Plamen Vatchkov • Kamen Spassov
Roumen Trifonov • Slavcho Manolov
Radoslav Yoshinov • Lyubomir Blagoev

INTEROPERABILITY IN ELECTRONIC GOVERNMENT APPLICATIONS

PLAMEN VATCHKOV • KAMEN SPASSOV
ROUMEN TRIFONOV • SLAVCHO MANOLOV
RADOSLAV YOSHINOV • LYUBOMIR BLAGOEV

INTEROPERABILITY IN ELECTRONIC GOVERNMENT APPLICATIONS

INTEROPERABILITY IN ELECTRONIC GOVERNMENT APPLICATIONS

ISBN 978-619-160-456-2
Avangard Prima Publisher
Sofia 2015

This book is intended for the students at the Sofia University and the Technical University of Sofia. It is also addressed to all IT professionals, computer and software engineers, undergraduate, graduate and PhD. students in mathematics and informatics, computer science, computer systems and technologies, computer and software engineering, e-governance specialization and information technology.

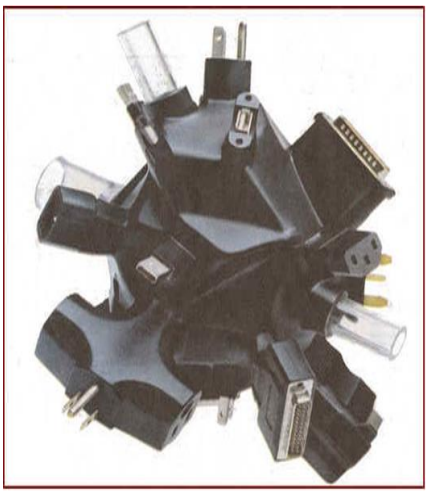
CONTENTS

INTEROPERABILITY 1
IN ELECTRONIC GOVERNMENT APPLICATIONS 1
PART 1 7
TERMINOLOGY, GENERAL CONCEPTS 7
PART 2 13
EUROPEAN ASPECTS 13
CHAPTER 2.1 13
LEGAL REGULATION AND STANDARDIZATION OF INTEROPERABILITY 13
CHAPTER 2.2 29
EUROPEAN STRATEGY, FRAMEWORK AND ARCHITECTURE OF INTEROPERABILITY 29
CHAPTER 2.3 46
INTEROPERABILITY ASPECTS 46
CHAPTER 2.4 68
EUROPEAN INITIATIVES 68
PART 3 86
NATIONAL ASPECTS 86
CHAPTER 3.1 86
NATIONAL INTEROPERABILITY FRAMEWORK 86
CHAPTER 3.2 103
REQUIREMENTS OF THE E-GOVERNANCE ACT AND ORDINANCES 103
CHAPTER 3.3 114
REALIZATION 114
3.3.1 STANDARDIZATION 115
3.3.2 NATIONAL DATA MODEL REGISTERS 125
3.3.3 UNIFORM ENVIRONMENT FOR E-DOCUMENTS EXCHANGE 138
3.3.4 THE ADMINISTRATIVE INFORMATION SYSTEM AS A CORE SYSTEM 143
3.3.5 COMPLIANCE VERIFICATION 150
REFERENCES 153

PART 1

TERMINOLOGY, GENERAL CONCEPTS

Fundamental nature of Interoperability



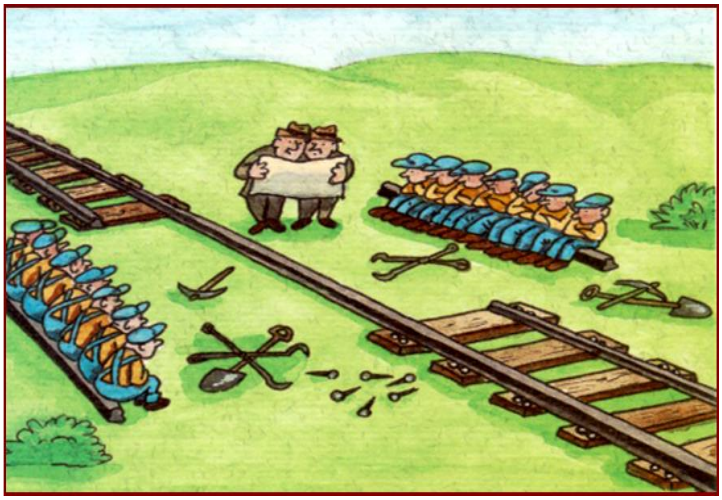


Figure 1-1

First of all, the vision of the concept of "interoperability" in our course – obviously, we mean information-related interoperability. This leaves out predominantly physical and mechanical aspects of interoperability, such as connectors for cabling, electric sockets, screws and threads etc.

Among the many modifications of the information-related interoperability we will focus on the interoperability of applications related to the e-Government (strictly speaking, e-Governance).

At the same time, however, we should not be confined to the technical aspects of interoperability. The area of our activities should include interoperability of legislation, organizational availability, business process model compatibility, skill capabilities of potential users, etc.

Interoperability can be defined from different point of view. The table below provides examples of some general definitions.

Focus of a definition	Definition
Definition from the field of engineering of technical systems	The capability to communicate, execute programs, or transfer data among various functional units in a manner that requires the user to have little or no knowledge of the unique characteristics of those units
Definition specifying the nature of systems and components exchanging and using information	Interoperability is the ability of two or more systems or components to exchange information and to use the information that has been exchanged
Definition including a concept of "process"	Interoperability is the ability of a system or process to use information and/or functionality of another system or process by adhering to common standards
Definition specifying the nature of a process and a system	Interoperability means the ability of ICT systems and of the business processes they support to exchange data and to enable information and knowledge to be shared
Definition specifying interoperability levels	Interoperability is the ability of systems and machines to exchange, process and correctly interpret information. It is more than just a technical challenge, as it also involves legal, organizational and semantic aspects of handling data

Table 1-1

The definitions considered allow inferring of main general characteristics of interoperability:

- it is the ability of ICT systems and business processes they support;
- the ability is related to exchange, processing, correct interpretation, use, and sharing of information;
- it involves technical, legal, organizational, and semantic aspects of handling data;

- manipulations with information adhere common standards.

The MODINIS program defines interoperability in the context of e-Government and specifies that ICT systems and business processes belong to public authorities, as well as points out a reason for exchanging of information. Therefore, interoperability is the ability of public authorities' ICT systems and business processes to share information and knowledge within and across organizational boundaries in order to better support the provision of public services as well as to strengthen support to public policies and to democratic processes

Therefore, interoperability in the context of e-Government is characterized in the following way:

- it is the ability of disparate and diverse organizations to interact;
- the interaction is needed for achievement of mutually beneficial and agreed common goals;
- the interaction involves sharing of information and knowledge between the organizations;
- the sharing occurs through the business processes of the organizations;
- the sharing occurs by means of the exchange, process, and correct interpretation of data between ICT systems used in the organizations;
- the interaction can happen between organizations of different levels: national, European, sectorial, etc.

We consider that the European Commission's definition of interoperability, announced in the "European Interoperability Framework for European public services" as follows:

- "interoperability is the capability of the information systems and the business processes they are supporting to exchange data and to integrate information and knowledge",
- is not fully adequate for all purpose.

It is advisable to adhere to more broad definition, which includes the human, the social and the organizational factors.

The good example is the definition of the Australian Government:

"Interoperability is not just a technical matter of connecting computer networks. It also embraces the sharing of information between networks and the re-design of business processes to deliver improved outcomes and efficiencies and to support the seamless delivery of electronic services.

Interoperability is an important element in the delivery of e-Service and integration initiatives. Within this context, it should be understood that:

• interoperability is not an end in itself, but an enabling capability;

• while standards are necessary, they are not sufficient for interoperability;

• an understanding of the business, social, political and cultural context of the organizations is essential;

• to be interoperable, an organization must actively engage in the ongoing process of ensuring that its systems, processes and people are managed in a way which maximizes opportunities for internal and external exchange and re-use of Information;

• organizational boundaries should not stand in the way of the right people having access to the right information to make informed decisions or to provide high quality service.".

Aspects of interoperability

Interoperability has 3 main aspects – organizational, semantic, and technical - which must be taken into account when developing a public service.

The organizational aspect of interoperability arises from differences in business processes and internal structures of organizations which are involved in the establishment and provision of public services and need to collaborate towards mutually beneficial and agreed European public service-related goals. Therefore, the aim of achieving organizational interoperability is to overcome all organizational obstacles, thus being able to set up the relevant intra- and inter-organizational workflows. In practice, organizational interoperability implies integrating business processes and related data exchange. Organizational interoperability also aims to meet the requirements of the user community by making services available, easily identifiable, accessible, and user-focused.

The semantic aspect of interoperability comes from different linguistic, cultural, legal, and administrative environments in the Member States in particular and multilingualism in the EU in general1. The main semantic conflicts are related to the structure of data and the meaning of data, for example, different values are used for the same entity (e.g. the value "foreigner" in one database may mean that the person is not a citizen of the country, while in another database it may mean that the person is not a citizen of the EU), different format for representation of the same data (e.g. data), different measuring units (e.g. centimeters in one database and in inches in another), etc.

Therefore, semantic interoperability is about managing of all semantic conflicts among different systems in a fully automated manner and possibility to add new systems or remove existent one at any time. Semantic interoperability enables organizations to process information from external sources in a meaningful manner and ensures understanding and preservation of the precise meaning of exchanged information. Resolving semantic conflicts can be achieved by using an agreed knowledge representation language. In other words, it is necessary to elaborate common taxonomy, dictionary of used terms or a catalog of inclusive proper data, which further will be made available to information systems.

The technical aspect of interoperability is related to ability of exchanging information between heterogeneous IT networks, applications, and theirs components. Technical interoperability is concerned with all technical issues (technologies, standards, policies) to guarantee that the technical components of the information systems of the collaborating authorities will be able to work together7. Therefore, technical interoperability covers the technical aspects of linking information systems1. It should be noted that technical interoperability is concerned not only with technologies at the physical connection layer (such as network protocols), but also with technologies that support the organizational and the semantic layers. It includes aspects such as interface specifications, interconnection services, data integration services, data presentation and exchange, etc. It is the most obvious aspect of interoperability because computer systems are built and developed with utilization of engineering technique and for every technical problem is possible to find a proper solution.

Benefits and beneficiaries of interoperability

Interoperability is both a prerequisite for and a facilitator of efficient delivery of European public services. Animation illustrates the impact of achieved interoperability. Therefore, the interoperability addresses the need for:

- cooperation among public administrations, to establish public services;
- exchanging information among public administrations to fulfill legal requirements or political commitments;
- sharing and reusing information among public administrations to increase administrative efficiency and cut 'red type' for citizens and businesses.

The results are:

- improved public service delivery to citizens and businesses, by facilitating the 'one-stop-shop' delivery of public services;
- lower costs for public administrations, businesses and citizens due to the efficient delivery of public services.

In the framework of the MODINIS program, the following five different settings in which the advantages of interoperable ICT systems are evident were identified:

- between different services referring to the same customer, namely bundling services (e.g. according to life events or problem scenarios) to save resources or to improve service quality (one-stop government);
- between different stages of a supply chain that is producing one or more services, namely when a single service cannot be produced completely by one single agency, there is a need for interoperability between data and workflow contributions from other agencies/ back offices;
- between single agencies in different geographical areas, namely interoperability referring to the direct data transfer from the system of one administration to the system of another administration (mainly geographical);
- between directories of services or documents, namely interoperability between local directories, common metadata about the services as well as algorithms for locating the right agency. One crucial issue concerns common descriptors for services and agencies;
- in auxiliary services (identity management, digital signature, etc.).

The next table summarizes the main beneficiaries of interoperability and advantages they receive from interoperable public services.

Beneficiary	Advantage
Public administrations of member states and European Commission services	- gain in efficiency when establishing European public services; - greater awareness of the risk of creating new e-barriers if they opt for public services solutions that are not interoperable at European Union level; - cooperation which facilitates the exchange, sharing, and reuse of information.
Citizens and businesses	- efficient and effective delivery of public services to citizens and enterprises across borders and sectors; - reducing costs; - preventing duplication of efforts; - reducing the administrative burden.
EU as a whole	- contribution to the achievement of the Lisbon goal of making Europe the most dynamic and competitive, knowledge-based economy by improving citizens' quality of life and by reducing administrative burden on enterprises; - more efficient implementation of European Union policies and initiatives; - fostering the enhancement of the common market via the four freedoms; - support of the economic integration of the countries and the consolidation of the internal market.

Table 1-2

PART 2

EUROPEAN ASPECTS

CHAPTER 2.1

LEGAL REGULATION AND STANDARDIZATION OF INTEROPERABILITY

Interoperability barriers

There are numerous obstacles that can hinder progress towards realizing the concept of e-Government, as has been recognized within the EU through various related Directives, communications and research initiatives. Substantial legal, political, administrative, social, institutional and cultural differences between Member States and regions in the EU make such understanding of the main impediments to e-Government of particular relevance to the growing number of important public services in the EU that seek to span national and regional boundaries (e.g. e-Procurement for cross border public tenders and support for employment mobility). New initiatives are also often needed when rapid technologically-enabled change creates problems.

There are seven main categories of barriers that can block or constrain progress on e-Government:

1. Leadership failures - slow and patchy progress to e-Government can result from a lack of adequate leadership during any stage in the initiation, implementation, promotion and ongoing support of developments.

2. Financial inhibitors – inappropriate cost/benefit analyses can fail to release the flow of investment at the levels necessary to support future e-Government innovation.

3. Digital divides - inequalities in skills, access to appropriate systems, knowledge and motivational support can limit and fragment take-up of e-Government.

4. Poor coordination - lack of coordination and harmonization can put a brake on establishing appropriate e-Government networks and services that cross governance, administrative and geographic boundaries.

5. Workplace and organizational inflexibility - the wide realization of e-Government benefits can be constrained or blocked by inflexibilities in responding to the need to make necessary changes in public administration practices, processes and organizational structures to allow them to be better able to make appropriate effective use of electronic networking capabilities and their facilitation of more sharing of information and service provision.

6. Lack of trust - heightened fears about inadequate security and privacy safeguards in electronic networks can undermine confidence in applications of e-Government that might pose risks, such as through unwarranted access to sensitive personal information or vulnerability to online fraud or identity theft.

7. Poor technical design - interoperability blockages caused by incompatibilities between ICT systems or difficult-to-use interfaces to e-Government services exemplify the kinds of practical flaws that can become serious operational obstacles to take-up of what otherwise appear to be valuable e-Government systems.

Legal dimensions of the main barrier categories highlight how laws and regulations are core foundations for building policies affecting e-Government within and between European, Member State and regional levels.

For example, EC Directives relating to e-Government include:

- Directive 1999/93/EC on electronic signatures;
- Directive 2001/29/EC on the harmonization of certain aspects of copyright and related rights in the information society and
- Directive 2002/58/EC on privacy and electronic communications.

Eight key legal dimensions are provided:

- Administrative law;
- Authentication and identification;
- Intellectual Property Rights;
- Liability;
- Privacy and data protection;
- Public administration transparency;
- Relationships between public administrations, citizens and other ICT actors and
- Re-use of public sector information.

Barriers: Legal area:	Leadership failures	Financial inhibitors	Digital Divides	Poor coordination	Workplace and organizational inflexibility	Lack of trust	Poor technical design
Administrative Law							
Authentication and Identification							
IPR							
Liability							
Privacy and Data Protection							
Public Administration Transparency							
Relationships							
Re-use of Public Sector Information							

Figure 2-1

Legal regulations of interoperability

Development of any European public service needs to take into account the current EU and national legislation concerning interoperability and e-Government. Since the first effort on interoperability at the end of 90s, the legal base is growing each year. Moreover, a lot of initiatives and events are related to interoperability issues and aspects.

The following documents made the legal European framework for interoperability:

- "Towards interoperability for European public services", COM(2010) 744, 16.12.2010. The document contains the approved European Interoperability Strategy and the European Interoperability Framework as its annexes;

- "Decision 922/2009/EC on interoperability solutions for European public administrations (ISA), 16.09.2009". It adopts the ISA program (ec.europa.eu/isa/), which focuses on back-office solutions supporting the interaction between European public administrations and the implementation of Community policies and activities in the area of interoperability;

- "Directive 2007/2/EC on establishing an Infrastructure for Spatial Information in the European Community (INSPIRE), 14.03.2007". Regarding the environment, the directive establishes an infrastructure for spatial information in Europe for the purposes of EU environmental policies and policies or activities which may have an impact on the environment. To ensure that the spatial data infrastructures of the Member States are compatible and usable in a Community and trans-boundary context, the directive requires that common implementing rules are adopted in a number of specific areas (Metadata, Data Specifications, Network Services, Data and Service Sharing and Monitoring and Reporting).

