Ministry of Economic Affairs and Communications

Department of State Information Systems

Estonian IT Interoperability Framework

Abridgement of version 2.0

This document is open for proposals from public, private and third sector organisations as well as from other interested parties. Please, send your proposals to the e-mail address: koosvoime@riso.ee

The framework is reviewed and, if needed, updated annually. In new versions, proposals made during the last period are taken into account. The Estonian IT interoperability framework as well as the related documents Estonian IT Architecture and Estonian Semantic Interoperability Framework can be downloaded at: http://www.riso.ee/eng/koosvoime.

Table of contents

Summary

One of the main objectives of the Estonian information and communication technology (ICT) policy in the coming years is to make state information systems citizen-oriented and service-based. Information systems have to be integrated into a single logical whole serving the population and different organisations. To this end, it is necessary to agree – on the state level – upon clear rules and agreements, and to use common middleware.

During the last couple of years, public key infrastructure (PKI) has been built and several user-oriented portals, such as http://www.riik.ee, http://www.eesti.ee, https://www.eesti.ee, have been developed in Estonia. In addition, data exchange layer called X-Road has been created. The present framework generalizes the positive trends in the development of state information systems and gives a systematic overview of them.

In order to implement the interoperability framework, the state has to be citizen-centred and its information systems must be service-based. Besides, as a member state of the European Union (EU), Estonia has to ensure interoperability of its information systems with those of other member sates. Though the functioning of state information systems is targeted at achieving the same rationality as the private sector, sharp differences between the state and the private sector remain. It is not the state's aim to "sell" services, but to ensure their expediency. It is presumed that in the nearest future, information systems will enable to perform several operations from one and the same place, e.g. service users will no longer have to visit officials and search for websites. The efficiency of public sector information systems cannot be measured by same indicators as that of the private sector (return on investment). In terms of integrated service provision, public sector information systems have to serve as pathfinders for private sector information systems. Participation through public procurement in the development of state information systems and satisfying the needs of the state as a whole poses a considerable challenge for the Estonian IT sector.

Institutions are autonomous as to the IT architecture and interoperability principles within their internal information systems, but when launching new IT projects, central and local government institutions have to follow the principles of the interoperability framework.

The framework has been elaborated by IT experts representing the central and the local government agencies as well as organisations from the third and the private sector. The work of the expert group was led by the Department of State Information Systems of the Ministry of Economic Affairs and Communications together with private sector specialists.

1 Introduction

1.1 Definition of interoperability and objectives of the framework

Interoperability denotes the ability of information systems and of business processes they support to exchange data and share information and knowledge.

The Estonian IT interoperability framework is a set of standards and guidelines aimed at ensuring the provision of services for public administration institutions, enterprises and citizens both in the national and the European context.

The IT interoperability framework and the related documents are obligatory to follow in order to ensure mutual communication between the information systems of central and local government agencies. The framework documents cannot, however, be regarded as legal acts. The obligatory nature of the framework is expressed through the following aspects:

- The framework and the related documents go through a consultation period during which central and local government agencies, the private sector, third sector organisations, as well as private persons can submit their proposals. Thus, the obligatory nature of the framework derives from the fact that the document serves as an agreement between different stakeholders.
- Pursuant to the Government of the Republic Act, the Act on the Databases of the State Information System (draft), and "The Principles of the Estonian Information Policy", co-ordination of the development of state information systems is assigned to the Ministry of Economic Affairs and Communications. The interoperability framework and the related documents are the basic documents of the state information system.

The following documents have been taken into account when drafting the Estonian IT framework:

- political decisions and legislation of the Republic of Estonia;
- „The Principles of the Estonian Information Policy 2004-2006", approved by the Government of Estonia;
- the EU Interoperability Framework and the related documents.

The Estonian IT interoperability framework serves as:

- a guidance for those elaborating concepts for country-wide information systems;
- a guidance for IT project managers in the public administration for elaborating concepts for the information systems of their institutions;
- an aid in the organisation of public procurements.

The aim of the IT interoperability framework is to increase public sector efficiency in Estonia by improving the quality of services provided to citizens and enterprises both at the Estonian and the EU level. The specific objectives of the framework are the following:

- to facilitate and, consequently, implement the transformation of institution-based public administration into a service-centred one, where all citizens can communicate with the state without knowing anything about its hierarchical structure and division of roles;
- to reduce public sector IT expenses through a wide use of centrally developed solutions;
- to improve the interoperability of new IT projects through a co-ordinated use of centrally developed infrastructure, middleware (public key infrastructure (PKI), data exchange layer X-Road, citizen's environment etc) and open standards;
- to improve the co-ordination and management of state information systems and to accelerate the development of IT solutions;

- to contribute to the co-development of the state information system;
- to allow autonomous development for all systems within the principles of organisational, semantic and technical interoperability;
- to ensure free competition in the area of public procurement.

The document examines the state IT interoperability framework from three aspects: organisational, technical and semantic interoperability.

The framework does not attempt at providing clear solutions to all IT-related problems in the state. The transformation from the institution-based world to a service-centred and citizen-oriented one is a longer process, necessitating changes in the legislation and in the organisation of public administration activities. Activities that do not require creative intellectual work by human beings should be detached from the typical activities of the public sector. The current version of the framework does not aim at describing new ways of governance that the development of information society brings along, but seeks to fix the rules, trends and principles necessary for the development of such a society from the viewpoint of information systems.

The first version of the framework was published in 2004 with the present version serving as its follow-up.

1.2 Key principles of the state IT interoperability

- The institution-based approach should be replaced by service-centred one;

- public services (including nested services) are provided free of charge for public sector institutions;

- the development of information systems is based on internet-centred approach;

- XML-based technologies are used for the integration of information systems and the presentation of data;

- information systems provide and use services via a data exchange layer based on multilateral agreements;

- course will be taken towards wider use of open standards;

- in developing information systems, open source based solutions are considered alongside proprietary ones;

- access to public services should preferably be ensured via a web browser by different channels and devices;

- all services requiring user authentication and authorization exploit the secure middleware X-Road for data transport;

- the authentication and authorization procedures of civil servants are based on the use of the Estonian ID card;

- as a temporary alternative, authentication mechanisms of internet banks can be used for citizen authentication;

- central and local government agencies co-operate in order to ensure the provision of information and services for citizens, officials or entrepreneurs from one place, without need to know anything about the subordinating system of the executive power or the division of roles therein.

1.3   Documents of the interoperability framework

The documents of the interoperability framework describe the main principles of the state IT interoperability. In the future, the framework will be complemented by several other documents dealing with matters concerning interoperability. All documents related to the state IT and interoperability framework will be elaborated in a co-ordinated manner and according to common principles. To this end, the following mechanism will be used:

- The initiator of an interoperability document (any central or local government agency) draws up, with the help of experts, an outline of the document and organizes a public discussion to analyse it.
- The document is published for discussion on the website of the Department of State Information Systems (hereafter: RISO) at http://www.riso.ee. Together with RISO, the document initiator informs network participants about the document. Comments made by participants are published on the web. A month later, the document initiator reviews all comments received and responds to them on the web. Depending on the type of the document, discussions can be open for participation to organisations representing the public, the private and the third sector, as well as individuals.
- Based on the feedback received, the initiator then prepares a new version of the document, which is again published on the RISO website. In case no further substantial comments are made to it, the initiator draws up a final document and, after the document has been approved by RISO, it will be considered final.
- All interoperability documents are open for comments all year round. At least once a year, the initiator is obliged to review the document and, if needed, to update it. Prior to the publication of a new version, an expert committee as well as other interested stakeholders are invited to submit comments on it within a period of one month.

