidelines and requirements of the National Archives.

2.30. Public sector institutions are responsible for archiving digital documents which emerged or were created as part of their activity.
2.31. Each document of the architecture of an information system's interoperability SHOULD describe the rules of archiving digital documents of that system and the mechanisms that guarantee their observance.

2.9. Openness

Openness is the will of persons, organizations and interest groups to share information and encourage discussion with an aim to reach a solution of problems. The framework presupposes that Estonia observes the principles of the Open Government doctrine, according to which citizens have the right of access to public sector documents and procedures in order to create an opportunity for the public to control fulfillment of public duties.

In the context of the framework, openness means that public sector takes into consideration the alternatives of open specifications, standards and software. When developing or ordering software, public sector should use the development methods of free software.

Public sector does not absolutize the principle of openness. In situations where open specifications have not achieved necessary maturity, or closed solutions are more efficient, public sector may use closed solutions. Decisions should be made, proceeding from the idiosyncracies of a particular case.

2.32. Public sector institutions SHOULD follow the principles of openness when developing the architecture of their information systems and procuring software.
2.33. The decision to use closed standards and specifications MUST be justified.

2.10. Reusability

Public sector institutions collect, issue, reproduce and distribute information in order to fulfill their

public duties. Using such information for any other purposese is reusing information,

2.34. Reuse of public sector information SHOULD NOT be restricted. Restrictions SHOULD NOT discriminate anybody or hinder competition.
2.35. Public sector information is meant to be reused by all the market operators and providers of added value.

Apart from information, public sector can reuse the experience of creating other institutions' information systems.

2.36. When creating their own information systems, public sector institutions, if possible, use solutions made by other institutions and their experience.
2.37. When creating free software, public sector institutions use the European Union Public Licence (EUPL) and as a development environment OSOR.eu (Open Source Oservatory and Repository, OSOR).

2.11. Technology neutrality and adaptability

When founding information systems, public sector's focus is on the functionality of the system that is being created. Technological decisions are not a priority and they usually emerge as a result of procurements.

IT solutions related technological decisions must be made transparently, rationally as well as saving state resources and taking into account the existing technological base. At the same time, equal treatment of software resources must be guaranteed as well as observance of competition rules in public procurements.

2.38. When developing functionality of information systems, technological decisions SHOULD be made as late as possible.
2.39. When procuring software, free software alternatives MUST be taken into account.
2.40. In order to guarantee equal treatment of solutions, public sector is RECOMMENDED when it orders functionality, also to order necessary infrastructure changes, needed to realize it.
2.41. Information systems interfaces MUST be created in a technology neutral way, using open standards, prescribed in the interoperability framework (XML, WSDL, SOAP etc.).

2.12. Effectiveness and efficiency

When developing information systems, public sector SHOULD make the most productive and efficient choice, in order to achieve the best solutions for the taxpayers' money.

In choosing the best solution, profitability of investments, costs on changing the infrastructure and organization as well as retraining costs, total cost, increace of flexibility, decrease of administrative hindrances, decrease of risks, transparency, simplification, work environment improvement and other aspects are taken into consideration.

2.42. With regard to procuring development work of the functionality of information systems, public sector MUST take into consideration as much as possible other factors of productivity and efficiency.

3. Service model and service room

3.1. Interoperability architecture of services

Information society is becoming more and more service oriented. Institution and official centred management of public business that used to dominate, is these days oriented more to results, users

and services. The information systems supporting these processes should also become service oriented and follow service oriented architecture (SOA).

The framework handles society as a service centred organization, which means that all the activities of officials, entrepreneurs, citizens and software/information system are viewed as services. End users see services from a joint service room. They are not interested in the organization that provides a service but in the service itself. Although the private and public sector act according to fairly different business rules, the users of their services are the same. Hence, it is practical if the private and public sector develop and manage the service room jointly.

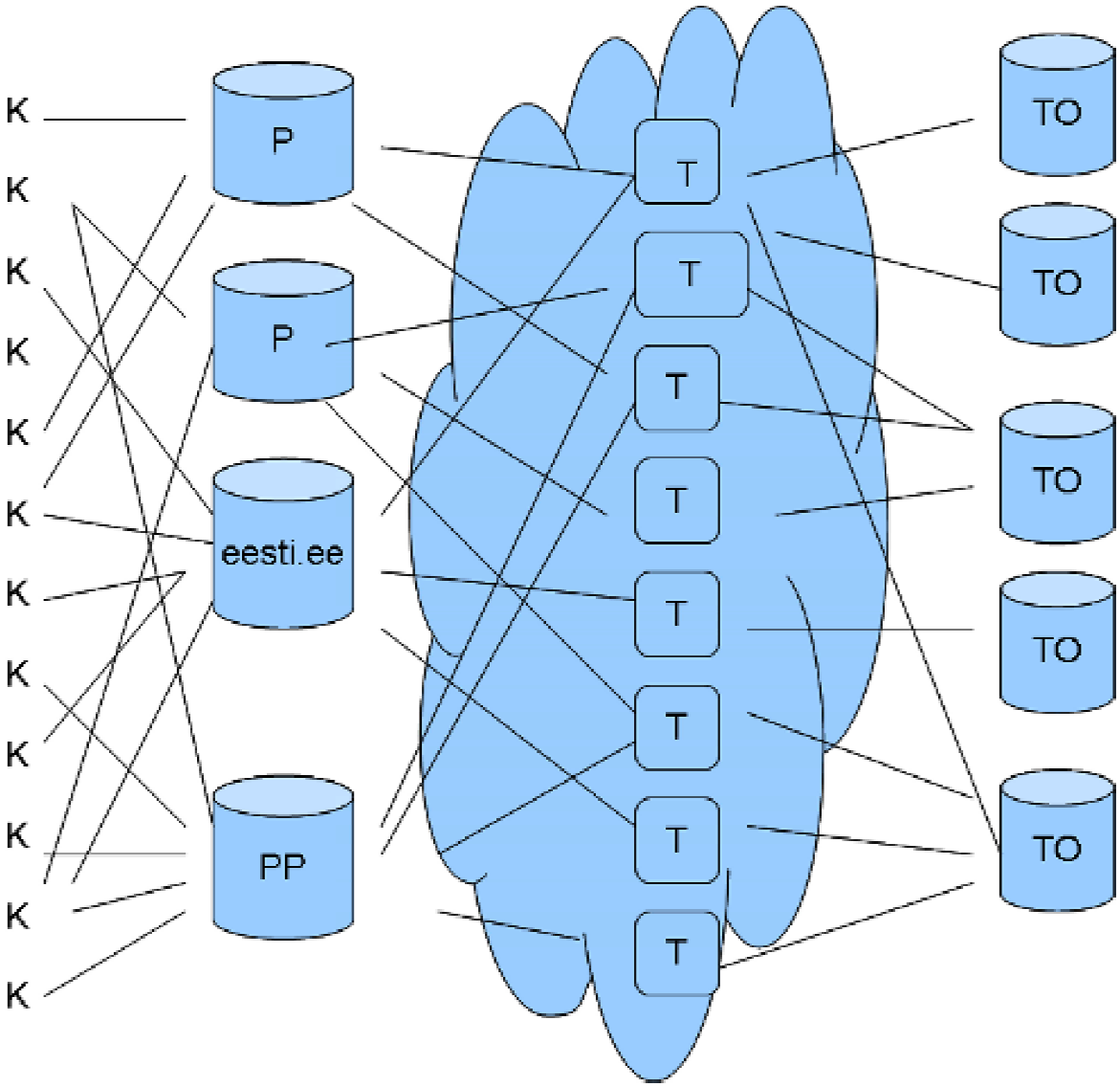


Figure 1. State information system as a service room. Services (S) are registered in the services catalogue (in EISA register). Front end systems and back-end systems are separated. Back-end systems are service providers' (SP) information systems. End users (U) are served by front-end systems, which are portals of institutions (P), information portal eesti.ee and other users' personal portals (PP).

Services are provided for citizens and businesses by state and local government institutions, private enterprises and third sector organizations.

Services are consumed by state and local government institutions, private enterprises, third sector organizations and private persons. Service room enables private persons using public services to represent both themselves and the business.

Everybody can use services either anonymously or personally. In the case of personal services, it is necessary, in general, to guarantee the evidential value of the service, users' authentication and authorization. Personal services are provided through data exchange layer X- Road.

In public sector information systems, front-end and back-end systems are clearly architecturally separated. Back-end systems are all public sector registers and databases. The task of back-end systems is data management and provision of network services, they do not deal with authentication and authorization. Hence, there is no need to build into back-end systems components of end user's authentication and authorization. Network services of back-end systems are made avalable for the end user only through service intermediaries (front-end systems).