- "Directive 2006/123/EC on services in the internal market, 12.12.2006". Regarding the internal market, the directive obliges Member States to offer service providers the possibility of completing electronically and across borders all procedures and formalities needed to provide a service outside their home country. It calls on Member States to establish single contact points to help service-providers enter their markets. It requires all procedures involved in establishing a business and providing services in another EU country to be fully online;

- "Interoperability for pan-European e-Government services", COM(2006) 45, 13.02.2006. The document sets out the basic requirements for implementing pan-European interoperability of e-Government services, outlines priorities in a structured set of policies and measures for achieving interoperability of e-Government services in the pan-European context and proposes further action as first steps to fill in this framework;

- "Ministerial Declaration on e-Government", 18.11.2009. The Ministers recognized that better public services need to be delivered with fewer resources, and that the potential of e-Government can be increased by promoting a common culture of collaboration and by improving the conditions for interoperability of administrations. One of the policy priorities, to be achieved by 2015 is - the implementation of the policy priorities is made possible by appropriate key enablers and legal and technical preconditions. There, it is pointed out that Public administrations should: - pay particular attention to the benefits resulting from the use of open specifications in order to deliver services in the most cost-effective manner; - regard innovation as an integral part of working. The Ministers took responsibility to promote innovation in e-Government services through research and development, pilot projects and other implementation schemes, to explore and develop the possibilities offered by new open and flexible service architectures.

"Granada Ministerial Declaration on the European Digital Agenda, 19.04.2010". In the declaration, the action related to advanced use of the open internet, security and trust and especially increase the strength of a smart, sustainable and inclusive European Digital Economy

by promoting inter alia smart and open public services such as e-Health and e-Government is mentioned.

In relation to public digital services the following actions are specified:

- respond to the Malmo Declaration on e-Government by developing more effective and efficient interoperable public services;
- ensure the implementation of e-Government strategies at an organisational, legal and technical level including e-ID and e-signatures;
- embed innovation and cost effectiveness into e-Government through the systematic promotion of open standards and interoperable systems, development of EU wide e-Authentication schemes and proactive development of e-Invoicing, e-Procurement (and pre-commercial procurement).

A number of other official documents, events, and initiatives are relevant in the context of interoperability of e[Government. They are displayed in the figure below and specified in chronological sequence.

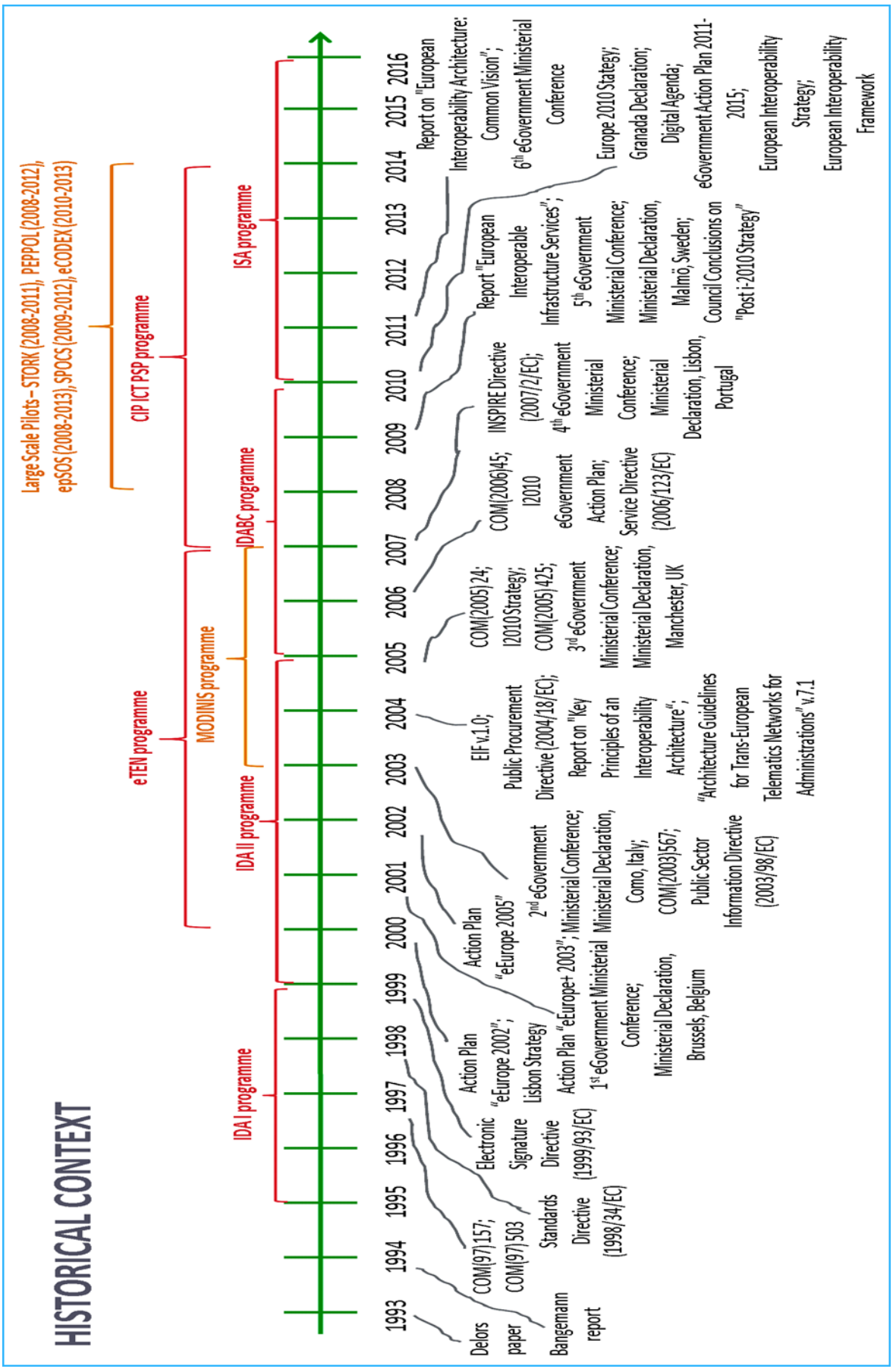

HISTORICAL CONTEXT
Large Scale Pilots – STORK (2008-2011), PEPPOL (2008-2012),
epSOS (2008-2013), SPOCS (2009-2012), eCODEX (2010-2013)
CIP ICT PSP programme
eTEN programme
MODINIS programme
IDA I programme
IDA II programme
IDABC programme
ISA programme
1993 1994 1995 1996 1997 1998 1999 2000 2001 2002 2003 2004 2005 2006 2007 2008 2009 2010 2011 2012 2013 2014 2015 2016
Delors paper
Bangemann report
COM(97)157; COM(97)503
Electronic Signature Directive (1999/93/EC)
Standards Directive (1998/34/EC)
Action Plan "eEurope 2002"; Lisbon Strategy
Action Plan "eEurope+ 2003"; 1st eGovernment Ministerial Conference; Ministerial Declaration, Brussels, Belgium
Ministerial Declaration, Como, Italy; COM(2003)567; Public Sector Information Directive (2003/98/EC)
Action Plan "eEurope 2005"
2nd eGovernment
EIF-v.1.0; Public Procurement Directive (2004/18/EC); Report on "Key Principles of an Interoperability Architecture"; "Architecture Guidelines for Trans-European Telematics Networks for Administrations" v.7.1
COM(2005)24; I2010 Strategy; COM(2005)425; 3rd eGovernment Ministerial Conference; Ministerial Declaration, Manchester, UK
COM(2006)45; I2010 eGovernment Action Plan; Service Directive (2006/123/EC)
INSPIRE Directive (2007/2/EC); 4th eGovernment Ministerial Conference; Ministerial Declaration, Lisbon, Portugal
Report "European Interoperable Infrastructure Services"; 5th eGovernment Ministerial Conference; Ministerial Declaration, Malmö, Sweden; Council Conclusions on "Post i-2010 Strategy"
Report on "European Interoperability Architecture: Common Vision"; 6th eGovernment Ministerial Conference
Europe 2010 Stategy; Granada Declaration; Digital Agenda; eGovernment Action Plan 2011-2015; European Interoperability Strategy; European Interoperability Framework

Figure 2-2

General concept of standardization

Standardization is the process of establishing and implementing technical standards, which could be a standard specification, standard test method, standard definition, or standard procedure. Standardization means that there is a standard specification, unit, instruction or something that is understood globally.

The Directive 98/34/EC of the European Commission suggests the following definition: "Standard is a technical specification approved by a recognized standardization body for repeated or continuous application, with which compliance is not compulsory and which is one of the following:

— international standard: a standard adopted by an international standardization organization and made available to the public;

— European standard: a standard adopted by a European standardization body and made available to the public;

— national standard: a standard adopted by a national standardization body and made available to the public."

A technical standard is an established norm or requirement about technical systems. It is usually a formal document that establishes uniform engineering or technical criteria, methods, processes and practices. In contrast, a custom, convention, company product, corporate standard, etc. which becomes generally accepted and dominant is often called a de facto standard.

The major players in the standardization

A technical standard may be developed privately or unilaterally, for example, by a corporation, regulatory body, military, etc. Standards can also be developed by groups such as trade unions and trade associations. Standards organizations often have more diverse input and usually develop voluntary standards: these might become mandatory if adopted by a government, business contract, etc. The standardization process may be by edict or may involve the formal consensus of technical experts.

International standards are standards developed by international standards organizations. They are available for consideration and use worldwide. The three largest and most well-established international standards organizations are the International Organization for Standardization (ISO), the International Electro-technical Commission (IEC), and the International Telecommunication Union (ITU), which have each existed for more than 50 years (founded in 1947, 1906, and 1865, respectively) and which are all based in Geneva, Switzerland. They have established tens of thousands of standards covering almost every conceivable topic. Many of these are then adopted worldwide replacing various incompatible 'homegrown' standards. Many of these standards are naturally evolved from those designed in-house within an industry, or by a particular country, while others have been built from scratch by groups of experts belonging to various technical committees. The mentioned three organizations together comprise the World Standards Cooperation (WSC) alliance.

In addition to the mentioned institutions, a large variety of independent international standards organizations such as the ASME, the ASTM International, the IEEE, the Internet Engineering Task Force (IETF), the World Wide Web Consortium (W3C), etc., develop and publish standards for a variety of international uses. In many such cases, these international standards organizations are not based on the principle of one member per country. Rather,

membership in such organizations is open to those interested in joining and willing to agree to the organization's by-laws – having either organizational/corporate or individual technical experts as members.

In the context of business information exchanges, standardization refers to the process of developing data exchange standards for specific business processes using specific syntaxes. These standards are usually developed in voluntary consensus standards bodies such as the United Nations Centre for Trade Facilitation and Electronic Business (UN/CEFACT), the Telecommunications Industry Association (TIA), and the Organization for the Advancement of Structured Information Standards (OASIS).

While European integration by way of the European Union has made remarkable progress in the last two decades, the process was – as we all know – by no means free of fric-tion. Ten-sions often emerge when the supranational institution and the individual member states clash over ques-tions of authority in a particular domain. Apart from more visible examples such as a common foreign policy or a common constitution, standardization policy can be a contested field of this kind. On the one hand, standardization contributes "in a significant way to the functioning of the single market, the protection of health and safety, the competitiveness of industry and the promotion of international trade, and has been supporting an increasing range of Community policies". To this end, the European Union endorses the work of the three European standards bodies: The Comité Européen de Normalisation (CEN, founded in 1961), the Comité Européen de Normalisation Électrotechnique (CEN-ELEC, founded in 1973), and the European Telecommunications Standards Institute (ETSI, founded in 1988). However, many mem-ber states have since long maintained standards (and standards bodies) of their own and have a vested interest in adhering to these established norms for a variety of reasons – some symbolic and some economic. The unification of the European currency system provides an excellent example for such possible tensions. While the unification process – starting with the implementation of the European Monetary System and the European Exchange Rate Mechanism in 1979 – beyond doubt helped to create a single market, the adoption of a common currency also met national resistance – partly out of fear of economic disadvantages and partly due to the high symbolic value of a national currency.

Relations of standardization to the interoperability

Many reasons explain the introduction of standardization and interoperability concepts. This is the main reason for having standards, as instruments can be tested and integrated in a defined procedure before deployment. It lends itself to the concept of introducing quality management or mission assurance procedures. Using standards make interoperability possible at interchange-ability level but also when dealing with data processing. On top of that schemes of sensor information, metadata would facilitate the interoperability by enabling the integration of different sources of information into a common system.

The standardization processes are expected to generate added value and benefits in an economic context: - enhanced product quality and reliability, reduction in costs, increased efficiency and ease of maintenance, simplify and improve usability, greater compatibility and interoperability of goods and services, improved health, safety and environmental protection.

In order to meet these requirements, it will be essential to get European industrial players involved in the standard definition process with the aim of reaching consensus between the major players from academia, government institutions and industry. Involved actors will be gathered in a group of Providers of Equipment and Services for Observatory Systems (PESOS); their specific objective will be the sharing of best practices and knowledge and the definition of standards for installing and operating systems.

Over the past two decades, standards related to the systems integration and interoperability underwent a remarkable evolutionary process. Its main steps of this process are marked as follows:

1. Information-oriented integration - ability of information systems to access information in applications of other systems. So called "**Format Standards**" correspond to this integration;

2. Process-oriented integration - exchange between applications in the context of process models models and abstractions of process automation. So called "**Orchestration Standards**" correspond to this integration;

3. Portal-oriented integration - visualization of internal processes through aggregated user interface - "**Portal Standards**";

4. Service-oriented integration - not only the transfer of information between applications, but also creation of complex applications from multiple "Back-End" systems - "**Service-oriented Standards**".

Selection of standards related to interoperability

Openness of standards or technical specifications is important for public administrations because of its relationship with interoperability, freedom and choice:

- openness lowers barriers to market entry, thereby widening the field to competition – leading to more choice, better quality and lower prices;
- openness spurs innovation by allowing more talent to contribute ideas and advance the state-of- the-art;
- openness strengthens the position of consumers vis-à-vis their suppliers;
- openness enables consumers to combine off-the-shelf products with custom-built products and turn-key systems;
- openness facilitates interoperability through transparency;
- openness enhances security through transparency;
- openness ensure access to information and services, now and in the future, as it avoids lock-in situations, making such access dependent from specific products.

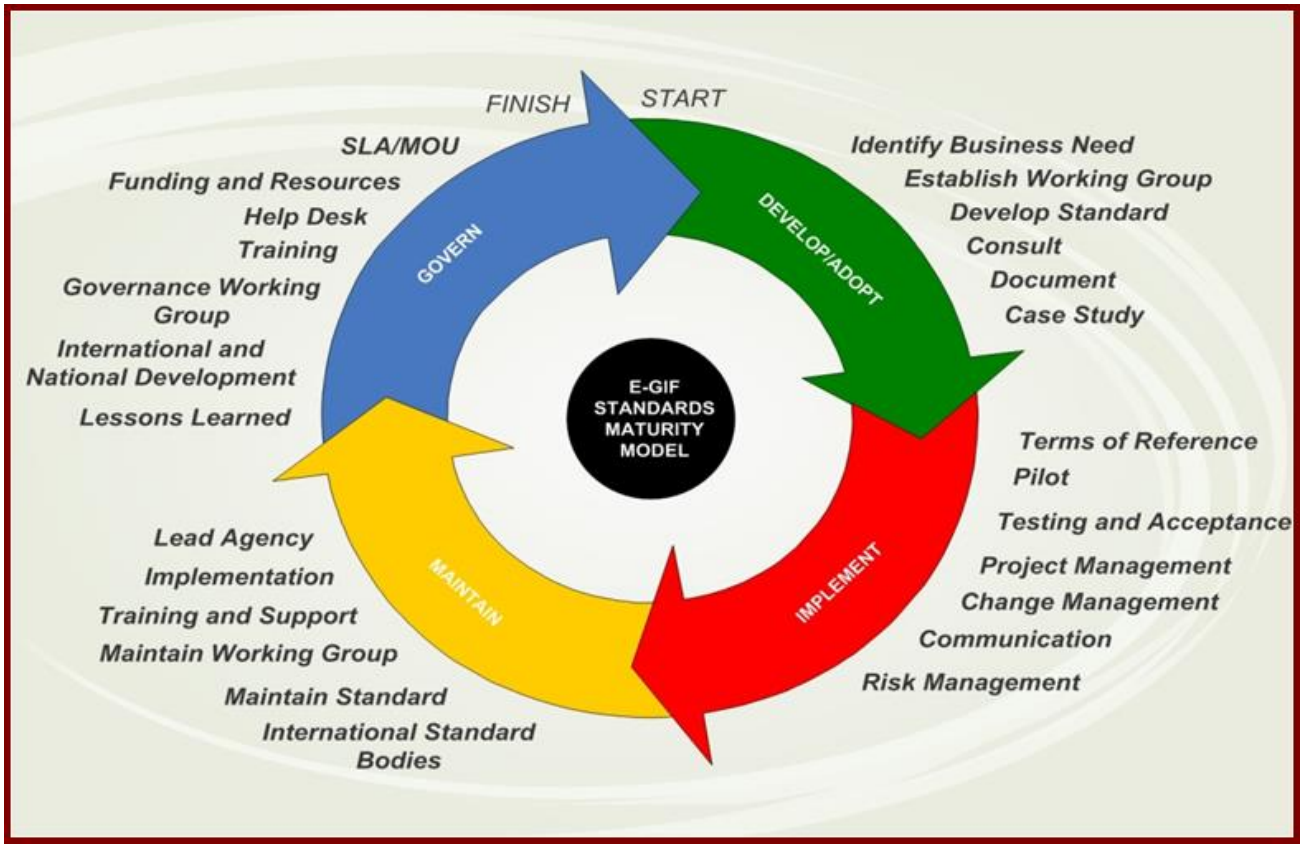


Figure 2-3

The basic criteria for choice of the standards are as follows:

- openness;

- level of accessibility and maintenance;

- maturity;

- potential;

- applicability to the national conditions.