2 Principles of interoperability

2.1 Dimensions of interoperability

Interoperability is analysed from three different angles:

- **Organisational interoperability** stands for the ability of organisations to provide, by making use of information systems, services to other organisations or to their clients. Organisational interoperability is associated with the activities of organisations and agreements between them. Organisational interoperability is ensured by legislation and general agreements.

- **Semantic interoperability** refers to the ability of different organisations to understand the exchanged data in a similar way. This presumes the creation of a mechanism allowing the presentation of service data and data definitions.

- **Technical interoperability** denotes the interoperability of infrastructure and software. Infrastructure interoperability is the ability of hardware acquired by different organisations to work in a connected way. It is ensured by the internet and the PKI infrastructure. Software interoperability refers to the ability of software used in different organisations to exchange data. Achieving software interoperability requires the establishment of common data exchange protocols, development of software necessary for the management of data connections, and creation of user interfaces in order to enable communication between different organisations.

2.2 Architecture of interconnected systems

Systems can be connected based on two principles of architecture:

- bilateral agreements,
- multilateral agreements.

Bilateral agreements   Multilateral agreements
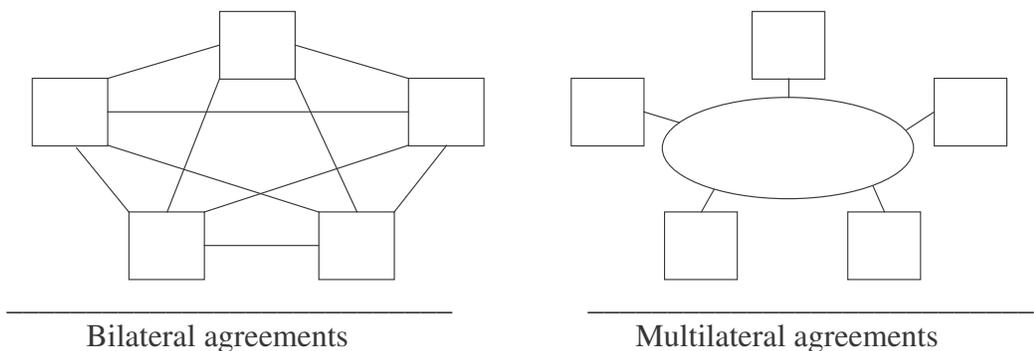
Figure 1. Types of agreements

There is a trend of moving from bilateral agreements to multilateral ones, allowing thus to considerably reduce the number of connections that are necessary for mutual communication between information systems, and facilitating, consequently, the management of connections. The responsibility for ensuring general compliance with rules of organisational, semantic and technical interoperability lies with organisations.

2.3 Public services and nested services

A public service refers to a service provided by an organisation to citizens, agencies, enterprises or organisations. A public internet-based service is characterized by the following factors:
- it is directed to personalised users (individuals);
- it is provided online;
- in case of central and local government agencies, provision of such services is established in legislation;
- in case of private companies and other organisations, the provision of such services is regulated by legislation or by contracts concluded with central or local government agencies.

In the electronic environment, a public service has to be accessible for its target group based on the following requirements:
- the service is provided to the user at as close level to him as possible;
- the service can be used with minimum previous training;
- minimum information is requested from the user;
- the service is secure to use for all.

An interconnection service is an operation performed by one organisation that constitutes a necessary part of an operation performed by another organisation, but which does not necessarily have a meaning in itself in this organisation. An interconnection service is used by an information system (programme). An interconnection service is not an independent service of an organisation performing it, but it may be either:

- a part of a public service operation provided by another organisation;
- or a part of an internal working process of another sub-organisation.

2.4 Descriptions and quality of services

Service descriptions are compiled by service providers and should preferably contain the following information:
- the syntax and the protocol of a service (e.g. in case of X-Road services these are given in a WSDL-file format);
- service provision policy (based on which principles, to whom and for which purposes the service is provided);
- quality indicators of the service (its functionality, reliability and efficiency).

Service descriptions are published in the administration system for state information systems (hereafter RIHA). To present the characteristics and indicators of a service, taxonomy has been created in RIHA's UDDI. The free text of the service description is published as a separate file in the public web (either in RIHA, at the service provider or elsewhere) to which a link has been created from service data maintained in RIHA (e.g. UDDI model).

It is the task of the service provider to describe a service in RIHA. The easiest way to do that is to describe services (including non-X-Road services) in a WSDL file that RIHA automatically reads and which completes data fields in RIHA. The universal part of the description (e.g. descriptions of protocol, policy etc) that applies for several services or databases should be stored in a separate file to which a link is created from the WSDL file.

In order to facilitate the description of services, the existing taxonomy in RIHA will be further elaborated, a guide for compiling service descriptions will be developed, and access to service descriptions in RIHA will be automated.

Describing quality indicators is necessary from the point of view of evaluating and ensuring the quality of services. The quality of a data service refers to the degree to which service indicators correspond to service requirements.
Service requirements are quality indicators set out in service description. Quality indicators characterize the functionality, reliability and efficiency of a service.
**Functionality indicators** describe the semantics of input and output parameters of a service as well as the preconditions for and outcomes of using a service.
Reliability and efficiency indicators describe fault tolerance, permitted frequency of failures, integrity, availability, usage volume and use of resources allowed for the service, as well as time spent on service provision. The availability and integrity of a service are presented as its security class.

Service providers are obliged to ensure the quality of their service, i.e. to systematically perform operations necessary for guaranteeing that the service complies with requirements set for it. At the justified request of service users, service providers are obliged to bring the quality of their service into accordance with the required level.