Front-end systems are divided into internal (e.g. Intranet) and public systems. Internal front-end systems are responsible for administering their employees rights of access to any service having evidential value in the country. Service using rights are personal and restrictions can be added to them (e.g. time limit with regard to using a service). Front-end systems should not grant rights to employees of other institutions. For rights management, front-end systems may use standard X-Road mini information system portal (MISP), integrate MISP into their front-end system or create their own application on the same principles. Qualified certificates are used for authorization of services with evidential value.

Services of back-end system having evidential value are provided through data exchange layer X-Road. On the occasion of such services, the information systems that intermediate the service (not end users) need to be authorized. Authorization takes place in the security server of such a back-end system. It is only front-end systems with an X-Road certificate that can apply to a back-end system service. In the security server, for each service there is a list of front-end systems that have an intermediary right for that service. A front-end system is added into the list if the front-end system's owner has a legal right to use the service or if a bilateral agreement has been signed. The administrator of the back-end system is responsible for administering the list of organizations using the service. In case of a justified claim, the back-end system's administrator is obligated to grant the applicant the right to use the service immediately.

3.1. Public sector SHOULD be the initiator of developing a joint service room.
3.2. Public sector institutions SHOULD review their activities and make them service centred.
3.3. Information systems of the public and private sector SHOULD follow the rules of service oriented architecture.
3.4. Information systems of service providers of the public and private sector SHOULD be separated from the information systems of service intermediaries (the so-called separation requirement of front-end and back-end systems).
3.5. Information systems SHOULD communicate only through services.
3.6. Public sector and private sector are RECOMMENDED to use a joint service room.
3.7. Public sector SHOULD provide personal services through data exchange layer X-Road.
3.8. To use services with evidential value, the front-end system is authenticated on the basis of an X-Road certificate and with an end user's qualified certificate in the front-end system.
3.9. Services with evidential value are authorized on two levels: the front-end system is authorized by the back-end system and a physical person is authorized by the front-end system.

Systems for general use intermediate services without access restrictions and services whose access rights are either calculable or can be found in the registers according to certain characteristics, for example:

- A person having an Estonian ID code gains access to services, where s/he can see data that the public sector has collected about him/her in registers. S/he can also engage in procedures with regard to himself/herself.
- A signatory of a private sector business (on the basis of the Commercial Register)gains

access to information on that enterprise and engage in procedures with regard to himself/herself.

- General practitioners get access to their services through a public portal if they have been registered in the corresponding register.

Systems for general use contain an authentication component for logging in with a qualified certificate. Systems for general use do not contain components of access management. Information portal eesti.ee intermediates for persons services, provided only in public interests.

When authorizing end users of services with evidential value, the following principles must be kept in mind:

3.10. Back-end systems SHOULD NOT engage in end user's authentication and authorization.
3.11. Network services of back-end systems SHOULD be available for an end user only through front-end systems.
3.3.12. Front-end systems MUST guarantee end user's authorization. For authorization the MISP component of X-Road MAY be used either directly or as integrated into the front-end system.
3.13. Systems for general use MAY intermediate services without access restrictions or services whose access rights are calculable or can be found in registers according to certain characteristics.
3.14. Systems for general use MUST use qualified certificates for authentication (logging in). Systems for general use SHOULD NOT contain components of access management.

3.2. The concept of service, requirements for services

Service[16] in a wider sense is an independent collection of consecutive functionalities of an organization. In a more narrow sense, a service (including an operational service) is a functionality by an organization supporting one or several organizational processes, and which an end user perceives as a whole.

e-Service is a service that is provided either partially or completely with the help of IT and communication technology.

Infrastructure service is a joint technical functionality used for providing one or several services or for information system management.

Public service is a service provided for citizens, institutions, businesses or other organizations by an organization. A public service is characterized by at least one of the following characteristics:

- provision and using of the service is a public interest of society as a whole
- in state and local government institutions, provision of services is regulated by legal acts
- in private businesses and other organizations, provision of services is regulated by legal acts or contracts signed with state and local government institutions.

Public service in an electronic environment must be available for the members of the service's target group in the following way:

- service is provided as close to the user as possible
- the user is able to use the service with minimum previous training
- as little information as possible is asked from the user
- for each user security of using is guaranteed.

Aggregate service or complex service is combined from reliable basic services. The user perceives a complex service as one service. If the complex service is provided by the service intermediary, the intermediary must have the right to use the basic services. If provision of complex services differs technologically from provision of a basic service, it is handled in RIHA as being equal with any other service. If the basic services of the public sector are mostly provided by the public sector itself, then complex services are rather provided by the private sector.

[16] Service is defined differently in different contexts. Here, the definition of the European Interoperability Architecture Task Force has been used.

In the case of aggregate service, it is possible to create X-Road complex enquiries. In the case of these enquiries, due to the complicated structure of aggregate services, there is a danger of accessing data, to which there was no access initially. It is also possible to combine public data from different databases, whose compilation may profile users. In the case of aggregate services, special attention must be paid to security related risks that are linked with service using rights as well as to the danger of combining data.

Authentication (identification) is a procedure during which the person and/or the information system that has applied for using the service, is identified.

Information system is authenticated (on X-Road) on the basis of a security server certificate granted by the data exchange layer of the state information systems.

End user's authentication is the responsibility of the service intermediary. End users are authenticated with a qualified certificate (ID card, mobile ID, etc.). Programmes using the services of the authenticated information system are authenticated additionally when they are launched, on the basis of the certificate of the person responsible for the programme. Citizens and entrepreneurs who use services through information portal eesti.ee are authenticated with an ID card or through online banks.

User authentication is a procedure, during which the rights to use a service are determined and granted to the authenticated user.

Persons using services through user information system are authorized by the institution managing that system. Users can be authorized through some other register (e.g. register of GP-s) or according to certain rules. This way, the users of a personal portal, on the basis of an ID code, receive the right of use for the services aimed at them.

Basic service (also, interlinking service) is the procedure of one organization, which is a necessary part for the operation of another organization, but which when considered separately within the organization, may not have an independent meaning. Basic service is used by information systems (programmes). The basic service may not be an independent service of the organization providing it, but it can be:

- part of the public service provided by another organization or
- part of the internal work process of another sub-organization.

Reusing. Public sector institutions collect, issue, reproduce and distribute documents to fulfill their public duties. Using these documents for other purposes is reusing.

Back-end systems authorize front-end systems on the basis of the front-end system certificate. User groups of front-end systems should register in RIHA. Responsibility for authorizing the front-end system or their user group lies on the service provider.

3.15. Public services MUST be provided free of charge. The only exceptions are the fees established by the State Fees Act.
3.16. Public sector SHOULD guarantee the private and third sector the reuse of their basic services and enable them with the help of basic services to combine new services with surplus value.
3.17. Whether information can be reused is decided by a competent institution according to the principle of subsidiarity.
3.18. If information reuse is permitted, public sector institutions SHOULD guarantee information reuse through network services for both business and non-business purposes.
3.19. In the case of aggregate services, special attention SHOULD be paid to the problems accompaning component services rights and the danger of violation of privacy, caused as a result of combining data.

Aggregating of services. Service provider, with the permission of a citizen, may use the data collected in the public sector information systems about him or her. Alongside the development of public services, people's feeling of safety must not suffer, protection of their principal rights, personal data and identity must be guaranteed, as well as reduction of unacceptable risks in IT

systems supporting a public service.

3.20. Service provider MAY, with the permission of a citizen, use the data collected about him or her in an aggregate service into public sector information systems.

3.3. Service levels

In the interoperability framework, organizations are considered service providers, no matter to what extent they can use for that purpose means of IT. The European interoperability framework distinguishes between five service levels: information service, web service, web form, full electronic service and personalized full electronic service.

Information service. The user can read online information about the service and download it into his or her computer. For citizens and entrepreneurs, the means of offering such a service are information portal eesti.ee, institutional web pages or other user information systems.

.

Web form. Forms can be downloaded and the service user can take the filled in forms personally to an institution or send them by ordinary mail, fax or e-mail. Citizens' and entrepreneurs' forms MUST be in open formats downloadable from institutional web sites.

Web service. Web service is similar to web form but a user can fill in a form online and send it straight from a web page. The user gets confirmation of the saving of the form in the information system of the institution. When creating web forms it is advisable to use standard X-Forms.

Full electronic service. The service is applied for and provided online. Full electronic service does not require any extra paperwork from the user.

Personalized full electronic service. Full electronic service, in the course of which the data on the user are checked in various registers and part of the data in forms is pre-filled.

EU countries have agreed on 20 electronic services that need preferential developing, out of which 12 are life arc services and 8 entrepreneural services.

Life arc services are as follows:

- income tax: declaration, notification of taxation
- jobseeking services through job centres
- social benefits: unemployment benefit, child benefit, medical expenses (compensation or direct payment), student benefit
- identity documents (passport and driver's licence)
- vehicle registration (new, second hand and imported second hand cars)
- applying for planning permission
- reporting to the police (e.g. in case of theft)
- public libraries (access to catalogues, retrieval means)
- certificates (birth, marriage): inquiry and reply
- entering into college/university
- notification of change of residence (change of address)
- health services (e.g. interactive counselling).