It is necessary to explain that the term "**Maturity of Standard**" has been introduced in compliance with so called "**e-GIF Standards Maturity Model**", presented above. The development process of an e-GIF standards falls into four phases: - development/adoption; - implementation; - maintenance; - governance.

The quality of this succession affects the effectiveness and applicability of the respective standard.

The choice of a fundamental standardization platform is of crucial importance, because of the exceptional diversity of the standards and the specifications related to the system integration and the interoperability. The evolution of the standardization process in respect to the system integration and the interoperability directs this choice towards the integration oriented to services. The latter allows not only for transfer of information from one application to another application in different information systems, but also creation of a complex application through services maintained in remote systems through the distribution of common business logics between the applications.

The basic practical approach to the choice of standards related to interoperability is a combination of:

- the classical Reference model for open distributed processing (international standard ISO/IEC 1076 : 1998), which defines the infrastructure for distributed processing of information between heterogeneous technological resources and multiple organizational domains;

- the last level in the evolution of the standards for system integration – the so-called "Service oriented architecture (SOA)" where "loose coupled" modules of applications are distributed, combined and used for the creation of new applications in the network.

The standardization of the information systems in the field of system integration and interoperability covers wider area than that of the so-called "formal harmonized standards" approved by official intergovernmental standardization bodies (such as ISO, ITU at a global level or CEN, CENELEC, ETSI – at European level). It covers informal and hybrid standardization processes – the production of sector consortia, such as: OASIS, IETF, W3Consortium, UN/CEFACT, OMG, etc.

The standards can be divided into two main groups related to the fields of application:

• horizontal standards – with general application (in all areas);

• vertical standards – with application in a specific area (branch, etc.). As an example for the objectives of the e-Government information systems these can be medical information, banking, geographic information systems, industrial product systems, etc.

Usually the interoperability frameworks are treating thoroughly only the horizontal standards, ensuring interoperability in the information systems within the administration. The vertical standards from areas concerned with these systems can be maintained by branch groups.

European project CAMSS

The **'CAMSS' (Common Assessment Method for Standards and Specifications**), an initiative of the European Commission's IDABC program and of Member States, aims to initiate, support and coordinate the collaboration between volunteer Member States in defining such method and to share the assessment study results for the development of e-Government services.

Member States are currently organizing the assessment of standards and specifications, e.g. within the context of their National Interoperability Frameworks. The CAMSS aims to improve interoperability through the sharing of expertise and best practices in the use of standards and specifications for software in e-Government, contributing to the efficiency of European government organizations thanks to the re-use of established assessments.

The CAMSS defines a method for assessing standards and specifications. It does not provide a general policy, and does not make recommendations at a European level. The project provides a tool enabling structure and exchange of information on standards and specifications for software in the field of e-Government. The second phase of the project provided a methodology for collaboration and exchange of assessment results among Member States, set up proposals for assessment studies to be carried out and subsequently shared, disseminated the assessment study results and conducted specific studies. It is left to the convenience of the Member States to decide on how to proceed with their own interpretations/ recommendations/regulations in using the assessment study results.

The four CAMSS criteria (Suitability, Potential, Openness, and Market Conditions) figure as a list of qualitative aspects of a standard or specifications to be taken into account, rather than

a quantitative evaluation. Each criterion is described with a series of questions and suggestions on how to implement the assessment. These elements will have to be adapted / interpreted according to the identified context and scope of the assessment.

Group of standards related to the interoperability – best European practices

The UK Technical Standards Catalogue defines the minimum set of specifications that conform to the technical policies as defined in e-Government Interoperability Framework (e-GIF). The current specification for the e-GIF covers the following areas: - interconnectivity, - data integration, - content management metadata, and e-services access.

Each area comprises tables containing specifications and includes version numbers and notes. Government is, however, committed to ensuring that these technical policies and specifications are kept aligned to the changing requirements of the public sector and to the evolution of the market and technology.

Technical specifications and standards under consideration are:

- standards for electronic forms;
- selection of specific business area related specifications;
- guidance on semantic web;
- ISO/IEC standards for XML schema languages;
- W3C XML 1.0 (third edition);
- XML specifications for office applications;
- standards for the UK government ICT architecture;
- standards for transactional interchanges.

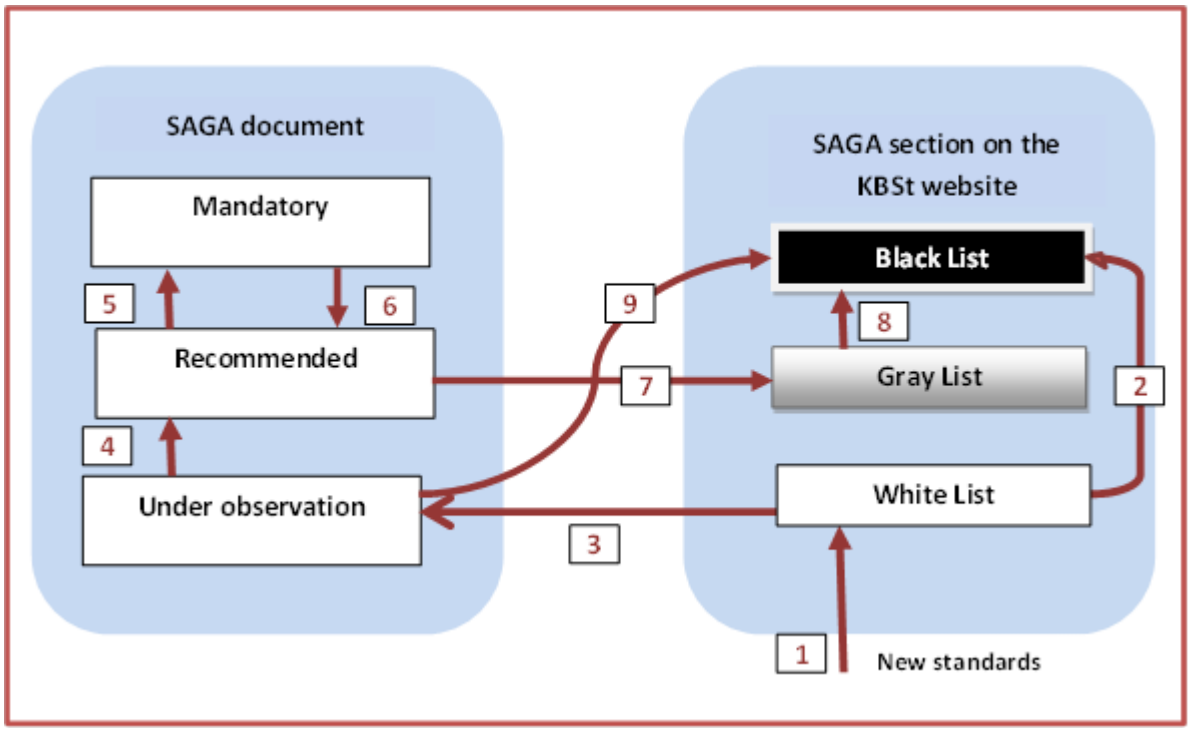


Figure 2-3

The German document "**Standards and Architectures for e-Government Applications (SAGA)**" divides standards into three categories:

- standards are **under observation** if they are in line with the intended development trend, are finalized and meet the minimum requirements for the openness of standards, defined in SAGA as follows: a. the standard has been published and the standard specification document is available either freely or at a nominal charge; b. the intellectual property (for instance, in the form of patents) of a standard or of parts of a standard must, if possible, be accessible without being contingent upon the payment of a license fee; c. the federal administration and the users of its services must be able to use the standard without restriction; d. the standard must remain published and freely usable in the future. These standards may not yet have proven their worth in practical application or do not meet all the aims of SAGA;

- standards **are recommended** if they have been tried and tested in practical application but if a more suitable, mandatory standard exists or if they do not meet all the aims of SAGA. However, minimum requirements for the openness of standards must be fulfilled and investment security warranted;

- standards are **mandatory** if they have been tried and tested in practical application and represent the preferred solution. They are established on the market and meet all the aims of SAGA. Such standards must be observed and applied with priority.

The picture above shows the dynamics of transitions of the standard between the categories of this classification.

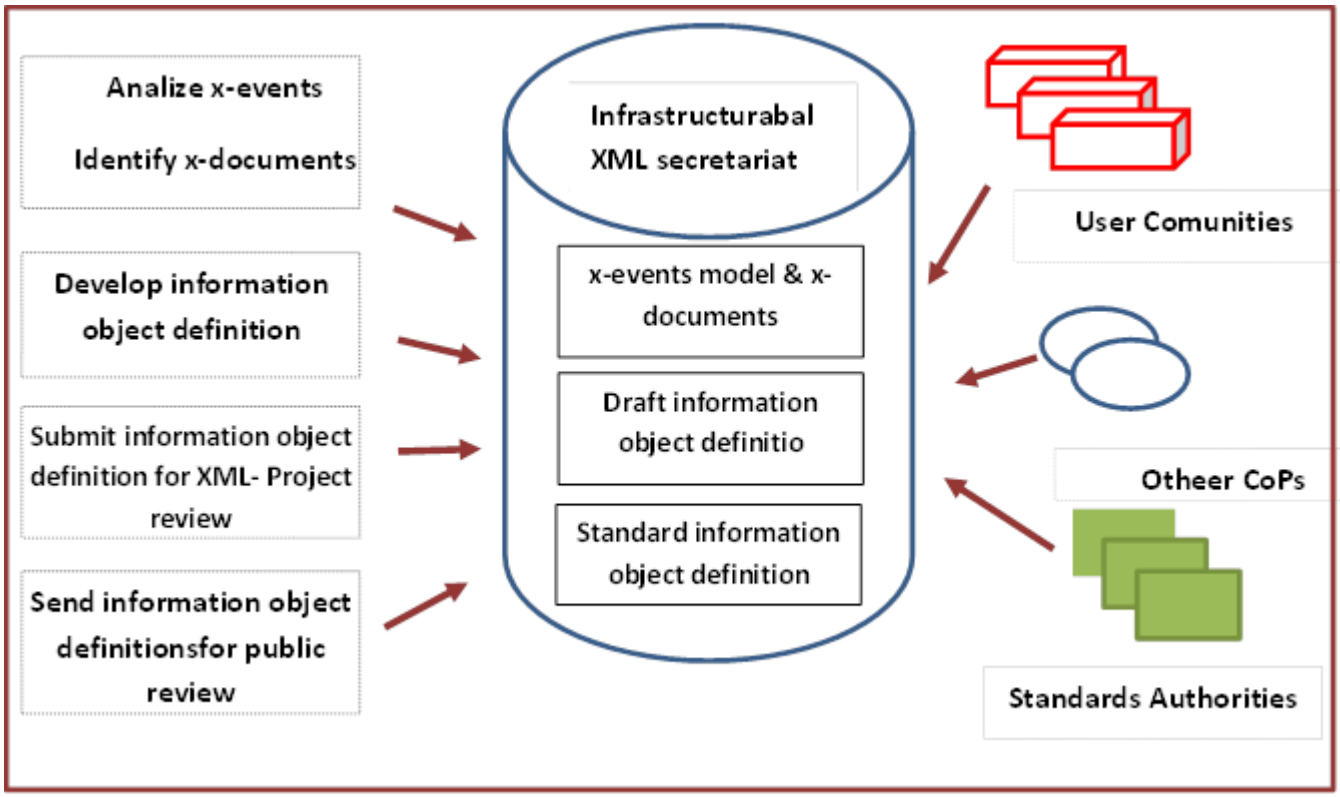


Figure 2-4

The Danish methodology for identifying, defining and documenting interoperability standards, and thereafter maintaining and disseminating them to users, is based on existing software and knowledge engineering and management processes and procedures. There are two primary concepts, both derived from established engineering practices, underlying this standardization activity: information objects and communities of practice. The applying

knowledge engineering and management procedures to the standardization process is justified in several ways.

First, the information objects that are the core of the digital public service's standards are derived from current practice and engineered to be re-usable between interchange formats. The information objects form the standardized core data and create interchangeable and re-usable "units of knowledge". These are derived by analyzing existing practice and applying application knowledge and expertise.

The second major concept, the communities of practice, deals with the usability of the standards and the end-users. In order to assimilate the domain knowledge of the users into the standardization process, a social framework is devised where users can be integrated – on their own terms.

The picture above depicts the phases of the standardization process.

Compliance with requirements of interoperability

Compliance refers to any explicitly stated rule or regulation prescribing any aspect of an internal or cross-organizational business process. Examples include service composition policies, service deployment policies, service sequencing or ordering policies, information exchange policies, security policies, Quality of Service policies, business policies, jurisdictional policies, preference rules, and intellectual property and licenses.

An existing process or process activity can be annotated to be compliant to a certain compliance rule of a specific regulation as probably implemented by a standard framework. This allows for reuse of legacy processes that need to be marked as compliant. Such processes would have to be validated manually, thus no validation at runtime may occur using this approach. Also the compliance for a process or process activity can be modelled. Thus for each of the compliance concerns an appropriate precisely specified model has to be defined using modelling techniques.

It is specific approach for design of the business process compliance. There are two primary roles involved in this approach: (i) a business expert, who is responsible for defining and managing business processes in an organization while taking compliance requirements into account, and (ii) a compliance expert, who is responsible for the internalization, specification, and management of compliance requirements stemming from external and internal sources in close collaboration with the business expert.

The approach encompasses two logical repositories: the business process repository and the compliance requirements repository, which are semantically aligned via shared domain ontology. Process models are defined and maintained in the business process repository, while the compliance requirements and all relevant concepts are defined, maintained and organized in the compliance requirements repository. The approach assumes the overall process to start either from the business process side or from the compliance requirements side. Process models can be specified in the Business Process Execution Language (BPEL); the de-facto standard for workflows that provides an XML-based language to describe the operational logic of the process and its execution flow.

Compliance in the telecommunication constituent of information systems

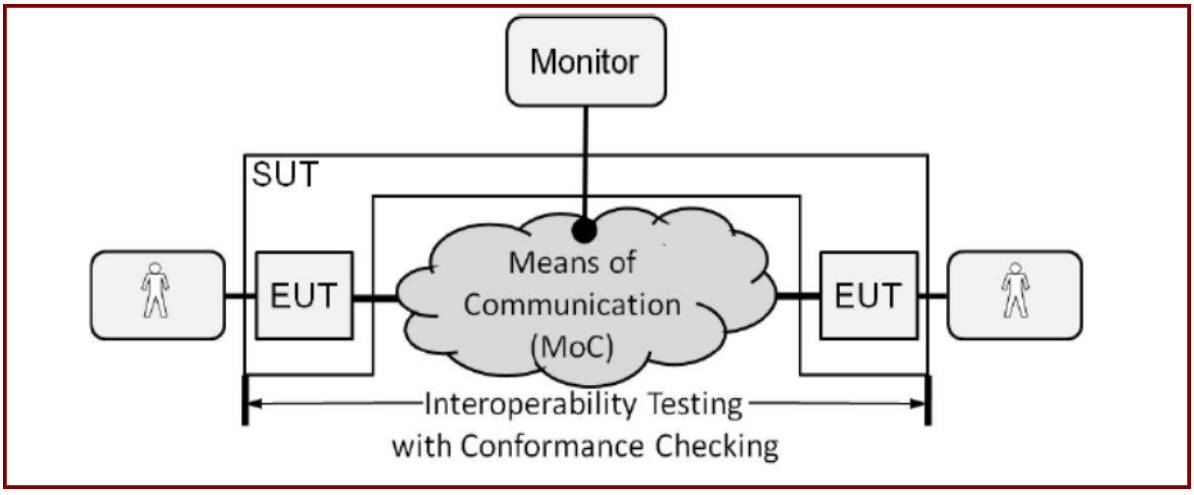


Figure 2-5

Systems that implement a set of standards need to be assessed for their interoperability with other systems. It is also necessary to demonstrate that they conform to the standards. At the standardization level, this in turn can be facilitated with the availability of open and validated test specifications.

Interoperability testing is the most intuitive way of confirming that two or more systems work together. A number of standardization organizations use interoperability testing events as a means to raise the status of a specification to the level of a standard. At European Telecommunication Standards institute (ETSI), interoperability testing procedures, so called Plugtests™, are organized and executed to provide feedback to technical bodies on the maturity of a given technology and its underlying standards. Such procedures can only be successful if testing is based upon an agreed set of interoperability tests.

The purpose of interoperability test specifications is to assess that a communicating system can provide functionality as defined in a specification, e.g. a set of standards. In the context of distributed systems, each system is called an Equipment Under Test (EUT) and the collection of all EUTs is called the System Under Test (SUT) as defined in the ETSI specification EG 202 237 “"Methods for Testing and Specification (MTS); Internet Protocol Testing (IPT); Generic approach to interoperability testing". In order to verify the correctness of the protocol procedures and to provide a basis for fault analysis, interoperability test specifications can be combined with supplementary conformance checks when assessing functionality. Such conformance checks are associated with standardized interfaces between different EUTs.

In addition, EG 202 237 describes the basic concepts of interoperability testing, a means of describing test architectures and a process for developing and executing interoperability test specifications.

Compliance verification - best European practices

UK e-GIF compliance

The ultimate test for interoperability is the coherent exchange of information and services between systems. If this is achieved then the system can be regarded as truly interoperable. Furthermore, it must be possible to replace any component or product used within an interface

with another of a similar specification while maintaining the functionality of the system. To be e-GIF compliant, a system should satisfy both these requirements.