2.5   *General structure of the state information system*

The state information system is regarded as a service-centred organisation, meaning that all operations performed by civil servants, entrepreneurs, citizens, as well as software are considered services. End users access services in a common service space. They are not interested in the organisation directly providing them the service, but in the service itself.
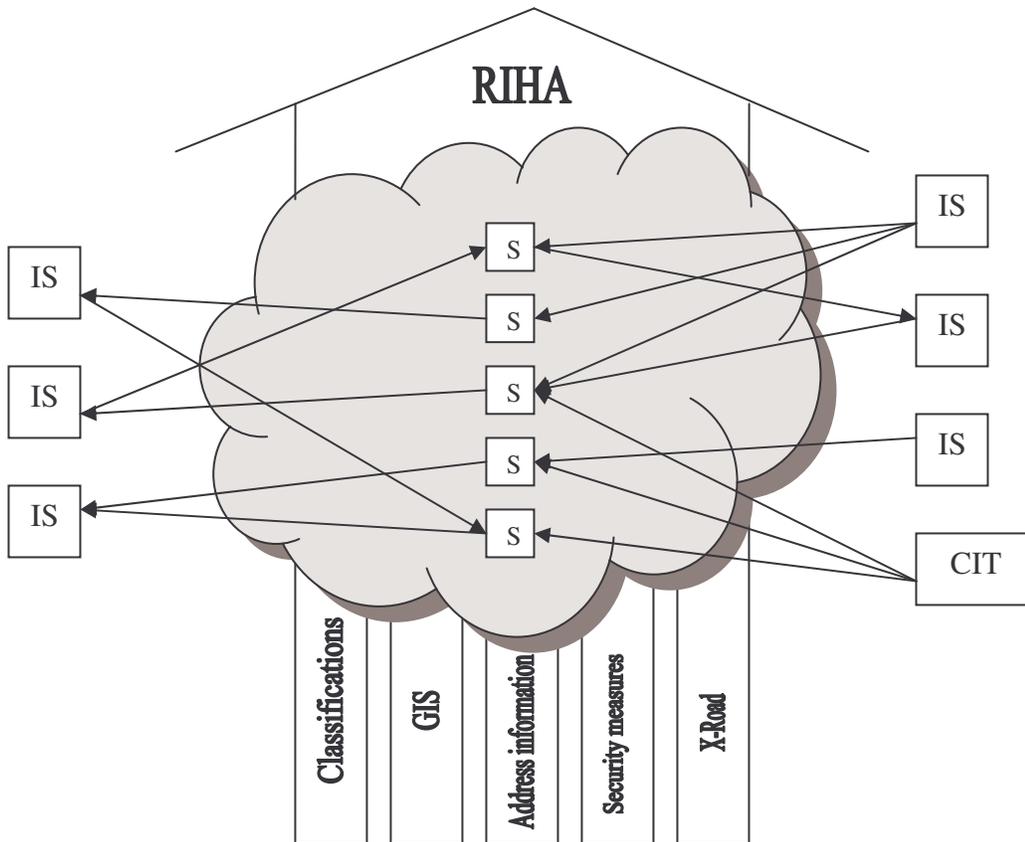
Figure 2. The state information system can be regarded as a service space, which is based on support systems and is administered through RIHA. Information systems communicate with each other via services (S – a service, IS – an information system, CIT – the citizen portal as a special guide to the information system).

Central and local government agencies, private companies, as well as third sector organisations all provide services.
Services are used by central and local government agencies, private companies, third sector organisations, and individuals. The common service space allows individuals to represent, when using public services, both themselves and the company they work for.
Services may or may not require authentication.

The logical components of the state information system are the following:
- information systems (both as service providers and service users);
- the administration system for the state information systems (RIHA) together with its services catalogue;
- the state-administered citizen IT environment;
- support systems and rules.

The support systems and rules for the maintenance of the state information system are the following:
  o the classifications system;
  o the system of address details;
  o the data exchange layer for information systems – X-Road;
  o the geodetic system;

10

o the system of security measures for information systems.

The classification system is a set of common principles for the administration and use of classifications. The system consists of:
- requirements for classifications;
- classifications;
- administrators of classifications;
- users of classifications;
- list of classifications and their administrators, classifications services.

The system of address details is a set of principles, which allows a unified identification of address objects both in their physical location and in different databases. The system of address details consists of:
- databases, which process and handle address details;
- requirements for chief processors of address details, for respective services and for users;
- X-Road address services.

The data exchange layer of information systems – X-Road – is an environment enabling secure internet-based data exchange.

The geodetic system consists of:
- the geodetic reference system;
- the system of plane rectangular coordinates;
- the height system;
- the gravimetric system.

The security measures system for information systems consists of:
- the procedure for the specification of security measures;
- the organisational and technical standard measures for data protection.

2.6 *Principles of data organization in the state information system. Data services*

Below given are the main definitions, rules and principles of data organization in the state information system.

State information system's basic data are data the use of which is obligatory in other databases in order to ensure authenticity in data processing. Basic data is set out in a legal act regulating the establishment of a database. The owner of the data in the state information system is the state. The legal effect of data does not change on their transfer over the data exchange layer of databases.

Person's right to access data about himself. Data maintained in state information system's databases are public and everyone has the right to access such data pursuant to the Public Information Act, except if access to or release of data is prohibited by law or if the data are intended for internal use only. Unless restricted by law, every person has the right to access data concerning himself in information systems and to access information about enquiries made about his data by other people. In cases provided by law, fees may be charged for access of data maintained in state information systems.

Restrictions upon recording data concerning security authorities. Data concerning a security authority, which are classified as a state secret or prescribed for official use, are only recorded in databases of security authorities. Upon recording other data concerning security authorities in state

databases, shadow information may be used if necessary. Shadow information is used on the basis of a classified directive of the head of the security authority in which the actual data concerning the security authority and the shadow information used upon regarding the data in state databases shall be set out.

Data service. A data service is the release, correction, erasure or addition of data processed in the state information system to a person, who is interested in obtaining the service and is entitled to it, either in the manner the entitled person has wished or pursuant to legislation (for a charge or free of charge).

Provision of a data service is a procedure during which the provider of the data service releases data to an authenticated and authorised service user or in the course of which an authenticated user of the data service adds or changes data in the data service provider's information system. The data service provider is responsible for the availability and correctness of his data.

Opening of a data service is a procedure during which the data service provider develops tools for the provision of the service, makes the service available over the data exchange layer, and publishes its description as well as user guide in RIHA.

Administration of a data service is a procedure ensuring to data users the availability of the service as well as integrity of the service data.

Use of a data service is a procedure during which an authenticated and authorised data service user either obtains data from the service provider or adds or changes data in the service provider's information system. Data service users are authorised and authenticated legal or physical persons.

The use of data services is free for central and local government agencies and for legal persons in public law for the performance of functions imposed on them by law. In addition, use of data services is free of charge for legal persons in private law performing public law functions.

Authentication (identification) **of data service users** is a procedure during which the person and/or information system applying for the use of a service is authenticated. Information systems are authenticated on the basis of the security server's certificate provided by the data exchange layer of state information systems. Authentication of persons using an information system is the responsibility of an agency administering the respective system. Officials of central or local government agencies are authenticated, if possible, with the national ID card. Programmes using the services of an authenticated information system go through an additional authentication when they are started and this is done on the basis of the certificate of a person responsible for the programme. Individuals and entrepreneurs using services via the citizen portal are authenticated with the ID card or through internet banks.

Authorisation of a data service user is a procedure during which the right of the authenticated person or information system to use the service is verified. User-oriented information systems are authorised according to their affiliation to certain user groups (a user group may consist of only one institution). User groups are created and administered in RIHA. The responsibility for the authorisation of user groups lies with service providers. Persons, who use services via user information systems, are authorised by agencies administrating the respective information systems. Use of the citizen portal does not require authorisation (authentication, however, is needed).

2.7   Open standards

In order to ensure interoperability, central and local government agencies use open standards and specifications in their information systems. In the context of this document, an open standard is a standard meeting the following criteria:

- It has been adopted and is further developed by a non-profit organisation. Its development is based on consensus and open decision-making procedures, allowing the participation of all competent interested parties.

- It has been published and is available free of charge or at a nominal cost for all users. Everyone must have the right to copy, distribute and use open standards for free or at a nominal cost.