Entrepreneural services are as follows:

- social support of employees
- corporation tax: declaration, notification
- VAT: declaration, notification
- registration of a new organization

- submission of data to agencies dealing with statistics
- customs declarations
- environmental permits (reporting added)
- public procurements.

3.4. RIHA as a catalogue of services

Information on services provided in public interests is published, apart from the service intermediary's portal, also in information portal eesti.ee. In the case of interoperable systems, publication of service intermediaries' information in the portal eesti.ee should be automatic. In addition, network services are registered in the register of the Management System of State Information Systems RIHA. The description of each service in RIHA contains:

- the syntax of the use of the service (for example, in the case of X-Road services it is described in the Web Service Description language , WSDL, file);
- the policy of providing a service (on what grounds, to whom and why the service is provided);
- quality indicators of the service (service functionality, operating reliability and efficiency).

Description of the service in RIHA is the task of a service provider. Description of quality indicators is necessary for assessing and ensuring the quality of a service. Quality indicators characterize functionality, operation reliability and efficiency of a service.

Functionality indicators describe the semantics of a service's input and output parameters and the preconditions and consequences of using a service.

Indicators of operating reliability and efficiency describe hindrance resistance, frequency allowed for hindrancies, integrity, utility load calculated for a service and resource use, for example, the time spent on providing the service. Service availability, confidentiality and integrity are submitted in a generalized way as a security class of a service.

Service provider is obligated to ensure quality of a service, in other words, constantly engage in procedures necessary for a service to comply with established requirements. Service user is entitled to demand from a service provider a service that meets quality requirements.

3.21. Information on services provided in public interests MUST besides service intermediaries' portals, also be published in information portal eesti.ee, network services MUST be described in RIHA.
3.22. Service provider MUST ensure functionality, operating reliability and efficiency of the service, according to the description of the service in RIHA.

3.5. Estonian and European Union conceptual model of services

The Estonian conceptual model of services was designed in 1998-2001 and realized in 2001 as a data exchange layer X-Road of information systems. X-road is a technical and organizational environment that enables organizing secure Internet oriented data exchange between digitally maintained state databases, enables conduction of secure data exchange between institutions/persons as well as organization of persons' access to the data stored and processed in state databases.

X-Road is a securing system of the state information system, using of which is compulsory in accordance with the Public Information Act[17] and the Government of the Republic's Resolution

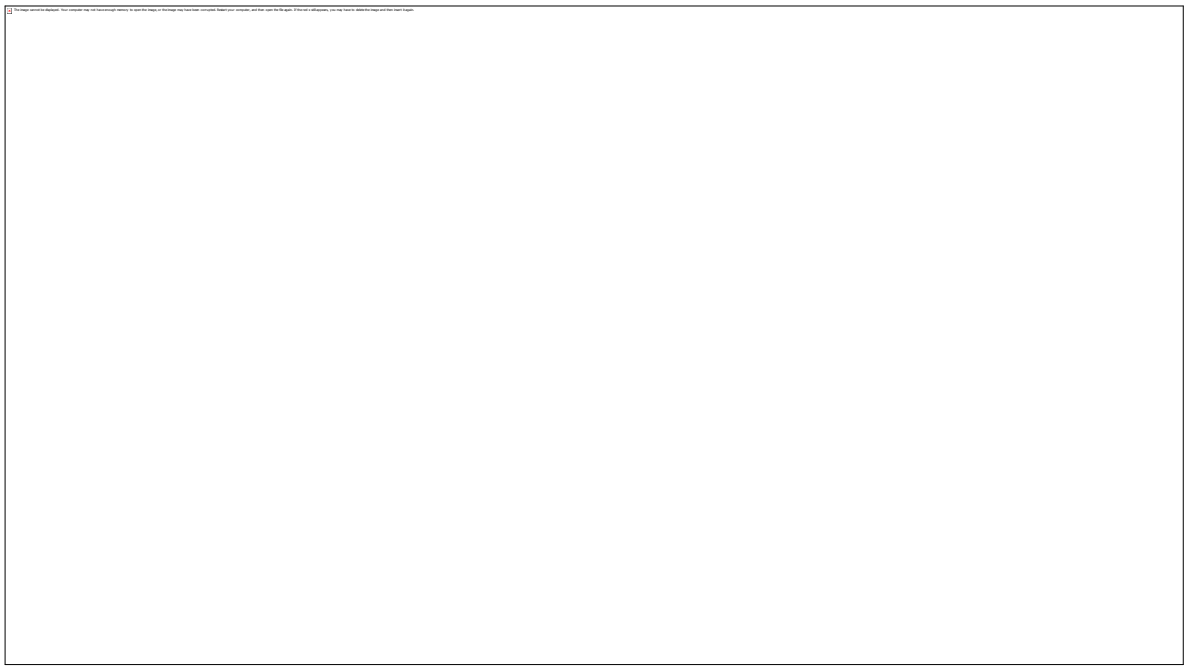
[17] https://www.riigiteataja.ee/ert/act.jsp?id=13256729

"Data Exchange Layer of Information Systems"[18] .

X-Road ensures that dispered information systems are loosely coupled through the use of uniform agreed XML schemes and protocols at data exchange19 . Secure services are realized as WSDL services. Using uniform schemes is obligatory in providing services as well as in mutual communication of document management systems through document exchange environment DVK20 .

3.23. The Estonian model of services is data exchange layer X-Road, which can be viewed as a realization of the European model of services. X-Road MUST be used in the case of services needing an evidential value.
3.24. With regard to coupling information systems, their rigid integration MUST be avoided. Information systems MUST be coupled as loosely as possible through joint agreed X-Road and DVK agreed XML schemes and protocols.

In designing the conceptual model of the European interoperability framework[21], the X-Road experience was also taken into account. That is why the Estonian model completely coincides with the EU conceptual model of services, whose main elements are provided in Figure 2. Data exchange layer X-Road can be viewed as a realization of the European model in one of the member states.



[18] https://www.riigiteataja.ee/ert/act.jsp?replstring=33&dyn=13256729&id=12956835
[19]http://www.ria.ee/x-tee
[20]http://www.ria.ee/dokumendivahetus
[21] Source: Research and Consultation Company Gartner report „Preparation for Update European Interoperability Framework 2.0 – Final Report", http://ec.europa.eu/idabc/servlets/Doc3665.pdf?id=31505.

Figure 2. European conceptual model of services

4. Interoperability dimensions

Like the interoperability framework of the European Union, so does the Estonian framework divide interoperability into five dimensions: political, legal, organizational, semantic and technical. The same approach COULD be used with regard to the information system of the whole country or any public sector institution and its information system. Interoperability dimensions can be defined as follows.

- **Political context.** In the political context dimension, the general context of an organization/information system is described, links with the surroundings, common visions, priorities and objectives. Political context contains, in a generalized form, also the remaining four dimensions.
- **Legal interoperability.** In the legal interoperability dimension, an overview is provided on the legal system regulating the organization/information system, legal view on services, data, information systems and security.
- **Organizational interoperability** is an ability of organizations to provide services for one another and their customers with the help of information systems. Documentation of the organizational dimension contains descriptions of operational processes, guidelines and rules defining the processes, service level agreements and descriptions of the procedure of management of changes.
- **Semantic interoperability** is an ability of organizations to understand the meaning of exchange information (data) in the same way. In the corresponding documentation, the semantic assets and the rules of semantic enrichment of data are described.
- **Technical interoperability** is an interoperability of technical and software infrastructure. The documentation of this dimension provides general architecture, summary of guidelines and standards as well as specifications of user interfaces, data submission and exchange.

With regard to founding information systems, it is relevant to analyse all the interoperability dimensions and document them in the document of interoperability architecture of the system. The information systems belonging to the state information system should submit the document of interoperability architecture of the information system through RIHA to an institution coordinating state information systems and to other institutions as stipulated in the Public Information Act.

4.1. The most important document of each information system of the public sector is the description of its interoperability architecture, where the technical architecture of the information system, semantics, legal system and political context are provided. Without such a document, no coordination and registration procedure of the information system is started in RIHA.