The aspects of the system where the tests need to be applied are:

• interconnection;

• data integration;

• e-services access;

• content management metadata.

The ultimate responsibility for compliance rests with the system's Senior Responsible Owner or Sponsor. Compliance is by self-regulation using normal departmental checking arrangements throughout the system's development lifecycle. It will be for service organizations themselves to consider how their business processes can be changed to be more effective by taking advantage of the opportunities provided by increased interoperability

An e-GIF Compliance Advisory Service is provided by the National Computing Centre (NCC). The service provides a structured web-based commentary about the e-GIF and a self-assessment questionnaire.

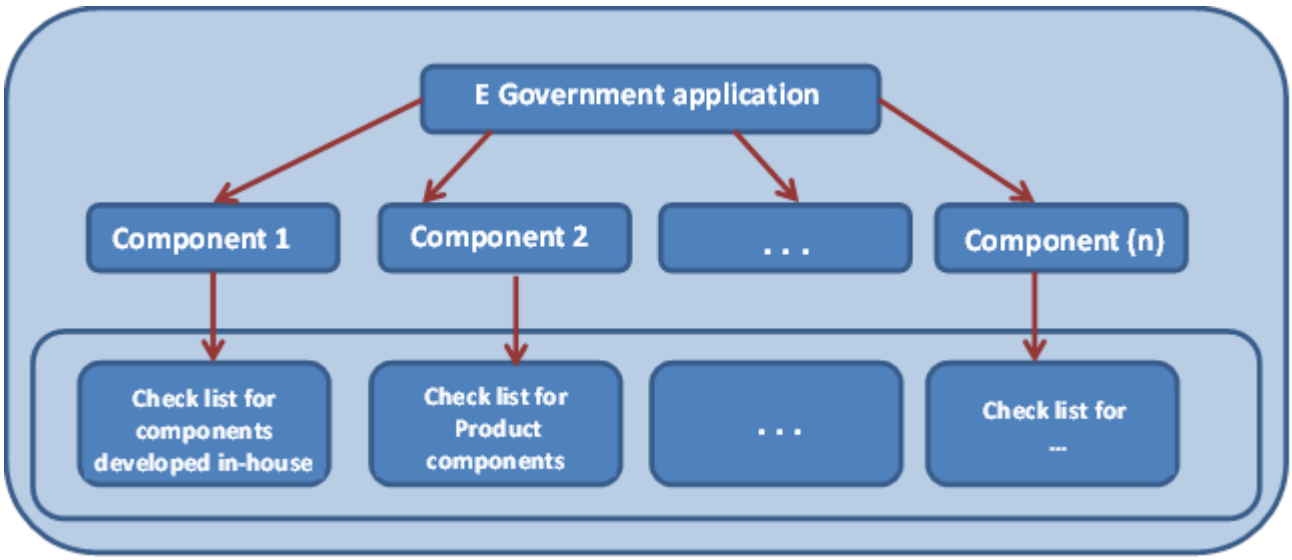


Figure 2-6

German SAGA conformity declaration

The SAGA conformity of an e-Government application is evaluated on the basis of the models, procedures and standards described in SAGA:

a. consideration of standardized process models;

b. consideration of standardized data models;

c. compliance with the standards and architectures described in SAGA;

d. use of existing one-for-all offers (OFA offers).

In order to enable a comprehensive statement concerning the SAGA conformity of an e-Government application – especially in conjunction with the implementation of complex, specialized processes – an application should first be broken down into individual components before evaluating its conformity. A distinction is made here between in-house developments and product components. In order to evaluate the SAGA conformity of products, importance is primarily attached to communication interfaces, data interchange formats and security. In the

case of in-house developments, the technologies for creating models and implementing the application are additionally relevant.

The homepage of the Federal Ministry of the Interior provides a blank and an example of a completed declaration of conformity with checklists for components developed in-house and for product components. The checklists feature topical areas which are relevant for in-house developments or for products, respectively.

Greek compliance demonstrator

The Interoperability Standards and Compliance Demonstrator developed in the Greek Interoperability Centre (GIC) and available only in the Greek language contributes in managing, processing and presenting the rules and guidelines that accompany the Greek e-GIF contents in every version published: (a) Certification Framework for Public Administration Sites and Portals, (b) Interoperability and Electronic Services Provisioning Framework, (c) Digital Authentication Framework, (d) Documentation Model for Public Administration Processes and Data.

With the help of a multi-criteria methodology that takes into account appropriate thresholds for compliance in each sub-framework and weights in rules categories and classification levels (i.e. Obligatory, Recommended and Under Consideration), as well as in standards' maturity levels (White List, Grey List and Black List), compliance of a Public Authority with the specifications of a given version of the Framework can be easily assessed in this demonstrator.

The primary objective of Demo D4 (e-GIF Standards and Compliance) is the design and deployment of an application that manages the information that describes a rule or a standard of the e-Government Interoperability Framework (e-GIF) and takes into account the structure of the Interoperability Registry. This application can also be used to evaluate the compliance of a Public Authority with the policies of a given version of the e-GIF.

CHAPTER 2.2

EUROPEAN STRATEGY, FRAMEWORK AND ARCHITECTURE OF INTEROPERABILITY

European Interoperability Strategy

The European Interoperability Strategy and the European Interoperability Framework, supporting the strategy and the framework levels of the interoperability governance pyramid, are considered to be two key elements in the Digital Agenda for Europe together forming the basis for future activities intended to improve interoperability for delivering European public services.

Implementation of the European Interoperability Strategy requires the following separation of roles:

- the European Commission will: - implement the European Interoperability Strategy through appropriate instruments such as the European Commission supported ISA program and the CIP ICT-PSP program; - e-Government implementation in close cooperation with member states and other stakeholders; - align its internal interoperability strategy with the European Interoperability Strategy through the e-Commission initiative; - ensure that the European Interoperability Framework is applied when implementing new legislation and establishing new European public services; - ensure the governance of the European Interoperability Strategy and related global and sectorial interoperability activities, in close coordination with member states.

- Member States should: - align national interoperability strategies with the European Interoperability Strategy and national initiatives and actions with corresponding initiatives and actions at European Union level; - work with each other and with the European Commission on implementing the European Interoperability Strategy, while monitoring the progress and impact of related actions at national level; - align their National Interoperability Frameworks with the European Interoperability Framework;

- take into account the European dimension at an early stage in the development of any public service that might become part of European public services in future; - contribute to the governance of the European Interoperability Strategy and related interoperability activities.

The European Interoperability Strategy was developed by the European Commission's Directorate-General for Informatics in cooperation and agreement with the member states and accepted in 2010. The strategy was prepared during the European Commission supported IDABC and finalized after a public consultation under the ISA which maintains it. It is directly steered by the CIOs of the member states.

To achieve the European-wide effective and efficient delivery of public services, activities at European Union and member state level should be coordinated. In addition, interoperability governance at European Union level should be established. The European Interoperability Strategy is at the top of the interoperability governance pyramid and it sets common, coherent approach and provides basis for an organizational, financial, and operational framework to support cross-border and cross-sectorial interoperability. The European Interoperability Strategy aims to provide guidance and to priorities the actions needed to improve interaction, exchange, and cooperation among European public administrations across borders and across sectors for the delivery of European public services.

Activities of the European Interoperability Strategy follow a defined set of principles which are described in the table given below.

Principle	Explanation
Reusability	**The European Interoperability Strategy activities will be reusable, based on sustainable approaches**
Transparency	**The European Interoperability Strategy activities are transparent and offer the possibility of traceability**
Openness and innovation	**European Interoperability Strategy activities are open, conforming to standards, allowing further developments and improvements and are vendor-independent**
Continuous improvement	**European Interoperability Strategy activities are based on continuous assessment and improvement**
Community of shared interest	**European Interoperability Strategy activities serve a community of shared interest. This can be on various levels: interoperability expert's community, European public services community or even the larger European community**
Trust	**European Interoperability Strategy activities are based on mutual trust. Public administrations should be assured that all transactions are secure, reliable, and trustworthy**

European interoperability activities are divided in the European Interoperability Strategy in three clusters which are specified in the table given below.

Main components	Goal	Specific activities
Trusted Information Exchange	**Defines how information needs to be treated to be able to achieve interoperability**	• to work via a limited number of politically relevant and concrete sectorial projects at European Union and member state levels; • to continue supporting, at European Union level, efforts towards the interoperability of key enablers (eID, eSignature, etc.); • to continue the SEMIC approach (www.semic.eu) and its methodology; • to work towards opening up base registers, taking into account associated best practices, the possible related risks and opportunities, as well as the various needs and expectations of the main stakeholders; • to work towards the establishment of a federated catalogue of services offered by public administrations in the European Union.

Main components	Goal	Specific activities
Interoperability Architecture	**Defines how the infrastructure needs to be organized to obtain interoperability**	• to develop a joint vision on interoperability architecture by first defining its scope and the needs for common infrastructure services and common interface standards; • to provide guidance on architecture domains where member states share a common interest; • to ensure the systematic reuse of architectural building blocks by the European Commission when developing services to be used by the member states. Here, existing infrastructure service components along with generic applications (IMI, early alert systems, grant management, etc.) could be reused and rationalized. Additionally, a catalogue of architectural building blocks available for reuse by the member states and the European Commission could be set up with contributions from the European Union and member states.
Assessment of the ICT Implications of New European Union Legislation	**Defines what the legal framework is in which interoperability can operate**	• to develop guidelines and methodologies at European Commission and member state level; • to test the usefulness of these guidelines by applying them to concrete cases involving policymakers and legal and ICT experts; • to ensure continuous improvement of the guidelines and methodologies based on the lessons learned from experience; • to ensure general application of the practice of assessing ICT implications towards a more systematic approach whenever changes occur in legislation (e.g. amendments or additions to ICT-related legislation).

European Interoperability Framework

The **first** version of the European Interoperability Framework was approved in October 2004. At the moment the actual version is the second version of the framework which was approved in 2010. The European Interoperability Framework is maintained under the European Commission supported ISA program (http://ec.europa.eu/isa/), in close cooperation between the Member States and the EC.

An interoperability framework is an agreed approach to interoperability for organizations that wish to work together towards the joint delivery of public services. Within its scope of applicability, it specifies a set of common elements such as vocabulary, concepts, principles, policies, guidelines, recommendations, standards, specifications, and practices.

The European Interoperability Framework is the overarching set of policies, standards, and guidelines which describe the way in which organizations have agreed, or should agree, to do business with each other.

The European Interoperability Framework is a non-technical document with the following main purposes:

- to promote and support the delivery of European public services by fostering cross-border and cross-sectorial interoperability;

- to guide public administrations in their work to provide European public services to businesses and citizens;

- to complement and tie together the various National Interoperability Frameworks at European level.

The target audience of the European Interoperability Framework addresses all those involved in defining, designing and implementing European public services, for example, managers of e-Government projects in Member States Administrations and European Union bodies, Member States Administrations, European Institutions and Agencies

The European Interoperability Framework is applied when:

- making decisions on European public services that support the implementation of European Union policy initiatives;

- establishing public services that in the future may be reused as part of European public services.

The European Interoperability Framework covers the following content:

- 25 recommendations for public administrations;

- 12 underlying principles;

- the conceptual model for public services;

- 3 levels of interoperability;

- the concept of interoperability agreements;

- the governance of interoperability.

EIF Principles

1. **Subsidiarity and proportionality** - the European Union only takes action when this is more effective than action taken at national, regional, or local levels and European Union action is limited to what is necessary to achieve agreed objectives

2. **User-centricity** - the needs of citizens and businesses determine what public services are provided and how they are delivered. Generally speaking, citizens and businesses will expect:

- to access user-friendly services in a secure and flexible manner allowing personalization;

- multichannel delivery, allowing access to services anyhow, anywhere, anytime;

- to access a single contact point, even when multiple administrations have to work together to provide the service;

- to provide only the information necessary to obtain the public service and to provide any given piece of information only once to administrations;

- administrations to respect privacy.

3. **Inclusion and accessibility** - public services should be accessible to all citizens, including persons with disabilities and the elderly, without discrimination

4. **Security and privacy** - citizens' privacy and confidentiality of information provided by businesses must be guaranteed

5. **Multilingualism** - information systems (level of the user interface and all levels in the design of European public services) supporting public services should cater for multilingualism

6. **Administrative simplification** - public services should reduce the administrative burden on businesses from information collection

7. **Transparency** - citizens and businesses should be able to understand and respond to (feedback) administrative processes and decisions that could affect them

8. **Preservation of information** - records and information in electronic form held by administrations for the purpose of documenting procedures and decisions must be preserved. In order to guarantee the long-term preservation of electronic records and other kinds of information, formats should be selected to ensure long-term accessibility, including preservation of associated electronic signatures and other electronic certifications, such as mandates

9. **Openness** - to encourage the sharing of knowledge among interacting organizations and stimulate debate to solve problems

10. **Reusability** - public administration solutions should be developed to facilitate sharing and reuse

11. **Technological neutrality and adaptability** - specific technological solutions or products should not be imposed on citizens, businesses, and other administrations

Conceptual model of the European Interoperability Framework

The conceptual model presented in the European Interoperability Framework suggests ways to organize the creation and operation of public services4. It illustrates that a European public service is a combination of existing public services provided at different levels of government and shows where interoperability is needed in such a complex environment.

The conceptual model:

- helps develop a common vocabulary and understanding about the main elements of a public service;

- emphasizes a building-block approach, allowing for the interconnection and reusability of service components when building new services;

- is sufficiently generic to be applicable at any level of government that provides public services, from local all the way up to European Union level.

The model recognizes that European public services:

- are based on information from various sources located at different levels of administration, in different Member States;

- combine basic public services constructed independently by public administrations in different Member States.

Therefore, it highlights the need for modular, loosely coupled service components interconnected through infrastructure and for working together to deliver European public services.

The conceptual model is shown in the figure below. It is flexible due to the fact that it allows different aggregate services to be created by combining basic public services from multiple providers.

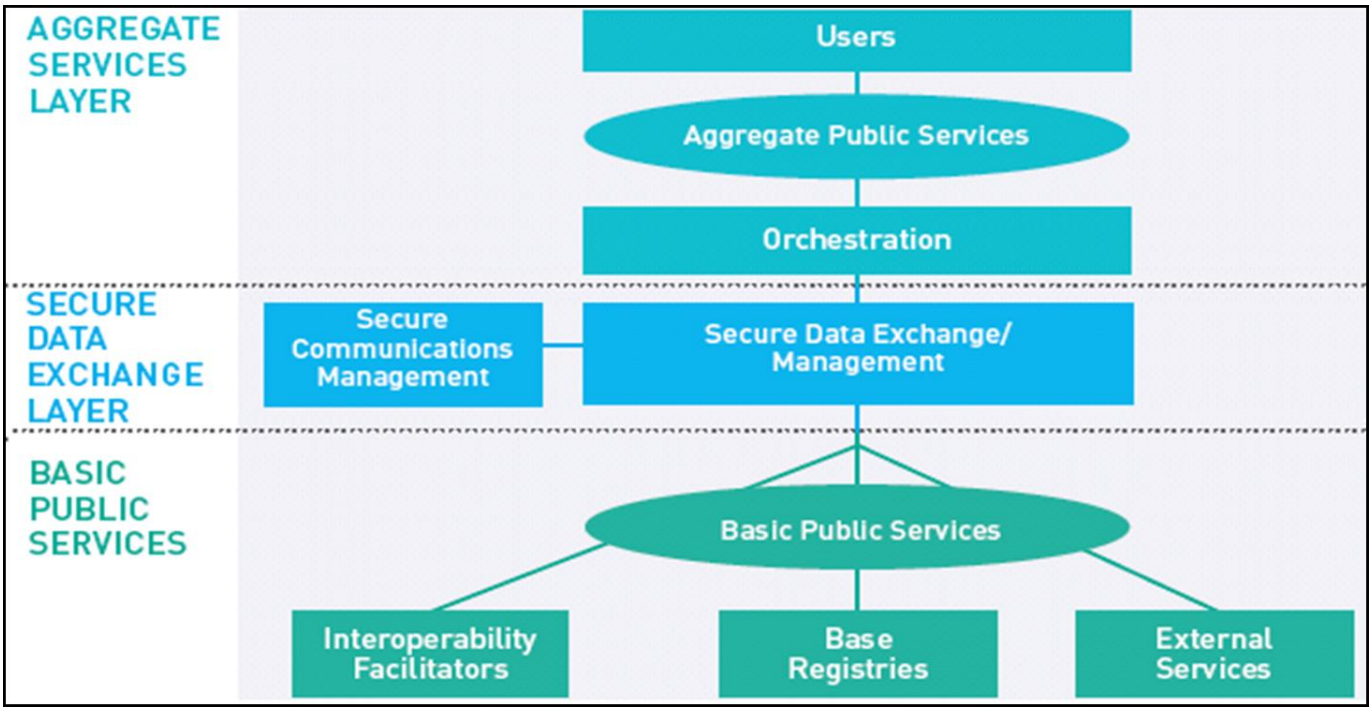


Figure 2-7

Agreements and Specifications

The provision of European public services requires cooperation among different public administrations at the different interoperability levels. For each level (organizational, semantic, technical) the organizations involved should formalize cooperation arrangements in interoperability agreements which should be drafted with sufficient detail to achieve their aim — to provide a European public service — while leaving each organization maximum internal autonomy.