- Patent rights and other intellectual property related to the use of an open standard or a part of it are available for all users without author's royalties.

- There are no restrictions on its re-use and distribution.

2.8   Principles of using open source software

According to the definition given by the Open Source Initiative (OSI, http://www.opensource.org), open source software (OSS) must meet the following criteria:
- the licence can be freely redistributed;
- its source code is available;
- the licence must allow modifications and derived works;
- the licence may restrict source-code from being distributed in modified form only if the licence allows the distribution of "patch files" with the source code for the purpose of modifying the he program at build time;
- the licence must not discriminate against any person or group of persons;
- the licence must not restrict anyone from making use of the program in a specific field of endeavour;
- the rights attached to the program must apply to all to whom the program is redistributed without the need for execution of an additional licence by those parties;
- the licence cannot be specific to a product;
- the licence cannot place restrictions on other software;
- the licence must be technology-neutral.

Any software corresponding to the principles of the OSI licence is considered open source software. For instance, the following licences correspond to OSI requirements: GNU General Public License (GPL), Berkley Software Distribution Licence (BSD), and Mozilla Public Licence (MPL). OSS products are, in essence, publicly available specifications, the development of which is discussed in the democratic manner and which are, due the accessibility of their source codes, interoperable.

Central and local government agencies have to observe the following principles concerning the OSS:
- In the development of information systems and in tender notifications, OSS-based solutions have to be considered alongside proprietary ones. Decisions may be made in favour of OSS, commercial software or combined one, but in case of equality in terms of other requirements, open source software is to be given priority. Decisions should be made on a case-by-base basis.

- In solutions that ensure mutual communication between information systems, in joint projects, in commonly used information systems, as well as in all new or modernized information systems only products supporting the use of open standards and specifications should be used.

- Adhering to company-specific products and services as well as developing dependence on them has to be avoided.

- When purchasing IT solutions, the code of the acquired software or, in case of a commercial product, its adaptations should also be procured, if possible.

- If possible, a principle is applied to any software procured by central or local government agencies according to which the procured software as well as its adaptations can be used without restrictions in other public administration institutions (the principle cannot be applied to

standard software the ownership of which lies with the software producer). In case several agencies have similar needs, joint software acquisitions should be considered.

2.9 Software in Estonian language

Estonia promotes the localisation and adaptation of software so as to bring it into accordance with the requirements of the Estonian language and culture. In addition to requirements set out in EVS 8[1], use of Estonian spelling checkers in text-based applications and employment of assistant module for text-indexing might be expedient.

---

[1] EVS 8:2000 Requirements on information technology in Estonian language and cultural environment

3 Nation-wide information systems

3.1 General principles

There are two types of nation-wide information systems:

- Common single point of entries that operate in collaboration of state information systems. Users of public sector information systems are not interested in state information systems as such, but rather in the data maintained in them. State information systems have to co-operate and function as a whole for users.
- Support systems refer to agreements between state information systems as well as the respective middleware. As a rule, support systems do not have a meaning in itself. These systems ensure interoperability and re-use of resources.

The establishment and development of nation-wide information systems is coordinated by a government agency that has been vested with the responsibility for the co-ordination of the respective field. The responsibility for the functioning of these systems lies with an institution designated by the co-ordinating government agency or an enterprise from whom the agency has ordered the performance of the respective activity.

State domains and portals are administered by an institution responsible for the co-ordination of state information systems, while the use of these domains and portals is organised by an agency or a company designated by the co-ordinating agency. The agency organising the use of portals and domains owns computer resources for providing, if necessary, website hosting service for public sector institutions.

In developing state portals, recommendations of the Web Content Accessibility Guidelines Working Group (WCAG WG) have to be followed [see http://www.w3.org/WAI/]. Requirements for website content have been published at: http://www.riik.ee/kord/ (only in Estonian).

In the public sector, institutional and thematic portals function as a whole in co-operation with state portals www.riik.ee and www.eesti.ee. In the development of these portals, the following principles have to be observed:

- the content of the portals is preferably XML-based and re-usable by any agency or person in any information system;
- for data exchange, XML format is used over http or https protocol;
- the used XML format is easily understandable and does not contain noise – unnecessary tags and details;
- the used XML format has to be documented in an understandable manner for developers;
- the presentation layer is realised as a separate application that communicates with the main application via XML texts and generates the HTML necessary for the user or realises the interface in some other way (WAP, SMS, desktop solutions etc). Direct generation of HTML text that does not support adaptable semantics from the main application has to be avoided;
- portals should be designed so that content producers could use it in a database-based manner, while for ordinary users, they would be generated in a static way;
- portals are not re-designed unless there is a clear need to add functionality;
- the tables of contents and summaries of portals are presented, in addition to their visual design, also as RSS or RDF feeds. Standard-based interoperability has to be ensured between institutional/thematic portals and the citizen information portal http://www.eesti.ee and the eState portal http://www.riik.ee.

3.1 Interoperability of state agencies' portals

3.1.1 Websites of state agencies

State agencies maintain at least one domain and one website that form a part of its information system. Data are generated into the web server mainly from agencies' operational information systems, ensuring, thus, the dynamic updating and efficacy of data. Static websites are connected to operational systems; they are added to the web server and regularly checked. Principles of data acquisition are set out in agencies' document management procedures.

A state agency's website is laconic, aesthetic, adequate, topical and ergonomic. The structure of text material on state agencies' websites has to be well-considered. The information and data management of a website must ensure that users could find solutions to their problems in a fast and transparent way. Use of pictorial material on state agencies' websites has to be brought to a minimum. The websites should include the following views:
- institutional,
- citizen-centred,
- thematic.

3.1.2 riik.ee domain

The riik.ee and gov.ee domains are administered commonly by state agencies. All institutions have the right to create third-level domains. It is recommended to use riik.ee domain names for websites bringing together several institutions of the same field (e.g. vanglad.riik.ee – a domain for Estonian prisons) and for the creation of web addresses for registers (e.g. teeregister.riik.ee for the Estonian Road Register).

3.1.3 eState portal http://www.riik.ee

The central element of the riik.ee domain is the single point entry, the eState portal www.riik.ee that operates in collaboration of public sector institutions. The portal http://www.riik.ee:
- ensures access to information provided by state constitutional institutions as well as central and local government agencies;
- reflects, in a balanced manner, the functions of all state institutions;
- through its English and Russian versions provides a balanced and adequate overview of Estonia's state structures to the rest of the world.

The eState portal functions as a whole with the following portals: the eDemocracy portal tom.riik.ee, the Government's portal valitsus.riik.ee, and the Prime Minister's portal peaminister.riik.ee. The portal allows performing search from all public sector websites.

3.2 Interoperability of thematic and citizen-centred portals

3.2.1 Thematic and citizen-centred portals

The websites of public sector institutions must include a thematic and a citizen-centred view. While the interoperability of institutional views is primarily ensured at the level of general information, thematic and citizen-centred portals require high interoperability and real information exchange. Works yet to be done in this field include the elaboration of taxonomy for thematic portals, the development of XML based standards for citizen-centred materials, and the creation of mechanisms for information exchange between thematic portals.