4.1. Political context

4.1.1. The political context of the interoperability framework of the state information system

The interoperability framework of the state information system is one of the information related political documents of the country. The framework is affected by several domestic and European initiatives:

- Action programmes of the Government of the Republic. Although the framework itself is not a political document, the decisions of government's action programmes that handle information society, affect the strategic principles of the framework
- Estonian Information Society Development Plan[22]
- Annual application plans of the Estonian Information Society Development Plan
- eGovernment Charter[23]
- European Union Interoperability Framework
- Initiatives of the EU interoperability programme (Interoperability Solutions for European Public Administrations, ISA) [24]
- Initiatives of the European Union information society and eGovernment[25]
- Digital Agenda for Europe[26]
- Principles of open government[27]
- The activities and initiatives of International Council for Information Technology in Government Administration (ICA) [28]
- The principles and guidelines of the Organization of Economic Coooperation and Development (OECD) [29]

4.2. The political context of the framework of interoperability of the state information system is made up by information society and ICT related decisions, development plans and application plans, but also agreements that that have emerged in the course of international cooperation.
4.3. The basis of the Estonian interoperability framework is the European interoperability framework.
4. The interoperability framework of the state information system imposes requirements on state information systems and is a metaframework for the documents of interoperability architecture of the public sector information systems.

4.1.2. Political context of public sector information systems

Each information system has its context. Creation of new services and information systems supporting them, or their rearrangement, in general, comes from activities on political level . Political will is usually expressed in legal acts, coalition programmes, development plans, application plans and other documents where it is expressed. If there is no clear political decision and legal basis for creating an information system/service, it has to be created beforehand.

It is relevant to analyse the context when drawing up each document of the architecture of interoperability of an information system. Information systems should support the objectives of organizations. Although from some angle, it may seem logical to merge, for example, the supporting information systems of the Government and Riigikogu, or integrate the information system of the Chancellor of Justice with that of the Ministry of Justice, it is questionable from the political point of view. It is not clear, the objectives of which organization the merged system must prefer. Although, by integrating information systems of administrative areas of ministries, at first glance, it is possible to economize up to 20%, such a decision may incur considerable extra expenses, if an agency of one ministry is transferred to the administrative area of another ministry. In that case, the information system of the tranferable agency must be removed from one information system and create a new infrastructure supporting the work of a new agency. But more important than avoiding economic loss, is to avoid dangers that come from violating the foundation of European democracy – the principle of subsidiarity.

[22] https://valitsus.ee/UserFiles/valitsus/et/valitsus/arengukavad/majandus-ja-kommunikatsiooniministeerium/T_iendatud_info_hiskonna_arengukava.pdf
[23] http://www.riigikontroll.ee/LinkClick.aspx?fileticket=n9QQmXYiTmA%3d
[24] http://ec.europa.eu/isa/
[25] http://ec.europa.eu/information_society/, http://ec.europa.eu/information_society/activities/egovernment/
[26] http://ec.europa.eu/information_society/digital-agenda/
[27] http://en.wikipedia.org/wiki/Open_government
[28] http://www.ica-it.org/
[29] http://www.oecd.org/

When changing the functionality of an organization and creating and developing its information system, it is necessary to have a clear perception of the connections between the organization and its operational processes and other organizations. Without a clear concept, no information system should be founded or changed.

Public sector has a number of single-type activities (e.g. accounting, personnel records), where the experience of one institution could be reused in another one. Centralization of such activities and creation of central national solutions would hinder competition. Ordering such services from the private sector, would bring about their partial centralization in the private sector, but at the same time, healthy competition between bidders of the private sector will be preserved as well as a choice of alternatives for the public sector.

4.5. Information systems and public services MUST be created proceeding from a real need, and they have to be endorsed with political decisions. For creation of a service and information system, there MUST be a legal base.
4.6. The attitude towards merging the information systems of institutions with different objectives SHOULD be careful. The owner of the system, when creating an information system and conducting a risk and profitability analysis must consider the opportunities of both the centralized and dispersed information system. The rationality of merging the information systems MUST be justified in the document of interoperability architecture of the information system.
4.7. The document of interoperability architecture of the information system MUST describe how the organization, its processes, information systems and services are connected with the sorroundings.
4.8. Public sector single-type activities are RECOMMENDED to be reused.
4.9. Public sector single-type activities are RECOMMENDED to be ordered as a service from the private sector.
4.10. In the public sector, monopolization of the solutions of single-type activities SHOULD be avoided.

4.2. Legal interoperability

Legal interoperability is a characteristic of legislation which guarantees preservation of appropriateness of legal meaning of data. Legal interoperability is ensured by linking the legal acts regulating the operational processes.

Each document of interoperability architecture of an information system should contain a part handling legal interoperability. When a new information system is created, for the coordination of information systems, the bills of additional legal acts and those that are changed must be submitted, in order to implement the information system.

The present division handles legal interoperability from the national aspect. Below, there is a list of general legal acts that regulate digital information. When preparing legal acts of administrative areas of ministries and local governments, the legal acts listed in paragraph 4.2.1 must be followed.

According to the principle of subsidiarity, each organization is responsible for designing and amending legal acts regulating its administrative area. Legal acts containing aspects of ICT are examined by an institution coordinating state information systems, following the coordination rules, described in division 4.2.2.

4.11. A document of interoperability architecture of a public sector information system MUST contain a part, handling legal interoperability.

4.2.1. General legal acts regulating the state information system

State information system is coordinated with legal acts, first of all, in the organizational dimension. In the semantic and technical dimension, interoperability is regulated with various agreements, standards or recommendations.

In a broader sense, the whole country can be handled as an information system. All the legal acts in

force in the country, extend to such an information system. In the present division, there is a list of legal acts that directly regulate digital information.

Public Information Act.[30] The act ensures that the public and everybody has access to the information meant for general use, and creates for the public control mechanisms over fulfillment of public duties.

Government of the Republic Resolution on the Management System of the State Information System.[31] The objective of the management system of the state information system is to ensure transparency of the management of the state information system, to plan state information management and to support the interoperability of databases of the state, local governments and private persons fulfilling public duties.

Government of the Republic Resolution on the System of Security Measures of the Information System.[32] The objective of the system of security measures of the information system is to establish security measures with regard to information systems and related information assets, which are used for processing sets of data, found in state and local government databases.

Digital Signatures Act.[33] The act stipulates the terms of the use of a digital signature and surveillance procedure over certification and time stamp services.

Spatial Data Act.[34] The act stipulates requirements with regard to spatial databases and services, for making them available and distributing them, it also stipulates management of geodetic and address details systems as well as the conditions of the seizure and release of topographic data, the procedure of developing spatial data infrastructure and organization of reporting, state surveillance over the appointment of location-addresses and responsibility for violating the requirements of the geodetic mark protection .

Electronic Communications Act.[35] The aim of the act is to create necessary conditions for the development of electronic communications. The act stipulates requirements for public electronic communications networks and services, radio communications, management of radio frequencies and numeration, equipment and surveillance over fulfillment of those requirements and responsibility for violating those requirements.

Archives Act.[36] The act stipulates collection, assessment, preservation and organizing access to archival documents and the foundations of the operation of archives.

State Secrets And Classified Information Of Foreign States Act.[37] The purpose of this act is to ensure the security and foreign relations of the Republic of Estonia, protecting state secrets and classified information of foreign states from disclosure and becoming accessible to persons who have not been granted access to such information.

Official Statistics Act.[38] The act stipulates legal foundations for organizing systematic and purposeful official statistical observations.

Personal Data Protection Act.[39] The act stipulates a person's fundamental rights and freedoms in line with public interests, when his or her personal data are processed.

Public Procurement Act[40] The act stipulates the procedure of public procurements, the rights and obligations of subjects who participate in public procurements as well as violations of the act, also

[30] https://www.riigiteataja.ee/akt/122032011009
[31] https://www.riigiteataja.ee/akt/13147268
[32] https://www.riigiteataja.ee/akt/13125331
[33] https://www.riigiteataja.ee/akt/13314840
[34] https://www.riigiteataja.ee/akt/128022011002
[35] https://www.riigiteataja.ee/akt/123032011011
[36] https://www.riigiteataja.ee/akt/13314609
[37] https://www.riigiteataja.ee/akt/108072011049
[38] https://www.riigiteataja.ee/akt/13338093
[39] https://www.riigiteataja.ee/akt/130122010011
[40] https://www.riigiteataja.ee/akt/106012011020

the procedure of state surveillance with an aim of promoting competition and ensuring transparency of public procurements and equal treatment of the participants in the bidding procedure.

Government of the Republic Resolution on the Data Exchange Layer of Information Systems.[41] The resolution sets requirements for the data exchange layer of information systems, its use and management.

Government of the Republic Resolution on the System of Classificators.[42] The resolution establishes a system of classificators (classifications), its composition and the procedure of management of classificators.

Government of the Republic Resolution on the System of Address Details.[43] The resolution establishes a system of address details, including appointment and submission of location-addresses, processing of address details and uniform principles of the provision of address services.

Resolution of the Minister of the Environment on Geodetic System.[44] The resolution establishes the geodetic system, its composition and application procedure.