A number of equivalent, competing specifications may be available at technical or semantic level as a basis for interoperability agreements. From one side, public administrations may decide to support multiple formalized specifications or technologies to communicate with citizens and businesses. However, from another side, taking into account efficiency, it would be

rational to reduce, as much as possible, the number of them when working together to provide a European public service.

Decisions concerning usage of formalized specifications and technologies should be based on transparency, fairness, and non-discrimination. One way to do this is to agree on a common assessment methodology and selection process taking into account:

- assessing and selecting formalized specifications:

- when public administrations select the formalized specifications or technologies to ensure interoperability, they should assess relevant formalized specifications;

- this assessment should be tailored to the specific interoperability needs of the public administrations in question, but based on objective criteria, primarily related to functional interoperability needs;

- when several formalized specifications meet functional interoperability needs, additional criteria on quality of implementation, market support, potential for reusability and openness can be used.

The specifications must be open and capable for reuse. The level of openness of a formalized specification is an important element in determining the possibility of sharing and reusing software components implementing that specification. This also applies when such components are used for the establishment of new European public services.

If the openness principle is applied in full:

- all stakeholders have the same possibility of contributing to the development of the specification and public review is part of the decision-making process;

- the specification is available for everybody to study;

- intellectual property rights related to the specification are licensed on FRAND (fair, reasonable, and non-discriminatory terms, a licensing obligation) terms or on a royalty-free basis in a way that allows implementation in both proprietary and open source software.

However, public administrations may decide to use less open specifications, if open specifications do not exist or do not meet functional interoperability needs. In all cases, specifications should be mature and sufficiently supported by the market, except if used in the context of creating innovative solutions;

The specifications can contribute to the standardization process. In some cases, public administrations may find that no suitable formalized specification is available for a specific need in a specific area. If new specifications have to be developed, public administrations may either develop the specifications themselves and put forward the result for standardization, or request a new formalized specification to be developed by standards developing organizations.

National interoperability frameworks

In parallel with development of the European Interoperability Framework, the Member States develop their National Interoperability Frameworks. By their nature, National Interoperability Frameworks are, in general, more detailed and often prescriptive than the European Interoperability Framework, which operates at a higher level of abstraction, as a ‘meta framework’ and, in line with the subsidiarity principle, does not impose specific choices or obligations on the Member States. The European Interoperability Framework and the National Interoperability Frameworks are complementary and must be aligned.

The EC supports a NIFO (National Interoperability Framework Observatory), whose main objective is to provide information about the National Interoperability Frameworks to allow

public administrations to share experiences and knowledge. It focuses on the analysis of the National Interoperability Frameworks based on a model that allows the comparison of various aspects. This model aims to highlight similar characteristics of the National Interoperability Frameworks and does not serve as a benchmarking tool. The NIFO was launched in 2008 under the IDABC program (ec.europa.eu/idabc/), where the analytical model was developed based on analysis of the Maltese, German and Danish National Interoperability Frameworks. The second phase of the NIFO saw the extension of this analysis to 33 countries, including all European Union Member States, European Economic Area and European Union Candidate Countries.

In the framework of the new European ISA program the project NIFO started in 2011 and will continue till 2015. Its objectives are:

- revising the comparative model to take into account the new European Interoperability Framework and the Digital Agenda;

- providing support to European Union public administrations to align their National Interoperability Frameworks with the European Interoperability Framework;

- setting up a new maintenance process to provide the most up-to-date information possible;

- analyzing the current national interoperability activities using the updated model and updating the respective factsheets with the results.

The benefits of the action are the following :

- providing guidance and support both for the development of new National Interoperability Frameworks and the alignment of current interoperability initiatives to the European Interoperability Framework;

- providing input to decision-making processes regarding national developments, and giving national policy officials an objective overview of the European situation and the position of their Member State;

- providing a better insight into the status of National Interoperability Framework developments across Europe, benefiting commercial enterprises that are involved in the realization of e-Government solutions, such as service integrators and software vendors.

In 2012, NIFO has published 29 factsheets presenting current status of national interoperability frameworks. The conclusion is that 17 out of 29 European countries have national guidelines on interoperability, nine of them are well-aligned to the European Interoperability Framework. At the same time, 12 countries do not yet have a policy or a guideline on interoperability. Factsheets are available at https://joinup.ec.europa.eu/elibrary/factsheet/national-interoperability-framework-observatory-nifo-factsheets.

European Interoperability Architecture

In general, interoperability at European Union level is promoted through several initiatives. All together they form the interoperability governance pyramid in which each initiative complements the other one

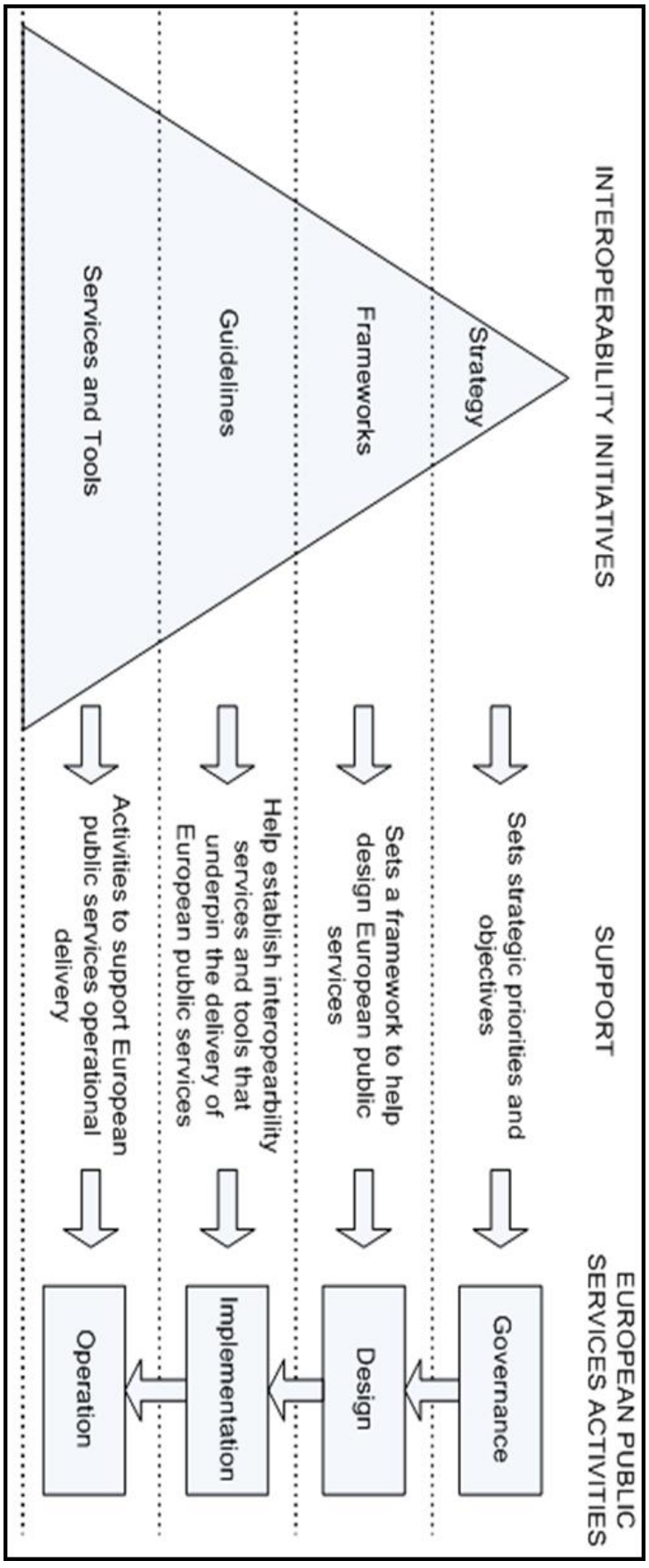

INTEROPERABILITY INITIATIVES
SUPPORT
EUROPEAN PUBLIC SERVICES ACTIVITIES
Strategy
Frameworks
Guidelines
Services and Tools
Sets strategic priorities and objectives
Sets a framework to help design European public services
Help establish interopearbility services and tools that underpin the delivery of European public services
Activities to support European public services operational delivery
Governance
Design
Implementation
Operation

Figure 2-8

Taking into account the current status of initiative efforts, the previous figure can be transformed in the figure given in the next slide. Therefore, the European Interoperability Strategy (EIS), accepted in 2010, focuses on the governance activities for interoperability towards European public services, the European Interoperability Framework (EIF), accepted in the same year, looks at the conception of European public services, the European Interoperability Architecture (EIA) study investigates the implementation of European public services, and the European Interoperable Infrastructure Services (EIIS) support the operation of European public services.

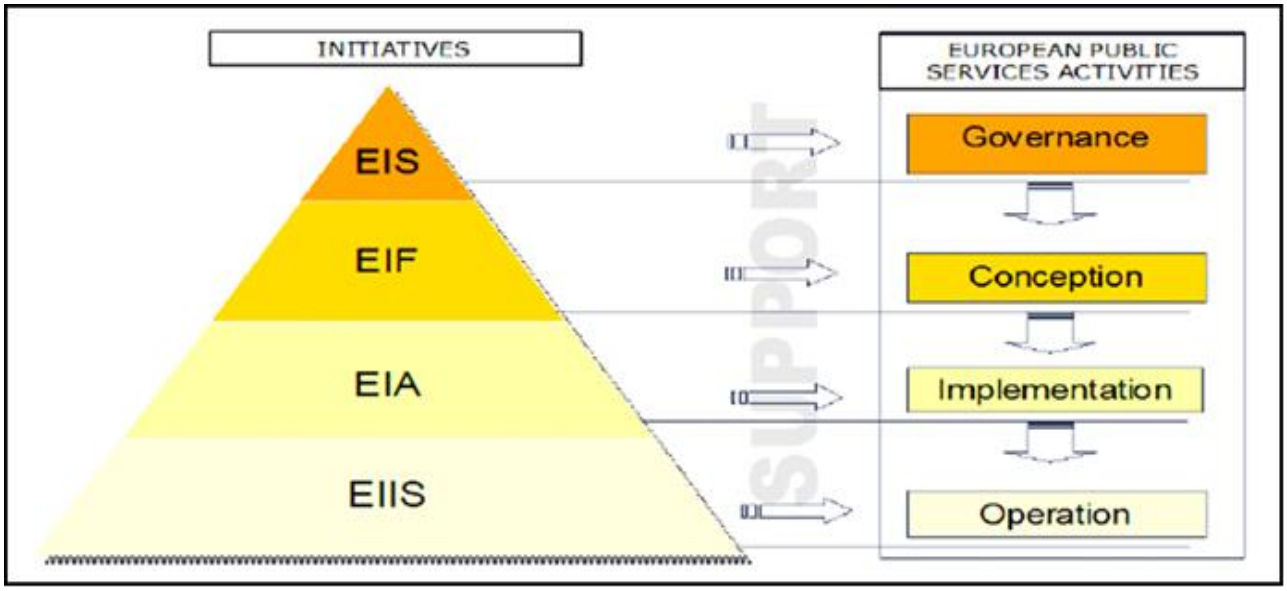


Figure 2-9

Therefore, the EIA is the practical and concrete implementation following the EIF.

At the moment, the latest achievement in the development of the EIA is the study on a common vision for an EIA, developed in 2011, in the framework of ISA program and its action „Towards a European Interoperability Architecture - Elaboration of a common vision for a European Interoperability Architecture – EIA". The scope of the study is limited to cross-border and cross-sector interactions between Member States and between Member States and Commission services, dealing with Administration-to-Administration interactions.

It is important to stress the difference between the common vision for an EIA and the EIA itself. The common vision for an EIA consists of the interoperability agreements that should be common on a European level, while the EIA consists of the solution specifications and solution instances that implement the common vision for an EIA.

Therefore, the common vision for an EIA is implemented on the meta-level by means of templates for interoperability agreements, and by means of a common set of interoperability agreements that are cross-border (i.e. European), cross-sectorial, highly feasible and have a high added value for interoperability. An interoperability agreement consists of one or more interoperability solution specifications, and an interoperability solution specification can be implemented by means of one or more interoperability solution instances.

The vision of the interoperability infrastructure represents a set of ICT systems that support the delivery of European Public Services to administrations, citizens and businesses. The ICT system can be further broken down in different interacting system components, which can be seen as the parts of the system. A system component can be of technical nature (e.g. workflow

engine, service register, single-sign-on module) but it can also be of functional nature (e.g. a pattern, a methodology).

Systems and their components, as part of the interoperability infrastructure, provide services. The term service refers to a discretely defined set of contiguous and autonomous business or technical functionality, making it important to distinguish business services from infrastructure services.

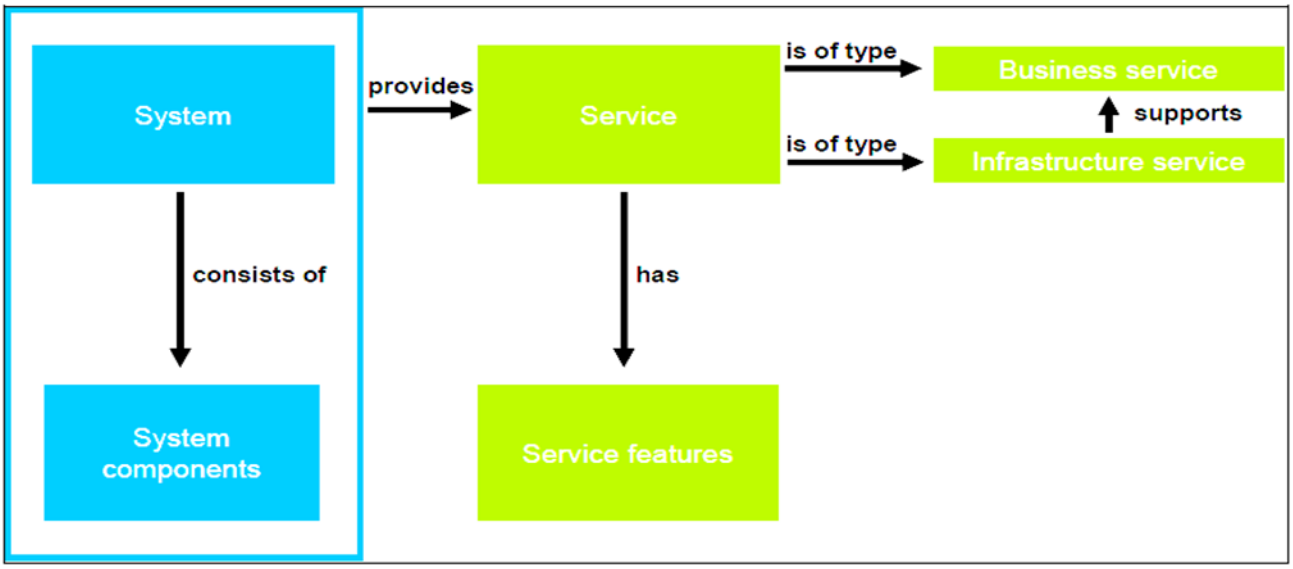


Figure 2-10

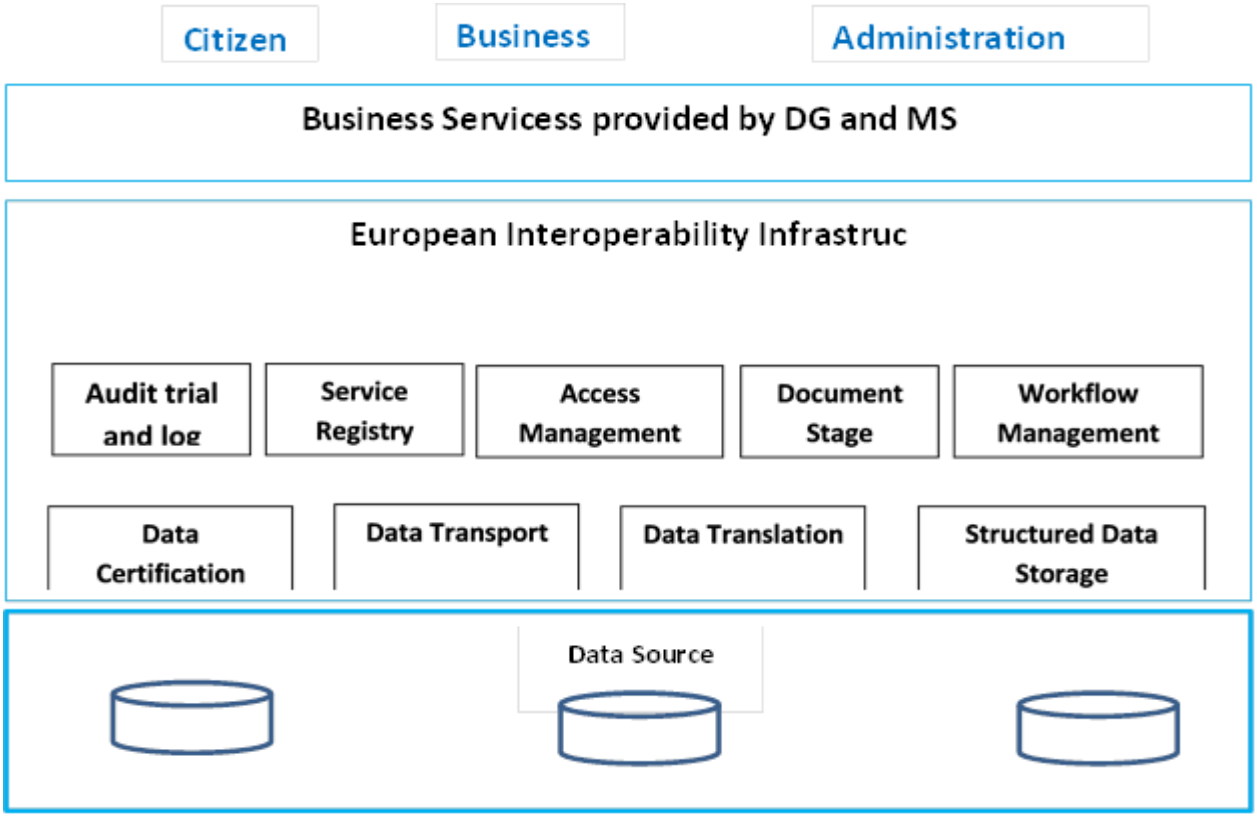


Figure 2-11

In order to identify and describe common interoperability infrastructure services to support European public services the European Commission undertook a study, which has selected components in existing systems or systems in development that were best positioned to be part of the solution that could deliver these EIIS. The study has also proposed implementation options for the EIIS and defined nine EIIS:

1. Audit trail and log chronologically records information about the usage of European public services - it collects data to examine how and when events occurred, who accessed a system and what actions he or she performed during a given period of time.