3.2.2 eesti.ee domain

Domains eesti.ee, estonia.ee, as well as eesti.info are administered commonly by interested institutions. All institutions can create third level domains. eesti.ee domain names should be used in thematic portals targeted at citizens (e.g. euro.eesti.ee and euro.estonia.ee). Besides, these domain names are suitable for websites developed for citizens in co-operation between several institutions (e.g. the joint portal on corruption – korruptsioon.ee – created by the Minister of Interior and the Ministry of Justice should have a name korruptsioon.eesti.ee).

3.2.3 Information portal http://www.eesti.ee

The information portal is freely accessible for all in order to inform the Estonian citizens about their rights and obligations as well as about services provided to them by public sector institutions. Such citizen information is relevant both for foreigners and permanent residents of Estonia in order to better understand the Estonian way of life.

As a general rule, holders of information are central or local government agencies, which publish information and documents.

The information portal ensures access to information provided by state institutions throughout the citizen's life cycle and by thematic fields. In order to avoid chaos in the content of the portal and to ensure that information could be easily found, the editors of the portal map the fields of life, elaborate the structure for presenting information, and, with the objective of avoiding duplication, centrally organise the initial drafting of texts to be contained in the portal. In order to keep the portal information constantly updated, institutions should notify the editors about any further changes in their field of administration.

State agencies monitor information concerning their field of administration on the eesti.ee portal and, if necessary, make proposals for updating it. Materials on the portal can be downloaded freely by all central and local government agencies in order to be published on their own websites. The information portal is linked with the so-called citizen portal. Central and local government agencies can use the e-service environment for the communication with citizens.

According to the EU interoperability framework, all member states are expected to develop analogical portals in the coming years.

3.2.4 Citizen portal https://www.eesti.ee/

Having passed authentication, the citizen portal allows citizens:
- to redirect the e-mail address provided to them with the national ID card;
- to use documents they need for their communication with the state;
- to use X-Road services;
- to use notification services;
- to use an environment for giving digital signatures.

Public sector institutions are obliged to provide e-services that require authentication and are targeted at citizens and the private sector (express services, notification services etc) via the citizen portal. Besides, respective links to the citizen portal should additionally be published on their own websites.

3.2.5 Portal Your Europe http://europa.eu.int/youreurope/

Your Europe is a multilingual portal giving individuals and businesses practical information about their rights and opportunities in the EU. The portal's front page information as well as its basic information, navigation sites, and an area for frequently asked questions are published in all 20 EU official languages. Specific services are in the language of a country providing the service and, additionally, in English, French and German. In addition, the portal contains links to national portals, where information must be presented in the official language of a particular country and, additionally, in at least one of the EU official languages.

3.3 Interoperable document management systems

The interoperability of document management systems denotes the ability of these systems to mutually exchange and manage digital documents. Document management systems exchange information without any interim paper forms and regular post services. Into these systems have been integrated processes for the use of network services and for the processing of network services targeted at citizens and enterprises.

In order to achieve interoperability of document management systems in central and local government agencies the following activities are needed:
- Further development of X-Road so as to ensure document and data transport over the data exchange environment. All document management systems need to have an interface with the central document exchange point.
- The elaboration of XML-based descriptions of documents and their metadata for document compilation in document management systems.
- All public sector document management systems must be able to communicate with the citizen's IT environment: to receive applications from citizens and entrepreneurs and to respond to them.

The responsibility for the interoperability of document management systems is assigned to the State Chancellery together with the National Archives of Estonia.

3.4 Interoperable geoinformation systems (GIS)

The interoperability of geoinformation systems means that geoinformation services are easy to use and digital maps are accessible for all authorized users and for other information systems.

The interoperability of public sector geoinformation systems has to be based on principles of open standards:

- preconditions have to be ensured for the usability of digital maps and spatial data together with data layers that are significant either from local or administrative viewpoint;
- all agencies, enterprises and citizens must have the possibility to use digital maps that have been developed by the public sector and are based on open GIS standards;
- it must be possible, without any significant additional costs, to exploit new geoinformation data sources, provide new e-services through open interfaces, and add to the existing e-services links to geoinformation services;
- authorized use of data has to be ensured (e.g. objects falling into the Category I of nature conservation are only accessible for authorized users).

Simple search mechanism has to be ensured for finding information about the availability of spatial data and maps, their accessibility, possibilities of use, as well as about conditions for their acquisition or use – a catalogue service must be developed about the availability of spatial data and possibilities of different map applications.

According to the trans-European initiative INSPIRE (http://www.ec-gis.org/inspire/), which aims at the creation of a spatial information structure for the European communities, new data sources have to be added to the interoperable system of service providers. In the development of regional geoinformation systems, principles of open GIS standards have to be followed.

The responsibility for the interoperability of geoinformation systems lies with the Ministry of Environment, which:

- develops a map interface to the X-Road;
- exploits, by using IT tools that are based on open standards, basic maps developed by the Land Board;
- in co-operation with other relevant agencies develops tools for the implementation of new spatial data layers.

3.5 Administration system for the state information system (RIHA)

The objective of RIHA is to ensure the interoperability of public sector information systems and the re-use of technical, organisational and semantic resources.

RIHA user groups are the following:
1) For service users, RIHA is a tool enabling:
- to obtain information about existing services as well as those under development, about service descriptions and principles of service provision;
- to apply for the right to use a service;
- to propose the creation of a new service;
- to use, according to one's rights, data services;
- to administer in-house access rights;

- to ensure legitimate use of data services.

2) For information systems administrators and service providers, RIHA is a support system for the performance of actions imposed on them by law, enabling:
   - to register information systems in RIHA;
   - to (formally) join with X-Road;
   - to join an agency's information system with X-Road;
   - to maintain statistics on the use of an information system;
   - to enter into RIHA data about an information system as well as to change, correct and archive them;
   - to create and open data services;
   - to describe services and principles of service provision;
   - to register services in RIHA (in case of X-Road services this is an automatic process);
   - to ensure access to data services for authorized users;
   - to register information system's classifications in RIHA.

3) For classifications administrators, RIHA will become a tool supporting the performance of the following tasks:
   - submitting a classification for approval, prior to its establishment, to the Statistical Office;
   - the establishment of a classification pursuant to a procedure prescribed in a regulation of the Government of the Republic;
   - the registration of a classification pursuant to a procedure established by a regulation of the Government of the Republic.

4) Legal persons in private law as well as citizens can obtain information from RIHA about the actual state of the state information system and about services opened for them by different state agencies. In addition, they can make proposals to information systems administrators about the creation of new services.

5) For the Ministry of Economic Affairs (for the Department of State Information Systems in particular), RIHA will serve as a supplementary instrument for the co-ordination of state information systems.

6) For the Estonian Informatics Centre, RIHA will be a tool for the development and administration of the data exchange layer X-Road, the state register of databases and other support systems for the maintenance of databases.

7) For the Statistical Office, RIHA will serve as a tool for the co-ordination of classifications and the administration of their metadata.

8) For the Data Protection Inspectorate, RIHA will be a support system for the supervision of personal data.

The responsibility for the use and development of RIHA is assigned to the Estonian Informatics Centre.

3.6 Support systems for the maintenance of databases

Support systems for the maintenance of state information systems ensure their horizontal interoperability. There are currently five support systems:
- the classification system;
- the system of security measures for information systems;
- the system of address details;
- the data exchange layer of information systems;
- the geodetic system.