4.2.2. Coordination of legal acts from IT aspect

The precondition of coordination of legal acts linked with information systems/databases for an institution coordinating a state information system, is coordination of their documentation in RIHA. Coordination of legal acts containing ICT aspects in an institution coordinating state information systems, takes place according to the following rules:

- all information systems related legal acts are examined by the Department of State Information Systems of the Ministry of Economic Affairs and Communications
- Department of State Information Systems of the Ministry of Economic Affairs and Communications checks, in addition to the text of the bill, the documentation submitted to RIHA from an information system/database, and on the basis of it draws up a coordination of the ministry
- a legal act linked with an information system not registered in RIHA is not coordinated by the Department of State Information Systems.

4.3. Organizational interoperability

In the context of state information system, by organizational interoperability we mean the ability of all organizations to provide a service through information systems to each other and to the public. In other words, it is the ability of organizations to act together proceeding from a common integral view and on behalf of a common agreed objective. A document of interoperability architecture of the information systems of the public sector must contain a part, handling organizational interoperability. It must cover at least the following aspects:

- a list of operational processes with their short descriptions, their mutual interoperability and interoperability with external operational processes
- principles of management of the life cycle of services
- description of the principles of management of changes of an information system.

4.12. An information system architecture document MUST contain:
- a list of operational processes of an organization;
- short decriptions of the principles of the management of services and changes;
- description of the mutual interoperability of operational processes and interoperability with external operational processes.

[41] https://www.riigiteataja.ee/akt/119012011015
[42] https://www.riigiteataja.ee/akt/12910889
[43] https://www.riigiteataja.ee/akt/12901083
[44] https://www.riigiteataja.ee/akt/12987975

4.3.1. Organizations

In developing and managing the state information system and providing public services, the organizations are divided as follows:

- level of coordination, management and financing (political level):
  - Ministry of Economic Affairs and Communications
  - ministries
- level of organization/realization /management :
  - IT departments of ministries
  - IT units of subsidiaries
  - cross-departmental competence centres: Estonian Information System's Authority, Estonian Land Board, Statistical Office
  - sphere specific competence centres: Centre of Registers and Information Systems, IT and Development Centre of the Ministry of the Interior, The National Examinations and Qualifications Centre, Estonian Tax and Customs Board, Estonian Agricultural Registers and Information Board, Estonian e-Health Foundation, State Infocommunication Foundation
  - private developers
  - private service providers for citizens and state institutions
  - non-profit organizations
- surveillance level:
  - Data Protection Inspectorate
  - Technical Surveillance Authority
  - Consumer Protection Board
  - Estonian Competition Authority
  - National Audit Office
  - Ministry of Economic Affairs and Communications
  - Estonian Information System's Authority

4.3.2. Responsibility

When developing and providing a public service:

- it is always the need and/or the opportunity to increase the value provided with the service, and/or to improve the quality of the service, that has to be kept in mind
- maximum use of ICT opportunities is made
- the necessity of changing the process of a service provision and legislature is always considered, proceeding from the technological solution that is to be employed
- a public service expenditure analysis for the whole life cycle of the service is drawn up, and when deciding on a development, the effect that the service that is being developed has on the state and/or local government budget, is taken into consideration
- the division of roles and responsibility between the public, third and private sector is weighed, and if necessary, corresponding legal acts are amended or updated.

When appointing the provider of a public service, the ratio of the value coming from providing the service and the expenses it incurs from the public or local government budget is considered. It is the chief executive officer (CEO) that is responsible for the development and management of a public service, according to the service level agreement. The expenses needed during the life cycle of a service are planned by the chief financial officer of an organization (CFO).

4.13. Public sector institutions MUST consider practicality of developing a public service and examine agreements of providing a public service.

Each institution has an information system that supports its fulfillment of duties. With regard to developing and managing the information system and providing public services, a governmental institution is guided by the duties imposed on it by law. If it is in line with law, a public service can

also be provided by a private organization.

With regard to developing IT solutions supporting public services, service oriented architecture is followed, as well as reuse opportunities of data, already created information systems and the services provided by the information systems. The chief information officer (CIO) is responsible for developing and managing an institution's information system as a whole. It is also chief information officer's responsibility to make sure that the architecture of the information systems in the organization conforms to the architecture of information systems enforced in the country, and that it is in line with the requirements of the interoperability framework. All the IT projects of an institution must be approved by CIO. Projects of information systems pivotal for the country and projects whose cost exceeds 200 000 euros, are examined by the chief architect of the state IT, whose duties are fulfilled by the Department of State Information Systems of the Ministry of Economic Affairs and Communications.

4.14. Projects of information systems pivotal for the country and projects whose cost exceeds 200 000 euros, are examined by the chief architect of the state IT. The duties of the chief architect of the state IT are fulfilled by the Department of State Information Systems of the Ministry of Economic Affairs and Communications.
4.15. Each institution MUST determine the role and duties of its chief information officer and appoint a person to fulfill them.
4.16. Each institution MUST determine the role and duties of its chief information security officer and appoint a person to fulfill them.

4.3.3. Cooperation and division of labour

When developing public services, governmental institutions word the aim of the development underestandably for the public and organize the best possible design for a technological solution. Governmental institutions SHOULD, first of all, deal with ordering technological solutions, not designing them. Governmental institutions prepare propositions for legal acts to be amended and enforce approved legal acts or their amendments. The principles of the division of labour are as follows.

4.17. In the case of new initiatives, public sector institutions MUST put the interests of the state and its population above the interests of the organization.
4.18, All interinstitutional links operate on the basis of multilateral agreements, bilateral agreements, if possible, are avoided. Service level agreements (SLA) must be published in RIHA.
4.19. Private sector institutions and non-governmental organizations are the owners of the information and data created or collected by them. The owner of the data of the state information system is the state. The structure and content of the data is the responsibility of a particular data administering organization, as a responsible and/or authorized processor.
4.20. With regard to data exchange, restrictions imposed by law and opportunities of organizations are followed.

The principles of the division of labour are as follows.

- The main principle: In the case of new initiatives, public sector institutions must put the interests of the state and its population above the interests of the organization.
- All interinstitutional links operate on the basis of multilateral agreements, bilateral agreements, if possible, are avoided.
- Private sector institutions and non-governmental organizations are the owners of the information and data created or collected by them. The owner of the data of the state information system is the state. The structure and content of the data is the responsibility of a particular data administering organization, as a responsible and/or authorized processor.
- With regard to data exchange, restrictions imposed by law and opportunities of organizations are followed.

4.3.4. Coordination

Estonia follows the principles of dispersed development in developing the state information system. The precondition of dispersed development is **a method of open coordination.** According to that method, a minimum number of rules is agreed upon, following of which ensures technical and semantic interoperability of information systems. The coordinator of the development and management of the state information system is the Department of State Information Systems of the Ministry of Economic Affairs and Communications.

4.3.5. Strategic planning

Strategic planning is based on the following documents and opportunities:

- The Programme of the Government of the Republic
- The state IT budget[45]
- Estonian Information Society Development Plan and Application Plan
- Support of structural funds[46]
- Development plans of ministries and their areas of government
- Cyber Security Strategy and Application Plan.

4.3.6. Council of Computer Science

Estonian Council of Computer Science has been launched to ensure horizontal coordination between the public, private and the third sector. The council advises the government on the issues of information society development and its chairperson is the minister responsible for coordinating the state information systems i.e. the Minister of Economic Affairs and Communications. The duties of the Council of Computer Science are as follows:

- working out suggestions on how to draw up general foundations and strategy of the development of Estonian IT
- examination of bills of legal acts regulating computer science and IT and expressing opinion about them
- advising the Government of the Republic on the issues of implementing computer science related development plans
- examination of development plans of the state information systems.

4.3.7. Coordination of information systems of local governments

When local governments build up their information systems, they are guided by the principle of subsidiarity and follow the valid legislature that regulates IT in the country. The state IT interoperability framework as an agreement also extends to local governments. Local governments coordinate their activities through the associations of local governments.

Local governments produce the content of national information systems and use their services through data exchange layer X-Road.

In the case of single-type services, local governments could consider joint ordering reusable development work and management of corresponding systems from the private sector, including, if necessary, the Ministry of the Interior.

With regard to decision services, for the provision of which, a citizen's interference is needed, it is practical for local governments to develop them independently, using, if necessary, the state portal

[45] IT budget is drawn up on the basis of that of the previous year, corrections are made according to the changed situation or predicted changes. Ministries collect the applications of their subsidiary units, examine the sums and reasonings at the in-house debate, and send the combined budgets to the Ministry of Finance for coordination.

[46] It is possible to apply for support from structural funds to launch and implement projects that develop information society. For that, it is necessary to follow a fixed procedure, responsible for which are the Department of State Information Systems of the Ministry of Economic Affairs and Communications and Estonian Information System's Authority.

eesti.ee, managed by Estonian Information System's Authority.

4.4. Semantic interoperability

Semantic interoperability is the ability of different organizations to understand the meaning of information similarly. What makes semantic interoperability complicated is the fact that the ways software systems are used, the aims and contexts are different, and that is why data submission, encoding and nuances of meaning are also different.