The logged information can be the exchanged information between the system and the users of the system (incoming and outgoing messages), the log-on data, the transaction content and properties-time, checks and other actions performed by the users as well as actions performed by system administrators, or automated actions initiated by the system. Audit trail and log records data generated by system processes and which do not correspond to specific user actions, and actions taken by identifiable and authenticated users.

2. Service registration - during the last decade Web services are being increasingly implemented by public administrations and private companies. Web services provide access to software systems over the Internet using standard protocols and enable e.g. public administrations to more efficiently integrate applications and improve the accessibility to business processes for citizens, businesses, partners, and internal staff.

Looking at the situation in the European public administrations, Member States and the European Commission currently lack visibility on the services offered by the different service providers across Europe. It occurs often that a public administration of a Member State and/or a Directorate General of the European Commission starts developing a certain service it wants to offer to internal staff, citizens and/or businesses, while a similar service is already offered by another service provider.

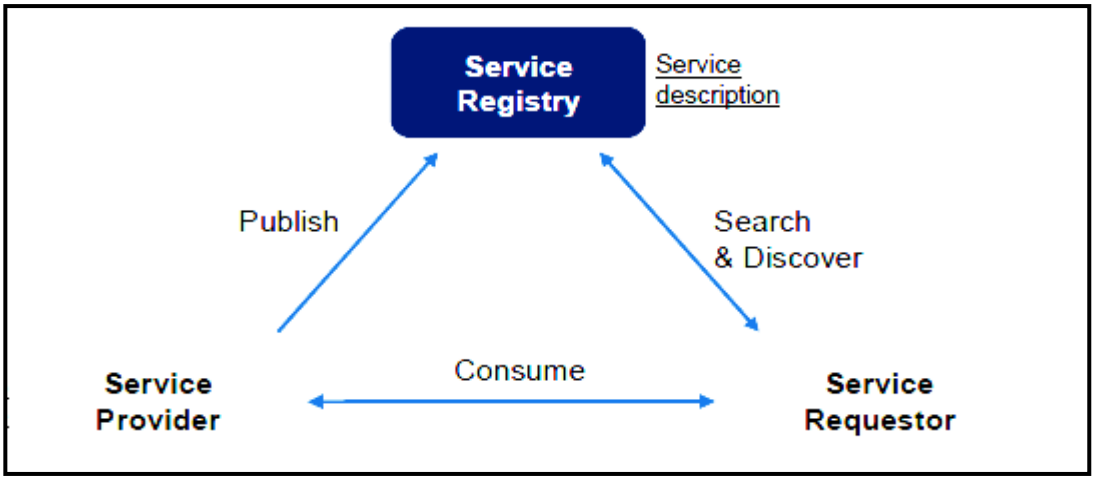


Figure 2-12

Service registries are central registries that provide a description of available services. The registry presents for each service how to use them, their current status, and their physical locations. A service registry maintains the catalogue of available services in a service-oriented context. Service producers publish services and register them into the registry such that consumers are able to find them. An enterprise may have one or more service registries that can be merged to one enterprise service registry, which is called a federated service registry.

3. Identity and access management encapsulates all the processes, policies, and technology solutions that manage digital identities and specifies how digital identities are used to

access resources. This infrastructure service includes entity authentication (the mechanism needed to manage controlled access of entities to applications) and authorization (the mechanism to define what access privileges an entity has within the application by defining roles and groups). Note that data authentication, which verifies origin and integrity of data, is not part of this "identity and access management" infrastructure service, as this is treated in the "data certification" infrastructure service.

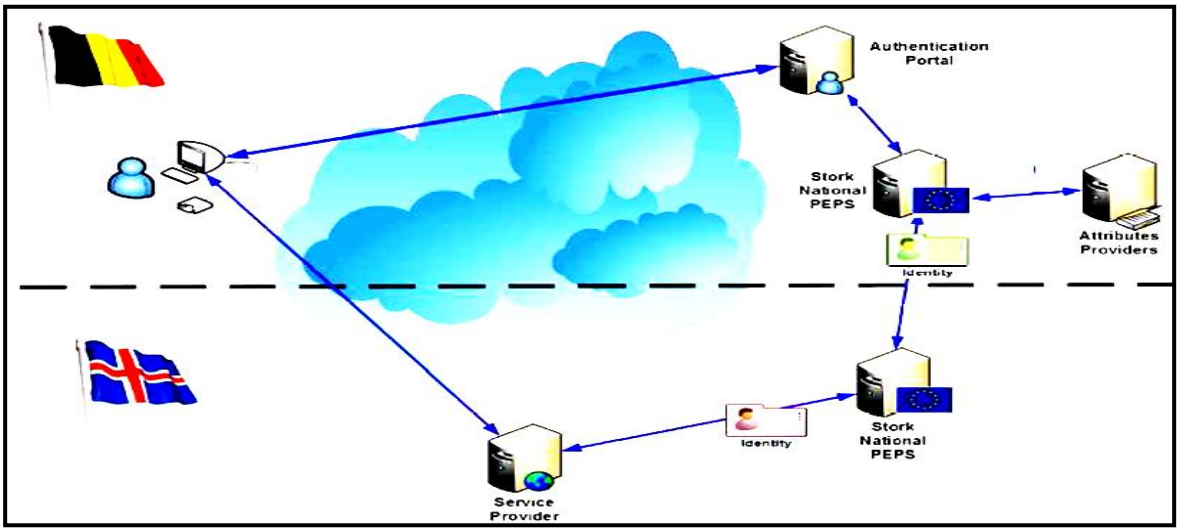


Figure 2-13

4. Data certification is defined as the process of signing an electronic information (which could also be an e-mail, a file or a data source), and of verifying whether the origin and integrity of information are what they are expected to be based on certificates issued by different Certification Authorities. This infrastructure service includes the creation, validation, and extension of advanced electronic signatures as front-end services in conformity with the requirements of the EC Directive. Validation of certificates and time stamping are back-end services to provide these front-end services, and may optionally offer also a direct client interface.

5. Data transport is the exchange of data in a reliable way by providing standardized transport capabilities. This service facilitates communication between systems for collecting and delivering data, and does not store the data centrally. Each system independently handles its own data and, when required, draws data from the database and sends it to another system.

6. Data translation facilitates data transfers between systems (using their own data format, data model and data encoding) and includes semantic translation, syntax translation and multilingualism capabilities.

7. Workflow management orchestrates interactions between workflow participants (human and systems) and provides each participant with the information that is necessary to complete his or her task.

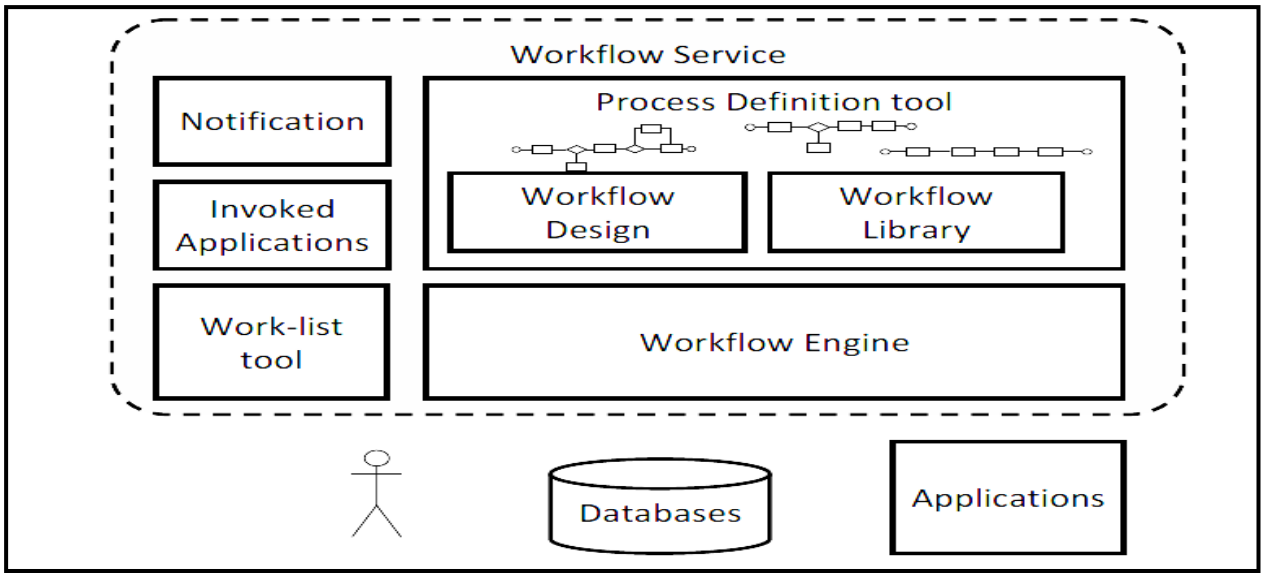


Figure 2-14

8. Document storage is used to store and to manage documents, providing features at each stage of the document life cycle: creation, retrieving, reviewing, versioning, distribution, publishing, archiving and eventual destruction. This service facilitates collaboration between different contributors to the document life cycle.

9. Structured data storage facilitates the exchange of data by providing a simple and structured interface to access data stored in large and complex databases. This service acts as an abstraction layer between the technical data structure of a database and the functional point of view of a standard user. The structured data service removes the need to maintain a schema, while your attributes are automatically indexed to provide fast real-time lookup and querying capabilities. This flexibility minimizes the performance tuning required as the demands for your data increase.

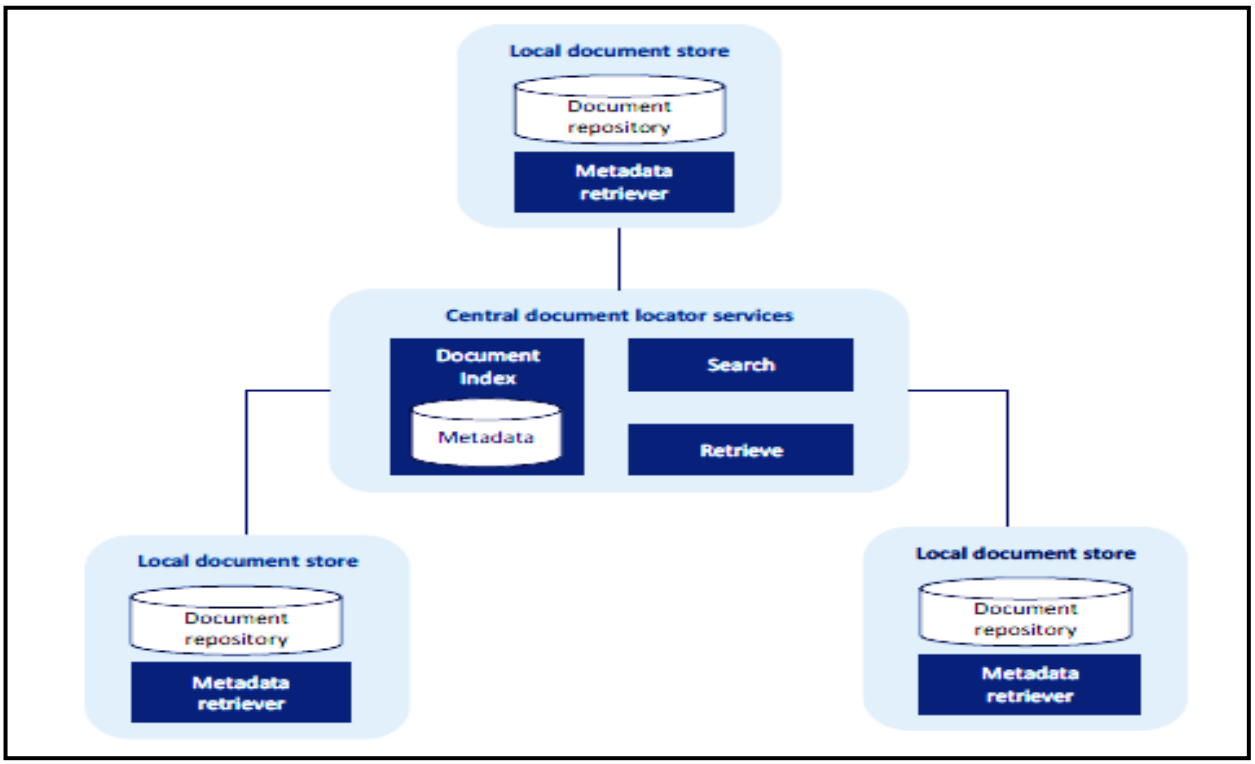


Figure 2-14

The assessment of the need and relevance of common infrastructure services indicated that from nine common infrastructure services identified by the European Interoperability Infrastructure Services (EIIS) Study Data Certification and Identity and Access Management are common infrastructure services with the highest need and relevance to be offered on a European level. Assessment of services is provided in the figure below.

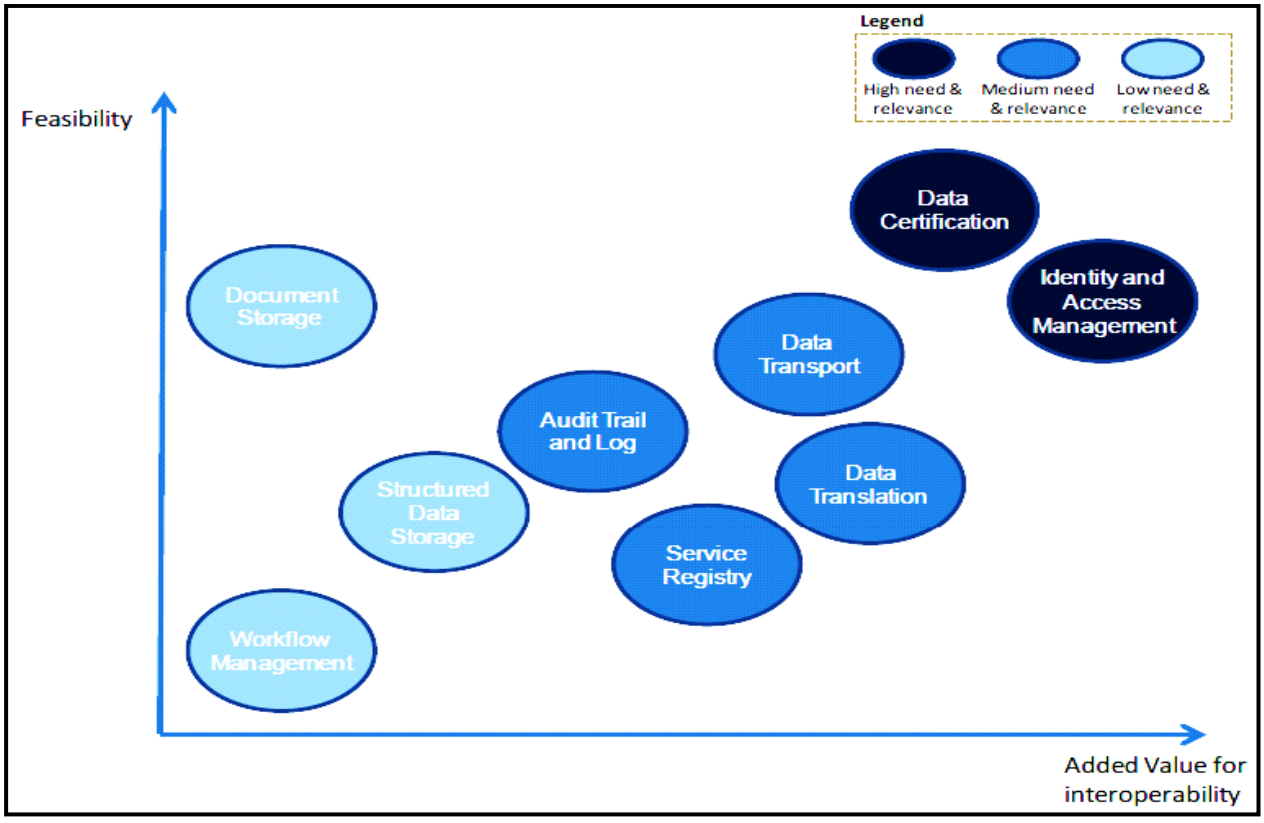


Figure 2-15

From the common vision for an EIA, the interoperability agreements were prioritized and concrete and practical solutions were discussed for the implementation of the top priority interoperability agreements. As a result, five actions related to the prioritized interoperability agreements and one transversal action were defined. These actions were identified as key actions to be taken into account for the ISA Program. As shown in the table below, the solutions to be implemented for the six resulting actions include mostly common frameworks and common services.