3.6.1   Classifications system

In order to understand, process and categorise data in information systems in a standardised way, data have to be classified and tagged. The use of classifications facilitates the unification of data, enables the information exchange between information systems (data providers and data receivers), and allows the comparison and analysis of the published data.

To ensure correct functioning of classification systems, their establishment and administration are supervised by a co-ordinating agency (the Statistical Office). Use of established classifications is mandatory for all central and local government information systems.

3.6.2   System of address details

The system of address details is a set of common principles, which ensures a unique identification of address objects both in their location and in different information systems and allows the comparison of addresses submitted at different times and on different principles.

The system of address details consists of:
- information systems that process and handle address details;
- requirements for chief processors of address details, for the respective services and users;
- address services.

The processors of address details include:
- the Land Board insofar as regards objects to be entered into maps defined in the Land Cadastre Act and to which location addresses are assigned pursuant to legislation;
- the Ministry of Economic Affairs and Communications insofar as regards constructions;
- the Ministry of Interior insofar as regards place names;
- the Road Administration insofar as regards national roads;
- the National Heritage Board regarding cultural monuments that are not constructions.

Address services and requirements for their use are the following:
- an address service is any activity associated with address details, such as the identification of the location of an address object, finding address objects in a certain administrative area, entering addresses into databases, as well as changing them according to rules imposed by the chief processor of address details;
- address services are realised as X-Road services;
- X-Road normalisation services are used for the normalisation of addresses;
- a normaliser of location addresses is a software tool facilitating the mutual integration of location addresses by enabling to correct spelling mistakes, to standardise abbreviations, as well as to check the existence of the entered address and correspondence to its description;
- in order to use address services, information systems or databases of an agency have to be joined with the X-Road; individuals are identified via the Citizen Portal;
- in line with the mandate of an agency, its information systems use address services either via the X-road or download the XML-formatted address details into their own information system.

3.6.3 X-Road – data exchange layer of information systems

X-Road allows information systems to use the common data exchange environment as well as the common set of interfaces and common authentication system. Joining an information system with X-Road allows to save up resources and to considerably increase the efficiency of data exchange both among state agencies and in the communication between the citizen and the state.

3.6.4 Geodetic system

The geodetic system consists of:
- the geodetic reference system;
- the system of plane rectangular coordinates;
- the height system;
- the gravimetric system.

The implementation of the geodetic system is based on the following principles:

1) The geodetic system is used for carrying out geodetic, gravimetric and cartographic work in case these data are entered into central and local government databases. In the maintenance of central and local government databases plane rectangular coordinates L-EST97 are used. EUREF-EST97 coordinates, BK77 heights and the values of GV-EST95 gravity acceleration are entered into central and local government databases as appropriate.

2) The implementation of the geodetic system does not extend to thematic maps and databases that are maintained on the basis of international agreements.

3) Coordinates maintained in databases on the basis of international agreements must be available for domestic use as L-EST97 plane rectangular coordinates.

4) Persons who maintain central and local government databases determine, in co-operation with the Land Board, parameters between coordinates of the hitherto used coordination systems and the L-EST97 ones.

3.6.5 System of security measures for information systems

The objective of the system of security measures for information systems is to define an unequivocal procedure for the specification of security measures for information systems; procedure for determining, pursuant to security requirements, security classes; and procedure for the selection of security measures according to security classes.

On the basis of a security analysis of an information system and taking into account the composition of data to be processed, security sub-classes are determined. In doing this, the security objective of data requiring the highest protection is taken into account. To indicate a security class, a letter referring to the respective data security objective and to the number of security level is used. The division of security classes is based on the following elements: data integrity (T – protection of data against falsification or unauthorised alteration of data and the ability to verify the data source), confidentiality (S – the availability of data only to authorised persons), time criticality of data (K – time within which data must become available once a need for them has arisen, i.e. their later availability will be of no importance), severity of consequences of delay (R – potential estimated damage caused by delay of data). The identification mark of a security class is formed of security sub-class identifiers in the following order: R-K-T-S (e.g. a concrete security class may look as follows: R1K2T3S1).

The selection of security measures according to security classes is carried out on the basis of ISKE (a three-stage standard security system for information systems) implementation guide. The Estonian Informatics Centre is responsible for the updating of standard security measures.

4 Organisational interoperability

In the context of information systems, organisational interoperability means the ability of organisations to provide, by using information systems, services to each other as well as to the wider public.

Organisational interoperability is based on the following principles:

- All interoperable institutions are autonomous organisations with a specific technological architecture.
- All connections between institutions are based on multilateral agreements; if possible, bilateral agreements are avoided.
- Private sector bodies and non-governmental organisations participating in the state interoperability framework own the information and/or data they create or obtain. Data in the state information system is owned by the state. Responsibility for the structure and content of data lies with an organisation administrating the respective data either as a chief or an authorised processor of data.
- In data exchange, legal restrictions as well as organisational capacities are taken into account.
- Interoperable institutions exchange information by user authorisation.
- Each institution determines access restrictions within its own information system. The use of nested services is agreed on between institutions.

4.1 State-level coordination of information systems

The non-hierarchic coordination system in Estonia ensures that necessary decisions can be made as close to the level where they occur as possible. The coordination of state information systems in Estonia is described on the scheme below.
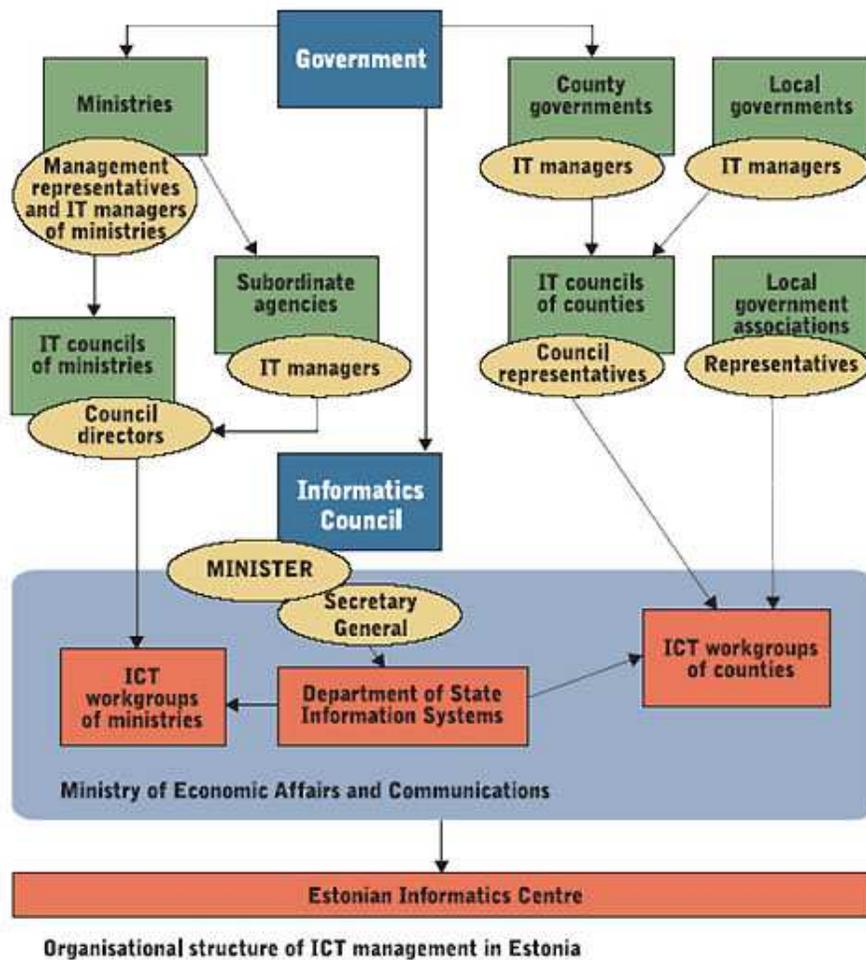
Figure 3. Coordination of the state information system