The assets of semantic interoperability are reusable metadata (XML schemes, data models etc.) and comparative data (classificators, taxonomies etc.). Ensuring semantic interoperability of two information systems presupposes the existence of their mutual semantic gateway. The semantic gateway should ensure semantic conversions, as a result of which the information systems could use each other's data adequately. Semantic interoperability framework is a collection of multilateral agreements and rules, which simplifies mutual linking of the systems in the semantic dimension.

Metadata level is the initial level for achieving semantic interoperability. To achieve interoperability on the level of syntax, the precondition is creation of repositories of XML schemes.

The following types of semantic interoperability assets exist: metadata, dictionaries, thesauruses, classificators, taxonomies, conversion tables, ontologies and service registers. Below are the short descriptions of these asset types.

Metadata. Metadata level is the initial level for achieving semantic interoperability. To achieve interoperability on the level of syntax, the precondition is creation of repositories of XML schemes.

Dictionary. A traditiomal dictionary is a list of notions and explanations. Creation of terminology is built on the documents used in the corresponding domain, and the terms, notions and their meanings specified there.
Thesaurus. Thesauruses are compiled on the basis of content links, not alphabetically. Hierarchy and subbordination between notions is characterictic of thesauruses. A thesaurus can contain as units, not only words and expressions of a natural language, but also agreed abstract descriptors, especially on higher, more abstract levels of an organization. When thesauruses are compiled ISO 2788-1986 standard is followed.

Classificator. Classificators have a similar task with thesauruses, but instead of notions, they use class names. A classificator is a mark-up guideline that classifies objects of one type according to a certain characteristic or a number of characteristics and identifies them univalently. By structure, classificators can be divided into hierarchic and linear ones.

Taxonomy. Taxonomies are treelike structures for categorizing objects. Hence, classificators can be viewed as a special case of taxonomies. The main difference between taxonomies and classificators lies in the fact that taxonomies have a higher level of abstractness.

Conversion table. The main aim of conversion tables is to describe both conformities of different classificators and transitions of different versions of classificators. Such transitions are necessary for ensuring interoperability on technical, organizational as well as semantic level.

Ontology. Philosophy handles ontology as a teaching on existence, but in information technology this concept has a more concrete meaning. In a broader sense, ontology is a collection of concepts together with all the links. In that sense, thesauruses, taxonomies and classificators are all special cases of ontology. In a more narrow sense, ontology of a certain domain is a system of concepts of that domain.

Specialized dictionary or ontology. Specialized dictionaries are created by specialized expert groups, whereas the existing terminology is used to describe concepts.

Service register. Service register is an environment which facilitates description and discovery of existing services. If it is a human-readable register, it can exist, for example, as a simple web site. A machine-readable service register enables the information system itself look for particular services, and through it increase its dynamics. In the context of the list of the state information systems, it is first of all the Web Service Description Language (WSDL) and the decriptions of services related to its documents, as well as the registers of the Universal Description, Discovery and Integration (UDDI)that have been kept in mind.

A detailed description of semantic interoperability has been provided in a separate document of the interoperability framework "Semantic Interoperability Framework". Below, the principles of semantic interoperability in the public sector have been provided.

4.21. Each document of interoperability architecture of an information system SHOULD contain a part dealing with semantic interoperability.
4.22. Each owner of an information asset publishes in RIHA the semantic descriptions of its information asset. The owner of an information asset is free to decide on the internal architecture of its information system as well as the principles of interoperability, but with regard to interlinking the information systems, it is compulsory to follow the principles of the framework.
4.23 The parties are free to choose which tools and standards they use when creating semantic assets and enriching information assets semantically. Semantic assets and annotated information assets MUST be published in RIHA according to the requirements of the semantic guideline.
4.24. Human-readable and machine-readable semantic assets of the state information system and annotated information assets are available for everybody free of charge, including representatives of the public and private sector and residents of the European Union.
4.25.The framework RECCOMENDS private businesses and their associations to participate in creation, publication and implementation of semantic assets.

4.5. Technical interoperability

When IT architecture of administrative agencies is designed, it is guided by the principles of service oriented architecture.

In the case of service oriented architecture, different systems provide information services through the so-called service interfaces, which other information systems can use. Descriptions of the interfaces must contain enough information to identify the service and to use it so that the system which uses the service need not know anything about the internal architecture, platform, etc of the service providing system.

In the case of service oriented architecture, the service intermediary and the actual service provider may not be one and the same person, and from the user's point of view it makes no difference.

Interoperability framework establishes the following objectives for the IT architecture of information systems.

- **Maintenance of data in one location.** Data are maintained only in such a database, where they are the main data. Pursuant to the requirements of availability, there may be a need to copy the main data, but in that case it has to be taken into account that the copy may have expired.

- **Linking business processes through main services.** Information systems communicate with one another with the help of main services. If an institution needs data from another institution for a business process or conduct workflow in another institution, main services are used for that. Institutions must take care of it that their data and services would be usable as main services. For example, situations in which one institution prints out a document and sends it by post to another institution, where it is typed into computer, should be ruled out.

- **Ensuring availability of main services.** If the service consumer's requirements for the

availability of the service are higher than the service provider's, it is the service provider that should raise the availability of the service . If it is not possible, other options may be considered, taking into consideration also legal aspects.

- **Avoiding single points of failure (SPOF) that paralyse the whole system.** Solutions when a single point of failure paralyses the whole system should be avoided.
- **Security.** Solutions used in the state information system must be secure, it means they must ensure confidentiality, authenticity, availability and provability of information.
- **Openness.** When choosing IT solutions, solutions based on open standards must be preferred.
- **Person's right to get acquainted with data about him/her.** Every person has a right to get acquainted with the data collected into information systems about him/her and also get information about inquiries made about him/her, if this right has not been restricted by law. Sometimes a fee may be charged for getting acquainted with the data, if stipulated by law.
- **Avaiability of services from one location.** State and local government institutions cooperate so that a citizen would obtain necessary information and services from the portal eesti.ee[47] and the personal information system[48].

4.22. Each document of interoperability architecture of an information system SHOULD contain a part handling technical interoperability.

5. Open standards

The Ministry of Economic Affairs and Communications organizes the mapping of IT related standard needs of public administration, promotes implementation of standards and disseminates standardization related information. The Technical Committee of the Estonian Centre for Standardization EVS TK4 is engaged in serving the Ministry of Economic Affairs and Communications (RISO)[49] in drawing up Estonian standards and guiding materials and taking over international standards. EVS TK4 mostly cooperates in the line of official standardization with International Organization for Standardization ISO and with the IT Joint Committee JTC1, created by International Electrotechnical Commission IEC as well as with the IT Association CEN/ISSS of the European Commitee for Standardization CEN.

The Estonian standards for information and document management are mostly drawn up by the Technical Committee for Standardization EVS/TK 22 “Information and documentation”. The committee's scope coincides with the scopes of ISO/TC 46 and ISO/TC 171 .

5.1.Estonian public sector MUST be an active member of IT communities as well as communities of standardization of information and document management, taking upon itself organization of activities of the corresponding communities.
5.2.Estonian public sector SHOULD support participation of Estonian experts in international standardization organizations.

The principles and structure of the public sector standards and the agreed standards have been described in a separate document “Open Standards”. The present document provides the most relevant decisions concerning open standards. Public sector agrees, at the guidance of the open

[47] http://eesti.ee
[48] https://www.eesti.ee
[49] http://www.riso.ee/et/it-standardimine/

standards working group and in cooperation with other concerned parties, on the minimum set of public sector open standards, compliance with which is compulsory for the public sector. The choice and assessment of standards is public and balanced.

Below, there is a list of the most relevant open standards, which institutions should use when communicating with one another or the public, on web sites and in public registers. With regard to in-house communication, institutions are allowed, although it is not recommended, to use other formats.

- CSV (*Comma Separated Value* [.csv]) – platform independent format for submitting sheet data[50]
- HTML (*HyperText Markup Language* [.html]) – hypertext markup language for creating web documents[51]
- BDOC – digital signature format, to replace DDOC, Estonian standard EVS 821:2009[52]
- DDOC – digital signature format, will be replaced with BDOC
- JPEG (*Joint Photographic Experts Group* [.jpg]) – graphics format[53]
- GZIP – package format[54]
- MPEG (*Moving Picture Experts Group* [.mpeg]) – video format[55]
- ODF (*Open Document Format* [.odf]) – open document format for office applications[56]; ODFsub-formats are .odb (database), .odf (formula), .odg (drawing), .odp (presentation), .ods (spreadsheets) ja .odt (texts)
- PDF (*Portable Document Format* [.pdf]) – platform independent document format[57]
- PDF/A (*Portable Document Format/Archive*) – format for archiving .pdf files[58]
- PNG (*Portable Network Graphics* [.png]) – raster graphics format[59]
- SVG *(Scalable Vector Graphic* [.svg]) – vector graphics format[60]
- TIFF (*Tagged Image File Format* [.tif]) – raster graphics format61
- TXT (*Plain Text, Text File* [.txt]) – plain unprocessed text format
- XHTML (*Extensible Hypertext Markup Language* [xhtml]) – extensible hypertext markup language[62]
- XML (*Extensible Hypertext Markup Language* [.xml]) – hypertext markup language[63]

5.3. In the Estonian public sector, there is an agreed minimum set of open standards which the public sector MUST follow. The choice and assessment of the standards is public and balanced.