Action	Common Framework	Common Service
Action 1- security requirements for the exchange of information across-border	Common specifications for security requirements of cross-border information exchange	
Action 2 – reuse of solution components	Framework for sharing and reuse of solution components	
Action 3 – central platform to publish interoperability assets		Central platform to publish interoperability assets
Action 4 – implementation of governance for EIA and RIA	Governance framework for EIA and RIA (incl. templates for IOP agreements)	
Action 5 - technical connection aspects for electronic data exchange	Common specifications for technical connection aspects of cross-border data exchange	Common platform for electronic cross-border delivery
Action 6 – establishment of contact points to govern the technical access	Guidelines document on how to establish contact points	

CHAPTER 2.3

INTEROPERABILITY ASPECTS

Three main aspects of interoperability

Interoperability has 3 main aspects – organizational, semantic, and technical - which must be taken into account when developing a public service.

Organizational aspect of interoperability arises from differences in business processes and internal structures of organizations which are involved in the establishment and provision of public services and need to collaborate towards mutually beneficial and agreed European public service-related goals.

Technical aspect of interoperability is related to ability of exchanging information between heterogeneous IT networks, applications, and theirs components. Technical interoperability is concerned with all technical issues (technologies, standards, policies) to guarantee that the technical components of the information systems of the collaborating authorities will be able to work together. Therefore, technical interoperability covers the technical aspects of linking information systems.

Semantic aspect of interoperability comes from different linguistic, cultural, legal, and administrative environments in the Member States in particular and multilingualism in the EU in general. The main semantic conflicts are related to the structure of data and the meaning of data, for example, different values are used for the same entity (e.g. the value "foreigner" in one database may mean that the person is not a citizen of the country, while in another database it may mean that the person is not a citizen of the EU), different format for representation of the same data, different measuring units (e.g. centimetres in one database and in inches in another), etc.

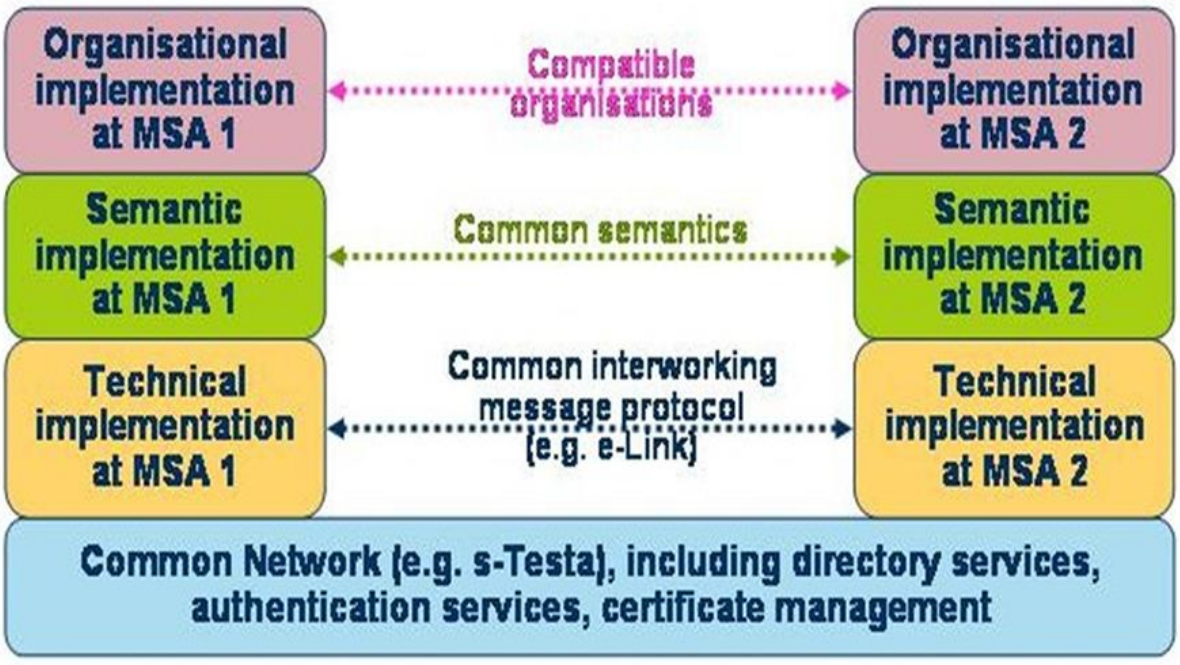


Figure 2-16

Organizational aspects of interoperability

Provision of public services requires collaboration of different public administration organizations which, in their turn, differ in business processes, internal procedures, and structures. These differences could put serious obstacles for achieving interoperability and effective supply of public services. Therefore, it is important to understand organizational issues and to solve them in appropriate way before establishment and provision of any public service.

Organizational interoperability arises from differences in business processes and internal structures of organizations which are involved in the establishment and provision of public services and need to collaborate towards mutually beneficial and agreed European public service-related goals. Therefore, the aim of achieving organizational interoperability is to overcome all organizational obstacles, thus being able to set up the relevant intra- and inter-organizational workflows. In practice, organizational interoperability implies integrating business processes and related data exchange. Organizational interoperability also aims to meet the requirements of the user community by making services available, easily identifiable, accessible, and user-focused.

Organizational interoperability is concerned with the coordination and alignment of business processes and information architectures that span both intra- and inter organizational boundaries. Coordination of business processes across organizational boundaries is essential if a single, aggregated view of a service from the customers' perspective is to be achieved.

Organizational interoperability, as the name implies, is the ability of organizations to effectively communicate and transfer (meaningful) data (information) even though they may be using a variety of different information systems over widely different infrastructures, possibly across different geographic regions and cultures.

Organizational interoperability depends on successful technical, syntactical, and semantic interoperability.

Achieving organizational interoperability requires the following activities:

- identification of the players and organizational processes involved in the delivery of a specific service;
- full examination of their organizational processes, procedures, and structures to determine better ways of doing business and to identify and address/remove any possible barriers. It includes alignment of existent business processes of different administrative entities or definition and establishment of new ones for efficient and effective interaction. Aligning business processes implies documenting them in an agreed way, so that all public administrations contributing to the delivery of European public services can understand the overall business process and their role in it;
- achieving agreement between administrative entities how to structure their interactions. This involves finding instruments to formalize mutual assistance,
- joint action, and interconnected business processes in connection with cross-border service provision. Examples of such instruments are Memoranda of Understanding on joint actions and cooperation and/or Service Level Agreements signed between participating public administrations. For cross-border action, they should preferably be multilateral agreements;
- integrating business processes and related data exchange;
- change management to ensure the accuracy, reliability, and continuity of the service delivered to other public administrations, businesses, and citizens.

Achieving organizational interoperability requires some key factors set on place. These factors are specified in the table given below.

Key factor	Explanation
Clear link between cross-organizational processes/services and the business strategies of the broader agencies	In a public administration environment, this means that the design and execution of the full set of public services by each separate agency and even more importantly the set of the new services that will derive from collaboration and interoperation among public administration agencies should be based on and be compliant with the general strategy and policy of the agencies involved and linked to their broader strategic mission and vision
Modelling and visualization of public administration services/processes	The modelling of the different processes involved in the workflow of the administration is being perceived as a crucial factor and it should be the first step prior to the design of new electronic services. Appropriate modelling of services and processes may support the service/process visualization and vice versa. Process diagrams visualizing the integration of systems should be structured through a series of views. These series of views should start with a customer oriented view, or some other actor's view, presenting the business level and add more and more details moving from a business perspective to a more technical perspective. Among other things, process modelling and visualization serve as vital preconditions to service monitoring. Both the explicit description of an electronic service (modelling), and the ability to monitor its current execution state bring very valuable visibility and transparency to the entire system
Involvement of the users by setting up communities of practice in the process of new service design	Organizational interoperability is "user-centric" in nature and requires the active involvement of the users in question (in this case, governments, public administration agencies and citizens/businesses). To ensure this customer-centric approach to service provision and to improve the efficacy of the public service, public organizations need to use their constituents to evaluate their internal processes, procedures and structures
Reuse of knowledge and experience related to the execution of internal and cross-agency business processes /services from the private sector	Public Administration agencies can easily reuse the experiences and models that have been successfully implemented in the private sector. To this end, e-business models developed in the enterprise sector should be assessed. Their use by public administration should also be encouraged where appropriate. Public organization could try to learn from these experiences and transfer knowledge to their own cross-agency and constituent relationships
Support of multi-channel service	This requirement calls for a loosely coupled back vis-à-vis front office systems to allow the delivery of services through

delivery	different and alternative channels
Identification and documen-tation of com-mon service functionality and features across public administration agencies	An organizational interoperability program needs to address possible common functionality across services and develop means for providing this identified common functionality. This common service layer is usually called Shared Service Layer and/or Auxiliary Services and includes infrastructure services such as authentication, e-payment, security, digital signature, electronic IDs, etc. In addition to such technical infrastructure, under this factor one can also include artefacts such as a common public administration service model. Instead of having each public administration organization develop its own infrastructure to support this type of functionalities, a centralized approach seems to be highly preferable as it creates economies of scale, provides common solutions for overall public administration and releases resources to be used effectively at the local level
Consensus on the mana-gement and responsibility of cross-orga-nizational processes	At any time, all actors participating in an electronic service (e.g. civil servants, citizens) should be able to know what is the status of the electronic service, in other words, who is responsible for its prior, present and next step(s). It seems that in most cases a central ownership of the overall service execution should be maintained by a single organization, most probably the actual service provider

Technical aspect of interoperability

An interoperability technology is an integrated, automated set of capabilities that makes it easier to share resources. The shared resources are usually data, but interoperability technologies may also promote the sharing of software, physical components, or even people. A fully deployed interoperability technology is one whose use has already saturated most of its potential application areas. An example of a fully deployed interoperability technology is American Standard Code for Information Interchange (ASCII), a old standard for exchanging character data that has almost totally replaced alternative character coding technologies such as Extended Binary Coded Decimal Interchange Code (EBCDIC) for the global exchange of character data. Fully deployed interoperability technologies may be extended or replaced by new technologies, but once in place they tend to remain stable due to the high cost and lack of benefits of replacing them with a comparable alternative.

Technical interoperability is concerned with all technical issues (technologies, standards, policies) to guarantee that the technical components of the information systems of the collaborating authorities will be able to work together. Therefore, technical interoperability covers the technical aspects of linking information systems. It should be noted that technical interoperability is concerned not only with technologies at the physical connection layer (such as network protocols), but also with technologies that support the organizational and the semantic layers. It includes aspects such as interface specifications, interconnection services, data

integration services, data presentation and exchange, etc. Therefore, technical interoperability should be ensured, whenever possible, via the use of formalized specifications

The technical interoperability is considering at the following fields:

- core technical interoperability covers all technical issues that are related to and support the very notion of interoperability, that is, data, information and meaning exchange and/or seamless distributed process execution (e.g. understanding the data syntax and/or semantics) amongst different information systems and organizations;

- supportive technical interoperability covers broader technical issues that do not directly affect this central interoperability function and that although are common in almost all information systems implementations, become more challenging and difficult to handle in environments where interoperation is required (e.g. availability).

In the core technical Interoperability the development and usage of the technologies are considered following key factors:

- data schemas and definitions; - SOAs and workflows;

- Semantic Web; - Semantic Web Services.

The supportive technical interoperability is considering at following key factors:

- accessibility - the front-end of an e-Government application/system must satisfy user needs regarding usability and accessibility (easy access to information and services);

- multilingualism and multiplatform devices – e-Government applications/systems should be multilingual and should support multiplicity of interface devices;

- security and privacy - data confidentiality and security mechanisms are considered as important aspects that need to be addressed in a technical interoperability dimension;

- subsidiary - the front-end should be able to provide different functionalities, modules, and options according to user rights belonging to different user categories;

- open standards - standards play a key role in enabling technical interoperability. Government policies that support the implementation or adoption of open standards improve technical interoperability and benefit governments as a whole.

The main technologies are often divided into four categories: structure/information technologies, structure/service technologies, semantic/information technologies, semantic/service technologies.

Technical interoperability – types of integration

The Conceptual Integration focuses on concepts, metamodels, languages and model relationships. It provides us with a modeling foundation for systemizing various aspects of interoperability, such as:

- Interoperability of processes aims to make various processes work together. A process defines the sequence of the services (functions) according to some specific needs of an organization. In a networked organization, it is also necessary to study how to connect internal processes of two organizations to create cross-organizational business process. This is supported by the CBP (cross-organizational business process) meta-model;

- Interoperability of services is concerned with identifying, composing and executing various applications (designed and implemented independently). Services are an abstraction and an encapsulation of the functionality provided by an autonomous entity. Modeling flexible

execution and composition of services can be supported by the platform-independent model for service-oriented architecture) metamodel;

- Interoperability of information/data refers are related to the management, exchange and processing of different documents, messages and/or structures by different collaborating entities.

The Applicative Integration focuses on methodologies, standards and domain models. It provides us with guidelines and patterns that can be used to solve real-world ICT interoperability issues. A methodology for applicative integration should be adapted to the business situation at hand. It should allow for both a Model Driven Development (MDD) and an Application Driven Methodology (ADM) approach depending on whether new solutions are to be developed or existing solutions are to be integrated. In some circumstances there will be a need for both, e.g. developing new services using service composition to integrate existing services. The methodology focuses on the models to develop and how to develop them. The models in question will depend on technical issues, business domain issues etc.

The Technical Integration focuses on the development and execution environment. It provides us with tools and solutions to develop and execute software models.

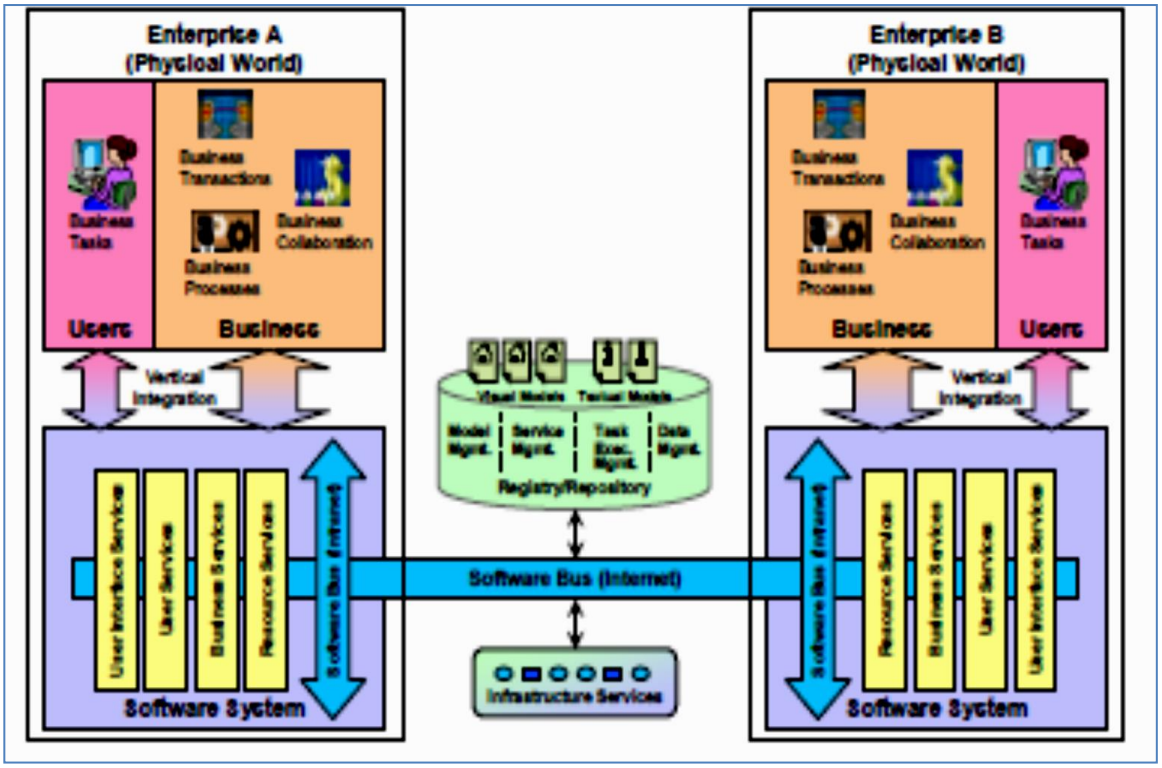


Figure 2-17

We will use the software bus as an architectural pattern for handling technical integration of software systems. The software bus will make us of infrastructure and registry/repository services. A software system can be structured according to a tiered architecture. We have identified four main tiers that should be seen as logical separations of a software system and not as a 4-layered architecture.

1. User interface tier provides presentation and user dialog logic. Sometimes, it is useful to make the presentation and user dialog separation explicitly, in particular to support reuse of user dialog on multiple platforms with different graphical capabilities, e.g. Web, PDA and Mobile phones.