Pursuant to the Government of the Republic Act, coordination of information systems as well as elaboration and implementation of economic policy in the field of informatics are assigned to the Ministry of Economic Affairs and Communications. The implementation of the information policy is based on annual information policy action plans, which state responsible authorities, measurable performance indicators, and evaluation of finances.

The responsibility for the implementation of the information policy lies with the Department of State Information Systems (RISO) of the Ministry of Economic Affairs and Communications together with the implementing agency under its jurisdiction – the Estonian Informatics Centre (RIA). RISO is responsible for the policy formulation, while it is RIA's task to ensure the implementation of the policy. In order to determine the responsibilities of different institutions for various initiatives, an overview is given below about concrete fields of responsibility in different organisational units.

4.2 Sectoral information systems

In accordance with the principle of subsidiarity, sectoral information systems are developed and administered independently by ministries and agencies in their field of administration. Responsibility for different fields of actions is divided between various state institutions:

Development of information society (Ministry of Economic Affairs and Communications): developing and implementing activities in accordance with information society.

Education, research and development (Ministry of Education and Research, Ministry of Economic Affairs and Communications): extensive training for the population will be increased so as to ensure their coping in the information society and guarantee readiness for making use of IT solutions.

Enterprise development (Ministry of Economic Affairs and Communications): promotion of pre-conditions necessary for the development of eBusiness.

Culture (Ministry of Culture, State Chancellery): development of a national database (eCulture) that would allow the integration of national information resources and the development of information services; development of digital archives; collecting digital information of archival value; digitisation of records as cultural heritage.

Health care (Ministry of Social Affairs): development of the eHealth project; modernisation of the health care system by implementing modern IT solutions.

Environment and spatial data (Ministry of Environment): aggregation of environmental data into a general national register; processing information related to land and geographic location, issuing guidance for the performance of public sector activities in the field of geoinformatics.

State and local government administration:
- State Chancellery is responsible for the modernisation of electronic document management and development of digital archiving in the public sector;
- National Electoral Committee is responsible for the development of eDemocracy;
- Ministry of Interior is responsible for increasing administrative capacity as well as for the development of Police and Border Guard information systems;
- Ministry of Finance is accountable for the readiness of IT systems for the administration of the EU structural funds, and for the development of the eTax and eCustoms Board;
- Ministry of Foreign Affairs is responsible for promoting Estonia in the world by using modern IT solutions.

In ministries, the development of information systems is co-ordinated by a ministries' IT councils, which make proposals to their IT development strategies and, proceeding form the information policy and respective action plans, drafts measures for their implementation. IT councils are formed by directives of ministers, while the council's work format (its members, frequency of its meetings etc) are left to its own discretion.

At regional level, ICT development is coordinated by IT councils established at county governors' offices. County IT councils organise the elaboration of county IT strategies and, proceeding from the information policy and respective action plans, draft measures for their implementation.

5 Technical interoperability

5.1 Objectives

The state IT architecture must meet the following objectives:

Preservation of data in one place
Data are preserved only in a database, where they serve as basic data. Availability requirements may lead to the copying of data, but in this case it has to be taken into account that data may be outdated.

Linking business processes via nested services
Information systems communicate with each other via nested services. If for the performance of a business process in one agency data is needed from or workflow has to be carried out in another agency, nested services are made use of. Agencies must ensure that the data and services it offers could be used as nested services. For instance, one should avoid a situation, where a document is printed out in one agency, delivered to another agency by post, and then once again scanned into the computer.

Ensuring the availability of nested services
In situations, where service user's requirements for the availability of a service are stricter than those of the service provider, the latter should increase service availability. In case this proves impossible, other solutions can be considered while taking into account legal aspects.

Avoiding „*single point of failure*"
Solutions, where the break-down of one part of the system may disrupt the functioning of the whole system, are to be avoided.

Security
Solutions used in the state information system have to be secure and ensure confidentiality, authenticity, availability and provability of data.

Open standards
When choosing IT solutions, those based on open standards have to be given preference.

Person's right to access data about himself
Each person has the right to access data that has been collected about him to information systems. In addition, everybody should be entitled to obtain information about inquiries made by other persons about them unless this has been restricted by law.

Single-point entry to services
Central and local government agencies co-operate in order to ensure that citizens, officials and entrepreneurs could obtain all the information and services they need from the following state central portals: http://www.riik.ee, http://www.eesti.ee and https://www.eesti.ee.

5.2 State IT architecture

In the elaboration of the state IT architecture, principles of Service Oriented Architecture (SOA) have to be followed.

In case of service oriented architecture, different systems provide diverse information services through the so-called "service interfaces", which can be used by other information systems. Descriptions of these interfaces have to contain sufficient information for the identification and use of a service without the need for the service-using system to "know" anything about the internal architecture, platform etc of the service-providing system.

In case of SOA, the service publisher and the actual service provider do not necessarily have to be the same, while from the point of view of the service user, this does not make any difference.

There are no restrictions as to technologies to be used for the application of SOA.

The cornerstones of the state IT architecture are the following:
- technical interoperability,
- security,
- openness,
- flexibility,
- scalability.

The efficient functioning of state agencies as well as the provision of quality services for citizens presumes the availability of high-quality information. Information is created as a result of certain events in the course of certain processes and it is preserved in state registers and information systems.

There are hundreds of information systems and registers in the state. According to one of the basic principles of the information society, information that has been created in state information systems has to be freely available for all authorised persons in order to ensure free flow of information. Information may be needed by citizens, agencies and entrepreneurs alike.

It is the state's task to ensure the availability of high-quality information and guarantee the existence of a data exchange environment enabling access to information.

It is not expedient for the state to fix a detailed architecture for the state information system. The general architecture of and requirements for nationwide information systems have been fixed in the document called „The Estonian IT Architecture", which forms a part of the state's interoperability framework.

6 Semantic interoperability

6.1 Definition of semantic interoperability

Semantic interoperability refers to the capability of information systems to adequately use data received from other information systems. Semantic interoperability is complicated by the fact that use of software systems, their objectives, as well as contexts differ, leading thus to differences in ways of presentation, coding and shades of meaning.

Semantic interoperability cannot be achieved by establishing similar requirements and standards for all software systems, as this would be neither realistic nor reasonable. Achieving semantic interoperability should be approached as a task to facilitate the work of software engineers and developers, who have to build interfaces with other software systems.