5.4. The framework RECOMMENDS public sector organizations to follow the interoperability framework document “Open Standards”, when they create their own information systems.

6. Software and open specifications

Software related recommendations and rules are handled in a separate document of interoperability framework. Below, are the most relevant requirements for software interoperability.

[50]http://tools.ietf.org/html/rfc4180
[51] Vt http://www.w3.org/wiki/HTML
[52] http://www.evs.ee/tooted/evs-821-2009
[53] ISO 10918 (.jpg), vt http://www.jpeg.org/index.html
[54] Vt RFC 1952
[55] MPEG4/ISO/IEC 14496
[56] Vt "ISO/IEC 26300:2006 Open Document Format for Office Applications (OpenDocument) v1.0" ja http://en.wikipedia.org/wiki/OpenDocument
[57]http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=51502
[58]http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=38920
[59] Vt http://www.w3.org/TR/REC-png
[60] Vt http://www.w3.org/TR/SVG/
[61]http://tools.ietf.org/html/rfc2306
[62] Vt http://www.w3.org/TR/xhtml1/
[63] Vt http://www.w3.org/TR/2000/REC-xml-20001006, in Estonian: http://www.riik.ee/xml/trans/REC-xml-19980210-ee.html

6.1. When founding information systems and in public procurements' tender offers, alongside proprietary solutions, free software alternatives MUST be taken into consideration. Decision MAY be made in favour of free software, commercial software or a combined solution, but in case other conditions are equal, software with a source code is preferred. Each case is decided on an individual basis.
6.2. In solutions ensuring mutual communication of information systems, joint projects and jointly used information systems, but also in information systems that are being founded for the first time or that are being refounded, only open standards and products and services that support specifications SHOULD be used.
6.3. In information systems dependence on company based products and services SHOULD be avoided.
6.4. When ordering information systems, it is RECOMMENDED to procure a software code or adaptations added to a commercial product. Procured software SHOULD be registered in the EU repository with a free software licence (e.g. EUPL).
6.5. When ordering software, state and local government institutions are guided by the principle that the ordered software and adaptations are usable, without restrictions, in other public administration institutions (the principle cannot be applied in the case of standard software, whose proprietary rights are owned by the software producer). If several institutions have similar needs, it is RECOMMENDED to order software jointly.
6.6. The solutions obtained as a result of the development work ordered by the public sector MAY be used by the contractor in business activities outside the public sector, if it does nor infringe upon the interests of the party that ordered the work.
6.7. The solutions obtained as a result of the development work ordered by the public sector can be used by the contractor in foreign projects, if it does not infringe upon the interests of the party that ordered the work; the party that ordered the work does not hinder it and, if necessary, facilitates it.
6.8. In procuring office software, public sector institutions are guided by the following principles:

- In office software procurements, public sector MUST take into account available alternatives that are suitable with regard to functionality
- Public sector MUST use file formats that are opened with free software for publishing in websites and communicating with the public (residents, private sector and other public sector institutions)
- Public sector MUST take into account the advantages of platform independent office softwares
- Public sector COULD take into account the advantages of website based, browser independent office software
- When choosing file formats, public sector COULD take into account possibilities of using office software functionality as a service.

6.9. When choosing software, transparent procedures SHOULD be used. As a choice, RISO ordered guideline MAY be used[64]

7. Joint infrastructure services

Infrastructure service is a joint set of operational rules or technical functionality for providing one or several services or managing an information system.

Infrastructure service is, for example, accommodation of information systems in the accommodation environment of the private sector, or a standard solution created for developing single-type information systems (e.g. waste handlers' register, pet register, local government's website etc.). The strength of Estonian information system is effectively operating infrastructure services, which ensure the operation of information systems as an integrated whole.

[64] http://www.riso.ee/wiki/File:HindamisJuhised.odt

Part of the infrastructure services – support systems – are compulsory for all service providing information systems. Use of support systems has been enforced by the Government of the Republic resolutions. Support systems are first of all a set of operational rules, but they can also be created on the basis of joint technical functionality.

7.1. Support systems

The support systems of the state information system ensure horizontal interoperability of information systems. There are six support systems:

- the classifications system[65]
- the system of security measures for information systems[66]
- the system of address details[67]
- the data exchange layer of information systems[68]
- the geodetic system[69]
- the administration system of the state information system[70].

7.1. Use of support systems for the maintenance of the state information system is mandatory pursuant to Public Information Act[71] §43[9] upon maintenance of all state and local government databases.

7.2. Joint supporting infrastructure

Joint infrastructure services are services that are practical to be developed centrally in the country, and which ensure free of charge functionality for all the other services. Joint infrastructure services could be a foundation for developing the architecture of one's own information system or a tool for creating certain functionality. The number and composition of joint infrastructure services changes with time. The most relevant infrastructure components are:

- backbone network Peatee[72], coordinated by Estonian Information System's Authority
- electronic identity infrastructure, coordinated by the Ministry of Economic Affairs and Communications. Certification service is provided by private sector institutions. The surveillance body of certification institutions is the Technical Surveillance Authority. Identity documents together with certificates are issued by the Police and Border Guard Board. The public sector developer and administrator of the public key infrastructure is the Estonian Information System's Authority
- The Data Exchange Layer of Information Systems X-Road[73], coordinated by the Ministry of Economic Affairs and Communications and developed and administered by the Estonian Information System's Authority
- Mini-information System Portal MISP, coordinated by the Estonian Information System's Authority
- Document Exchange Centre DVK[74], coordinated by the Ministry of Economic Affairs and Communications and administered and developed by the Estonian Information System's Authority
- Information portal eesti.ee[75], processed by the Estonian Information System's Authority
- Citizen's personal information system “Minu asjad“ in information portal eesti.ee, whose authorized processor is the Estonian Information System's Authority

[65]https://www.riigiteataja.ee/akt/12910889
[66]https://www.riigiteataja.ee/akt/13125331
[67]https://www.riigiteataja.ee/akt/12901083
[68]https://www.riigiteataja.ee/akt/119012011015
[69]https://www.riigiteataja.ee/akt/128102011003
[70]https://www.riigiteataja.ee/akt/13147268
[71]https://www.riigiteataja.ee/akt/122032011009
[72]http://www.ria.ee/ASO
[73]http://www.ria.ee/x-tee
[74]http://www.ria.ee/dokumendivahetus
[75]https://www.eesti.ee/est

- Information portal of services and information systems, the management system of the eGovernment information system[76] (RIHA), coordinated by the Ministry of Economic Affairs and Communications, and whose responsible processor is the Estonian Information System's Authority
- Spatial data infrastructure[77], coordinated by the Estonian Land Board
- Free software information portal, coordinated by the Ministry of Economic Affairs and Communications (under development, will be accommodated into EU joinup environment)
- Open data information portal and supporting infrastructure, coordinated by the Ministry of Economic Affairs and Communications (the central components are being prepared).

7.1. When creating a public sector information system, the advantages of using joint infrastructure services of the state MUST be taken into account.

8. Management of interoperability frameworks

8.1. The interoperability frameworks of the state information system

The interoperability frameworks of the state information system handle information systems from the point of view of the state as a whole. The frameworks have been harmonized with the European frameworks and should ensure interoperability of Estonian information systems with those of other member states as well as with Europe centred information systems. The documents of the framework have been divided into four groups:

- general documents
- frameworks of interoperability dimensions and spheres of activity
- infrastructure
- guidelines and procedures.

The present document is a main document of frameworks. The documents of the framework are constantly updated and the current state of the documents is published in the wiki of the state information systems[78]. After updating, the official version of the document is endorsed, which is coordinated with the institutions of the public sector and published on the website of the framework of interoperability[79].

Preparation of the interoperability framework and the related documents is conducted by the Ministry of Economic Affairs and Communications (MKM), as the ministry responsible for the development of the state information system. At MKM, there was created a working group of interoperability of the state information systems, whose task is to advise the Ministry on working out documents of interoperability. For the sub-topics of the interoperability framework, there have been created official and unofficial working groups.

Administrative institutions have a duty to describe their services and information systems in the Management System of State Information System RIHA 80. RIHA processes support continuity of management of services and systems through changes.

[76]https://riha.eesti.ee/riha/main
[77]http://geoportaal.maaamet.ee/
[78] http://www.riso.ee/wiki/
[79] http://www.riso.ee/et/koosvoime/
[80]http://www.ria.ee/RIHA

The creation of state centred components of infrastructure (See chapter 7) is coordinated by the Ministry of Economic Affairs and Communications. Management and use procedures of central components can be enforced by legal acts. The authorized processor of the central components ensures their development and management during their whole life cycle.

8.1. The Ministry of Economic Affairs and Communications coordinates the initiatives relating to the interoperability of the state information system and MUST ensure modernity of the interoperability frameworks of the state information system.
8.2.The interoperability of services and information systems is administered during their whole life cycle in RIHA.
8.3. The creation and development of joint infrastructure components that support services is organized, during their whole life cycle, by the Ministry of Economic Affairs and Communications.

8.2. Interoperability frameworks of public sector institutions

Public sector institutions should analyse all the issues of interoperability of their institution and compile on the basis of it, the framework of interoperability architecture of their institution. Public institutions should submit their document of interoperability architecture of the information system through RIHA to an institution coordinating the state information systems and to other institutions as stipulated in the Public Information Act.

An institution's framework of interoperability architecture must be harmonized with the Estonian and European interoperability frameworks. An institution's framework is used in coordinating the legal ascts submitted by the institution in the Ministry of Economic Affairs and Communications, in making financing decisions from structural funds, in coordinating and registering information systems and services in RIHA. The framework can be used as an assisting or guiding material in information system related procurements, development works, maintenance of systems and in other activities.

In order to harmonize interoperability frameworks, it is practical to use a questionnaire[82], which sums up the requirements of the interoperability framework of the state information systems.

8.4. In their framework of interoperability architecture, public sector institutions MUST provide a description of the principles of the technical architecture of the information system, semantics, legal system and political context.
8.5. A public sector institution's framework of interoperability architecture is published in RIHA, and it is kept up-to-date during its whole life cycle.
8.6. An institution's framework of interoperability architecture MUST be harmonized with the interoperability frameworks of the Estonian information system. For harmonization, the most suitable tool is a questionnaire prepared for that purpose[83].

9. Harmonization of the Estonian framework

[81] http://www.creativecommons.ee
[82]http://www.riso.ee/wiki/Kysimustik#Koosv.C3.B5ime_raamistik_ja_arendusraamistik
[83]http://www.riso.ee/wiki/Kysimustik#Koosv.C3.B5ime_raamistik_ja_arendusraamistik

with the European framework

The European Union eGovernment Action Plan 2011–2015 measure 2.4.1 sets an objective that the interoperability frameworks of the member states SHOULD be harmonized by the year 2013. In the table that follows, there are 25 recommendations of the European Framework[84] and the corresponding requirements in the Estonian Interoperability Framework.

Recommendation of the European Framework	Corresponding requirements of the Estonian Framework
1. Public administrations should align their interoperability frameworks with the European Interoperability Framework to take into account the European dimension of public service delivery.	3.23, 4.1, 4.3, 4,4
2. Public administrations should ensure that public services are accessible to all citizens, including persons with disabilities and the elderly, according to e-accessibility specifications widely recognised at European or international level.	2.7–2.12, 2.17
3. Public administrations should consider the specific needs of each European public service , within the context of common security and privacy policy.	2.13–2-15
4. Public administrations should use information systems and technical architectures that cater for multilingualism when establishing a European public service.	2.16–2-24
5. Public administrations should formulate together a long-term preservation policy for electronic records relating to European public services.	2.31, 2.32
6. Public administrations should aim for openness when working together to establish European public services, while taking into account their priorities and constraints.	2.33, 2–34, 5.1, 5.2
7. Public administrations are encouraged to reuse and share solutions and to cooperate on the development of joint solutions when implementing European public services.	2.35–2.38, 6.1–6.13
8. Public administrations should not impose any specific technological solution on citizens, businesses and other administrations when establishing European public services.	2.39–2.42, 6.1, 6.9
9. Public administrations should develop a component-based service model, allowing the establishment of European public services by reusing, as much as possible, existing service components.	3.1–3.14, 7.1
10. Public administrations should agree on a common scheme to interconnect loosely coupled service components and put in place the necessary infrastructure when establishing European public services.	3.23, 3.24, 7.1, Resolution of the Government of the Republic "Data Exchage Layer of Information Systems"[85]

[84] European Interoperability Framework, http://ec.europa.eu/isa/strategy/doc/annex_ii_eif_en.pdf
[85]https://www.riigiteataja.ee/akt/12956835

Recommendation of the European Framework	Corresponding requirements of the Estonian Framework
	Model realizations X-Road[86] and DVK[87]
11. Public administrations should make their authentic sources of information available to others while implementing access and control mechanisms to ensure security and privacy in accordance with the relevant legislation.	2.13, 3.8–3.14, 3.21, 3.22, 3.23, Resolution of the Government of the Republic "The System of Security Measures of the Information System"[88]
12. Public administrations, when working to establish European public services, should develop interfaces to authentic sources and align them at semantic and technical level.	3.21, 3.22, 3.23, 4.17–4.22, Resolution of the Government of the Republic "Data Exchange Layer of Information Systems"[89], Semantic Interoperability Framework[90]
13. Public administrations, when working to establish European public services, should use a common taxonomy of basic public services and agree on minimum service requirements for secure data exchange.	2.13, 3.1–3.14, 3.21, 3.22, 3.23 Resolution of the Government of the Republic "Data Exchange Layer of Information Systems"[91]
14. Public administrations should carefully consider all relevant legislation relating to data exchange, including data protection legislation, when seeking to establish a European public service.	2.13, 4.11, 4.12, Personal Data Protection Act [92]
15. Public administrations should document their business processes and agree on how these processes will interact to deliver a European public service.	4.12-4.16
16. Public administrations should clarify their organizational relationships as part of the establishment of a European public service.	4.12, 4.17-4.20, Resolution of the Government of the Republic "Data Exchange Layer of Information Systems", 3.22. Resolution of the Government of the Republic "Management System of State Information System""[93]
17. Public administrations working together to provide European public services should agree on change management processes to ensure continuous service delivery.	4.12, Resolution of the Government of the Republic "Management System of State Information System"[94], Software framework
18. Public administrations should support the establishment of sectorspecific and cross-sectoral communities that aim to facilitate semantic interoperability and should encourage the communities to share results on national and European platforms.	4.21–4.25, Semantic framework

[86]http://www.ria.ee/x-tee
[87]http://www.ria.ee/dokumendivahetus
[88]https://www.riigiteataja.ee/akt/13125331
[89]https://www.riigiteataja.ee/akt/12956835
[90]http://www.riso.ee/et/files/RISsemantikaV07-loplik.pdf
[91]https://www.riigiteataja.ee/akt/12956835
[92]https://www.riigiteataja.ee/akt/130122010011
[93]https://www.riigiteataja.ee/akt/13147268
[94]https://www.riigiteataja.ee/akt/13147268

Recommendation of the European Framework	Corresponding requirements of the Estonian Framework
19. Public administrations should agree on formalised specifications to ensure technical interoperability when establishing European public services.	4.5, 5.1-5.4, "Open Standards"[95]
20. Public administrations, when establishing European public services, should base interoperability agreements on existing formalised specifications, or, if they do not exist, coooperate with communities working in the same area.	5.1-5.4, "Open Standards"[96]
21. Public administrations should use a structured, transparent and objective approach to assessing and selecting formalised specifications.	5.3, "Open Standards"[97] 6.9.; Software framework; Guideline "Principles of Software Assessment" [98]
22. When establishing European public services, public administrations should prefer open specifications, taking due account of the coverage of functional needs, maturity and market support.	"Open Standards"[99] Software framework; Guideline "Principles of Software Assessment" [100]
23. Public administrations should lead or actively participate in standardisation work relevant to their needs.	5.1, 5.2. "Open Standards"[101]
24. Public administrations should ensure that interoperability is ensured over time when operating and delivering a European public service.	8.2, Resolution of the Government of the Republic "Management System of State Information System"[102]
25. Public administrations should establish a framework for the governance of their interoperability activities across administrative levels.	8.1-8.6, Resolution of the Government of the Republic"Management System of State Information System"[103]

[95]http://www.riso.ee/wiki/Avatud-standardid
[96]http://www.riso.ee/wiki/Avatud-standardid
[97]http://www.riso.ee/wiki/Avatud-standardid
[98]http://www.riso.ee/wiki/File:HindamisJuhised.odt
[99]http://www.riso.ee/wiki/Avatud-standardid
[100]http://www.riso.ee/wiki/File:HindamisJuhised.odt
[101]http://www.riso.ee/wiki/Avatud-standardid
[102]https://www.riigiteataja.ee/akt/13147268
[103]https://www.riigiteataja.ee/akt/13147268