Reaching semantic interoperability is, to a great extent, a matter of organisational, social and educational nature: first of all, support is needed for system specialists in order to better understand each other's fields of activities, to compile sound documentation of data structures and protocols, and to facilitate the search of such documentation.

In order to publish data stored in them, information systems use various tools, beginning from languages, dictionaries, classifications, and rules until complex ontologies. Similarly to software and hardware of an information system, we can also speak of its semantic assets.

A more profound treatment of issues related to semantic interoperability has been given in a document called „The semantic interoperability of the state information system."

6.2 Semantic interoperability assets

The semantic interoperability assets are divided into syntactic assets and semantic assets. In order to ensure semantic interoperability between two information systems, a semantic gateway has to be established between them. Semantic gateway has to ensure semantic alterations leading to adequate use of each other's data between information systems. The semantic gateway of a state information system is a set of multilateral agreements and rules that facilitates the mutual linking of systems on the semantic level.

Syntactic interoperability assets include XML schemas, metadata schemas, and core components. Principles need to be fixed on state level for the publication of data-schemas and for the definitions of metadata. The syntactic level of interoperability is the first stage in achieving semantic interoperability and it can be achieved by creating repositories for XML schemas.

Semantic assets of semantic interoperability denote information resources that have been created in order to ensure the interoperability of information systems. Semantic assets of semantic interoperability are divided as follows (the division is based on the IDABC working paper „IDABC Content Interoperability Strategy"):
- dictionaries,
- thesauri,
- nomenclatures,
- taxonomies,
- mapping tables,

- ontologies,
- service registers.

6.3   Organisation responsible for ensuring semantic interoperability

Semantic interoperability depends primarily on high-quality documentation of databases, services, applications and areas. The main objective of an organisation ensuring semantic interoperability is to co-ordinate the development and regular updating of such documentation. Semantic interoperability can be improved by elaboration of standards, dictionaries, thesauri and nomenclatures. At the same time, references to these semantic assets can be made in the legislation; if necessary, their use can be made mandatory.

The development of an organisation responsible for ensuring semantic interoperability of the state information system should be based on the following principles:

- The role of the central co-ordinator should be assigned to the State Information Systems Department of the Ministry of Economic Affairs and Communications of Estonia, the staff of which should be increased by a semantic interoperability architect.
- In all major areas expert groups should be formed with a task of drawing up, upgrading and changing the documentation of the respective sector. Since these major areas more or less coincide with the fields of administrations of ministries, it would be expedient to establish expert groups in all ministries, assigning them the task of compiling and maintaining respective dictionary-documents.
- In case mutual agreements will not be sufficient for achieving semantic interoperability, cross-sectoral working groups should be formed. The aim of such groups should be to create and maintain instructions on the translation/modification of data objects of one area into those of another area.
- On the international arena, Estonia would benefit from participation in the work of IDABC semantic interoperability working groups, which aim at elaborating mutual agreements and semantic gateways for the semantic interoperability between information systems of different countries. For the realisation of projects that aim at the creation of connections with information systems in another country, bilateral expert groups representing both parties will be established.

6.4   Architectural requirements for semantic interoperability

In planning the system architecture, the following guidelines should be taken into account in order to facilitate semantic interoperability:

- for data exchange, XML format is used over http or https protocol;
- the XML format used should be easy to understand and not to contain excessive noise: unnecessary tags and details;
- the XML format used must be documented in an easily understandable manner for developers;
- the presentation layer should be realised as a separate application that communicates with the main application via XML texts and generates the HTML necessary for the user or realises the interface in some other way (WAP, SMS, desktop applications etc);
- direct generation of HTML text that does not support adaptable semantics from the main application has to be avoided.

7. Infrastructure requirements for state IT interoperability

Infrastructure refers to hardware, software and network resources that support the mutual communication between people and organisations, access to information systems, and use of services.

The basic principles of the development and maintenance of infrastructure are the following:
- The primary responsibility for the development, application and maintenance of the state information infrastructure lies with the private sector.
- In maintaining its infrastructure, the public sector proceeds from the principle of subsidiarity, according to which all state agencies are responsible for the development of the infrastructure of their own information systems, while considering also the general principles of the state IT interoperability framework.
- The public sector encourages the private sector to invest and participate in the development and maintenance of state infrastructure.
- In the provision of infrastructure services, the state fosters and protects free competition.
- The state ensures free access to its infrastructure both for service providers and service users.
- The state information infrastructure forms a part of the global information infrastructure.

Centrally developed infrastructure

In order to ensure interoperability of public sector information systems, the public sector assumes responsibility for the development and maintenance of several infrastructure components. The responsibility for the co-ordination of these components is assigned to a ministry responsible for the co-ordination of state information systems, while infrastructure development is, as a general rule, outsourced from the private sector. The functioning of central infrastructure systems is ensured either by state agencies or by outsourcing respective services from the private sector. The use of central components is mandatory for public sector agencies. The central components are the following:
- the data exchange layer X-Road;
- the interoperability layer of geoinformation systems;
- the interoperability layer of document management systems;
- the infrastructure ensuring the interoperability of websites maintained by public sector agencies, the state portal www.riik.ee, as well as the domain riik.ee;
- the infrastructure ensuring the interoperability of thematic portals as well as the information portal www.eesti.ee;
- the layer of interoperable personalised portals (citizen portal(s), entrepreneur portal(s), civil servant(s) portals);
- the system of classifications;
- the system of address details;
- the administrative system for the state information system;
- the security system;
- the geodetic system.

Central consolidation

In developing their infrastructure, public sector agencies co-operate with each other. Use of infrastructure components acquired through central consolidation is not obligatory for them. Partial central support is given to the following activities:
- joint procurements of software licences;
- consolidated purchasing of external internet connections and the development of backbone network for state agencies (partly usable also by local governments);
- limited web hosting of domains riik.ee, gov.ee, eesti.ee and estonia.ee.

Infrastructure outsourced from the private sector

In the acquisition of infrastructure, public sector agencies have to co-operate with each other. Assistance for the development of their infrastructure can be obtained from the Estonian Informatics Centre under the administration of the Ministry of Economic Affairs. Private sector services are used for the following components of infrastructure:

- Acquisition of software. State agencies are encouraged to co-operate in software acquisition.
- Acquisition of system software. State agencies are encouraged to co-operate in the acquisition of software systems.
- Development of services related to public key infrastructure.
- Establishment of development environments. Public sector agencies should not develop their own development tools or development environments. They are encouraged to co-operate with each other in order to ensure their interoperability.
- Hosting services. Public sector agencies are encouraged to co-operate in the outsourcing of hosting services from the private sector.
- Back-up services. Public sector agencies are encouraged to co-operate in outsourcing back-up services from the private sector.

The division of roles in the development of state infrastructure is as follows:

- the state plans the general development of IT systems, establishes requirements with regard to IT systems for state agencies, co-ordinates co-operation between state agencies in the field of IT systems, and performs the role of the supervisor;
- private companies design specific objects or IT systems and provide consultancy for state IT specialists;
- private companies carry out state's orders, and develop and maintain the state infrastructure, while the state is not the owner of the technology necessary for the functioning of the components of its infrastructure.