2. User service tier provides the user's model, which may include user session logic and user-side representations of processes and information. It is an abstraction for a set of business services, making the business service provision (and the communication mechanisms) transparent to the user interface tier.

3. Business service tier provides components that represent business functionality and pervasive functionality (vertical vs. horizontal services). This tier provides enterprise-level services, and is responsible for protecting the integrity of enterprise resources at the business logic level. Components in this tier can be process-oriented, entity-oriented or workflow-oriented. For performance reasons, entity-oriented components are typically not exposed outside of this tier.

4. Resource services tier provides global persistence services, typically in the form of databases. Resource adapters (e.g. JDBC or ODBC drivers) provide access, search and update services to databases and its data stored in a database management system (DBMS) like Oracle or Sybase.

In addition to these four tiers we need a software communication bus so that services deployed at the various tiers can interoperate both within a tier and across tiers. The Connection interoperability is defined as "Ability of information systems to exchange signals" and is the most basic technical interoperability. Without connection interoperability there would be no way to transfer information between two systems. Connection interoperability assures the existence of a common channel for the systems to send information over. The use of communication standards such as TCP/IP solves this interoperability problem because it can be expected that every system understands the information sent with this protocol.

Main technologies

The Technical Interoperability on the other hand refers to the mere possibility to exchange information. Technical interoperability includes the definition of transmission routes and protocols (for instance SOAP, HTTP, FTP, IP, SMTP). The respective standards are parts of the technology viewpoint, for instance section "Communication". A common language for data description is the required technical precondition for interoperability XML is identified as the mandatory standard for exchanging data.

The main directions of the technical interoperability technologies can be systematized as follows:

A. Process modeling – the role models and flow charts should be used to define simple processes. All the roles and systems related to a process must be identified, and the process steps must be described in the form of flow charts.

The Unified Modeling Language (UML) should be used for object-oriented modeling in the preparation and documentation of large projects. Use cases and activity diagrams are a particularly tried-and-tested way of creating and coordinating transparent specifications. These specifications can be reused with the respective tools.

B. Data modeling – the Entity Relationship Diagrams should be used when developing relational database schemas. Functional data models for a special rough concept should also be presented using ER diagrams. UML should be used in data modeling for object-oriented applications. For instance, class diagrams are the approach of choice which can also be used in other applications or by other tools. XML data structures can be directly generated from the corresponding specifications.

C. Interchange formats for data - XML v.1.0 is a language derived from the Standard Generalized Markup Language (SGML) which should be used for structured data description.

The language enables the extension and addition of tags. The data described can be prepared for presentation using the Extensible Stylesheet Language (XSL).

XML is to serve as the universal and primary standard for the interchange of data between all the information systems relevant for administrative purposes. New systems to be installed should be capable of exchanging data using XML. Existing systems do not necessarily have to be XML-enabled.

D. Data transformation - if applications use different XML schemas, conversion from one format to another can become necessary for data interchanging purposes. This format conversion operation is carried out via the XSLT language defined by W3C as part of XSL (Extensible Style sheet Language).

E. Application architecture - this direction defines programming languages and technologies for implementing the application architecture. The first part of this are the standards for the middleware of the e-Government architecture module with special emphasis on the aspect of application integration. This is followed by an extension of the standards to cover applications without middleware, so that the middleware standards can also be used for simpler applications.

E1. Application architecture with middleware - the development and integration of the following applications (integrated applications) on the middle layer, i.e.

a. One-for-all offers (OFA offers)

b. applications which directly integrate basic components or libraries provided for this purpose, and

c. applications designed, as a whole or in part (components), for re-use (porting) require the use of Java 2 Platform, Enterprise Edition (J2EE) technologies. J2EE is a specification which defines several programming interfaces and a development process. J2EE in its entirety constitutes an architecture that considers and supports major aspects of business-critical applications.

E2. Application architecture without middleware - in addition to the standards discussed in the previous section, the following technology is also available for simple e-Government applications without middleware. PHP (Hypertext Preprocessor) can be used for applications without an integration requirement, i.e. non-distributed, stand-alone applications which do not communicate with one of the one-for-all offers (OFA offers), with legacy systems or other e-Government applications.

F. Client Applications - the client is a software on a terminal device which makes use of a service offered by middleware. The client layer includes both the classical user site with all the options state-of-threat technology has to offer in order to interact with public administrations, with access to information possible via different media. The following media are currently the most popular, so that optimum conditions for the widespread use of e-Government applications will exist if the information on offer is tailored to these devices:

a. Computers (PCs, notebooks)

b. Mobile phones / personal digital assistants (PDAs)

c. External systems (e.g. ERP systems by industrial companies)

The so-called "thin client" seems to be the most promising device in terms of public acceptance. Thin clients come with very low-profile hardware and software requirements and rely on the server to provide as much functionality as possible.

G. Communication - within the "communication" element, a distinction is made between application, middleware and network protocols as well as directory services.

G1. Middleware communication - in the case of middleware communication, a distinction is made between server applications that communicate within an administration and client applications outside the administration which communicate with an administration server

G2. Server-to-server communication within the administration - Java Remote Message Interface (RMI) is particularly suitable for internal communication between Java objects. Via RMI, an object on a Java Virtual Machine (VM) can invoke methods of an object that runs on another Java VM. Java Remote Method Invocation is part of the Java 2 Standard Edition (J2SE) and hence also part of the Enterprise Edition (J2EE). Simple Object Access Protocol (SOAP) should be used for communication between the party supplying the server and the user of a server within the meaning of the SOA reference model. SOAP can be used to exchange structured data as XML objects between applications or application components via an Internet protocol (e.g. via HTTP).

G3. Client-to-server communication - web services should be used for access by client applications via the Internet to server applications at administrations. By providing a web service layer for an existing server application, it enables client systems to invoke the functions of the applications via the Hypertext Transfer Protocol (HTTP). A web service is a software component which uses SOAP in order to communicate with other components via the HTTP standard protocol. XML is used for the message content itself. XML was already described as a universal and primary standard for the interchange of data between all the information systems relevant for administrative purposes. The Web Service Interoperability Organization (WS-I) defines profiles of existing standards in order to facilitate the compilation of the required standards. The profile to be applied is WS-I-Basic v1.1 and includes XML Schema v1.0, SOAP v1.1, WSDL v1.1 and UDDI v2.0.

G4. Network protocols - the IT environment of administrations currently uses IP v4 (RFC 0791, RFC 1700) in conjunction with TCP (Transmission Control Protocol - RFC 793) and UDP (User Datagram Protocol - RFC 768). IP v6 is the next version of the IP protocol which is not yet very widely used. One of the changes compared to the current version 4 is the extension of the IP address to 128 bits in order to permit addressing of multi-embedded and mobile IP-based systems in future.

G4. Application protocols - the File Transfer Protocol (FTP - RFC 959, RFC 1123, RFC 2228, RFC 2640) is considered the standard file transfer protocol. FTP is one of the oldest Internet services. FTP enables the shared use of files, offers users standardized interfaces for different file system types, and transfers data in an efficient and reliable manner. FTP is typically somewhat faster than HTTP when larger files are to be downloaded.

G5. Directory services – the Lightweight Directory Access Protocol (LDAP v3 - RFC 2251) is an X.500-based Internet protocol which is optimized with regard to hierarchically structured information and which is used for directory service access

Platforms enabling technical interoperability

A Service Oriented Architecture (SOA) is a software model in which the concept of a ‘service’ is an abstraction of a function used by an application. SOA logically decouples the service requester from the service provider by isolating the service definition from a service implementation.

SOA addresses the business demand for applications to be responsive to business needs and to adapt to dynamic business environments. In a SOA environment one often needs to facilitate the communications between service requesters and service providers that possess differing service characteristics (in such cases, service metadata may be available that describes a service’s requirements, capabilities or other general information regarding service usage).

B. The Enterprise Service Bus (ESB) provides a vital ingredient of the SOA environment. An ESB decouples the service requester from the service provider by mediating (if necessary) the service interaction between communicating participants. We call this decoupling service virtualization. Interposed between requester and provider, an ESB simplifies service connectivity by dealing with the service selection process and handling any mismatches that might occur. For example the requesters and providers might have different security or reliability requirements, or the interface provided by the service might not exactly match the interface expected by the requester. An ESB can also be used to introduce additional functionality into the communications path between interacting services. We call this aspect-oriented connectivity.

An ESB is a recommended element for any SOA-based solution that requires mediation to facilitate a requester-provider interchange.

An ESB includes a distributed, configurable infrastructure, whose tasks are to provide:

• Routing: The ESB acts as a match-maker between service requester and service provider.

• Conversion: The ESB handles protocol or interaction differences.

• Transformation: The ESB can be programd to handle interface mismatches that might occur and compensate accordingly, if possible.

• Aspect-oriented connectivity: Additional “added-value” functionality.

The services that connect to the ESB may declare their service characteristics or their expectations relating to service interactions (including any requirements on other participants).

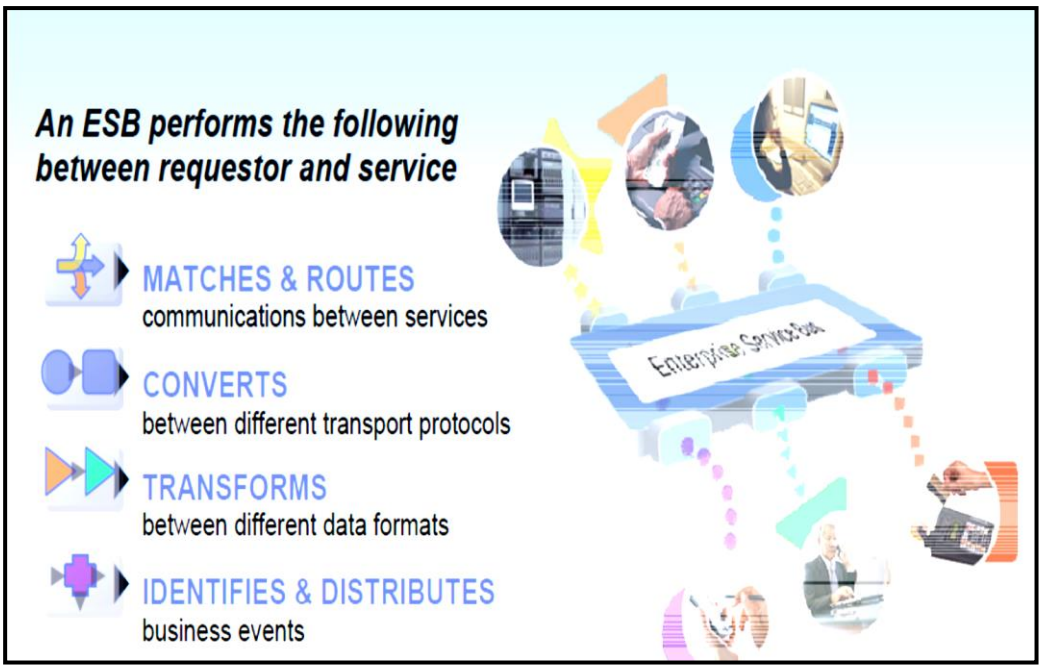


Figure 2-18

The ESB is given responsibility for delivering messages between requesters and providers, ensuring the required functionality as defined for the interaction. Service requesters send requests which are then mediated (if required) by the ESB. The ESB routes and transforms each request message into a format acceptable to the service provider. Service providers receive these requests and can react to them without having to know about a request's origin. Similar mediation takes place for any response message sent back by the service provider. The ESB is

transparent to the service requesters and providers: it matches a service requester's requirements with a service provider's capability, adding value to service interactions without changing the service providers or requesters themselves.

Information exchange

The National Institute of Standards and Technology defined **electronic data interchange (EDI)** as "the computer-to-computer interchange of strictly formatted messages that represent documents other than monetary instruments. EDI implies a sequence of messages between two parties, either of whom may serve as originator or recipient. The formatted data representing the documents may be transmitted from originator to recipient via telecommunications or physically transported on electronic storage media." It distinguishes mere electronic communication or data exchange, specifying that "in EDI, the usual processing of received messages is by computer only. Human intervention in the processing of a received message is typically intended only for error conditions, for quality review, and for special situations. For example, the transmission of binary or textual data is not EDI as defined here unless the data are treated as one or more data elements of an EDI message and are not normally intended for human interpretation as part of online data processing".

The most popular EDI standards are as follows:

- American National Standards Institute Accredited Standards Committee X12 (ANSI ASC X12),

- United Nations/Electronic Data Interchange For Administration, Commerce and Transport (UN/EDIFACT) ,

- electronic business XML (ebXML).

ANSI ASC X12, chartered by the American National Standards Institute (ANSI) in 1979, develops EDI standards for national and global markets. With more than 315 X12 EDI standards and increasing X12 XML schemas, ASC X12 enhances business processes, reduces costs and expands organizational reach. Members include standards experts from health care, insurance, transportation, finance, government, supply chain and other industries. The ASC X12 body comes together three times each year to develop and maintain EDI standards that facilitate electronic interchange relating to business transactions such as order placement and processing, shipping and receiving information, invoicing, payment and cash application data, and data to and from entities involved in finance, insurance, transportation, supply chains and state and federal governments.

Committee members jointly develop and promote EDI standards that streamline business transactions, using a common, uniform business language. With more than 275 transaction sets, ASC X12 standards can be used to electronically conduct nearly every facet of business-to-business operations.

United Nations/Electronic Data Interchange For Administration, Commerce and Transport (UN/EDIFACT) is the international EDI standard developed under the United Nations. The work of maintenance and further development of this standard is done through the United Nations Centre for Trade Facilitation and Electronic Business (UN/CEFACT) under the UN Economic Commission for Europe, in the Finance Domain working group UN CEFACT TBG5. EDIFACT has been adopted by the International Organization for Standardization (ISO) as the ISO standard ISO 9735.

The EDIFACT standard provides:

- a set of syntax rules to structure data;

- an interactive exchange protocol (I-EDI);

- standard messages which allow multi-country and multi-industry exchange.

Example of XML-based standards is Electronic Business using eXtensible Markup Language, (e-business XML or ebXML). It is typically referred to, is a family of XML based standards sponsored by OASIS and UN/CEFACT whose mission is to provide an open, XML-based infrastructure that enables the global use of electronic business information in an interoperable, secure, and consistent manner by all trading partners. The ebXML architecture is a unique set of concepts - part theoretical and part implemented in the existing ebXML standards work.

Telecommunication and networking

European Information and Communications Technology Industry Association (EICTA) defines telecommunication and network Interoperability as **"the ability of two or more networks, systems, devices, applications or components to exchange information between them and to use the information so exchanged".**

Quoting the Institute for Telecommunication Sciences **"Interoperability involves consideration of how information is exchanged (through networks of networks) and used (through user-based and network-based applications and services). Interoperability issues involve, for example, specification of protocol suites, provision of basic and enhanced services, secure information exchange among authorized users, user selection of transit networks and content providers, connection admission control, end-to-end quality of service, network management, and user data element format, processing, and storage/retrieval."**

Telecommunication networks interoperability is a topic of increasing importance, because it is the main enabler for the vision of service convergence. Contrary to what could have been anticipated, these trends have not produced a simplification or reduction of infrastructure and scenarios: on the contrary, the result of this transformation is an explosion of heterogeneity, an explosion of the number and types of:

- networks,

- services and applications,

- operators and service providers.

This world of heterogeneous elements exerts a pressing and critical demand for the concept of interoperability and its variations:

- interoperability of networks and of network management systems,

- interworking of applications and transparency between services,

- interfacing among operators and service providers, exchange of Quality of Service (QoS), Service Level Agreement (SLA) information and accounting rules.

Network interoperability is indispensable in order to achieve end-to-end connectivity. The miracle of being able to call anybody in the world using the old Public-switched Telephone Networks (PSTNs) is due to interoperability. The same applies for the ability to call any Global System for Mobile communication (GSM) phone in the world, or to connect to any computer via the Internet. The more and more diverse networks exist, the greater the need to ensure that they can interoperate, so that end-to-end communication is possible.

At the same time, the more difficult the problem becomes. Interoperability is of benefit to all actors of the value chain: The user benefits because he can communicate with whom he wants

or needs anywhere and anytime, with a single terminal. The network operator benefits because it can select the best equipment from different manufacturers according to the best price and performance. The manufacturer benefits because it can sell the same equipment to different countries or operators, and benefit from economies of scale in fabrication and marketing. Public authorities benefit because they can coordinate responses from different critical infrastructures networks.

Interoperability can be achieved either by having the two networks conform to a common protocol standard, or by defining a standard interface to which all networks need to adhere, or by providing a gateway between them that translates between the two protocols.

In practical terms, standards are the tools that make possible the design of interoperable systems. Actually, to speak of interoperability is to speak of standards, and vice-versa. An interoperability standard is a document that establishes engineering and technical requirements that are necessary to be employed in the design of systems, units, or forces and to use the services so exchanged to enable them to operate effectively together. There are several organizations, some established by governments and some by industry initiatives that create standards.

The key standard groups dealing with telecommunications networks interoperability are:

- International Telecommunication Union - Telecommunications Sector (ITU-T) focus on Multi-media, Satellite, Fiber Systems, Radio systems, Broadcast Video areas,

- European Telecommunications Standards Institute (ETSI) focus on electronic communications networks and services, and related areas such as intelligent transportation and medical electronics areas,

- Committee T1-Telecommunications (Committee T1) focus on Multi-media, Network Reliability areas,

- Institute of Electrical and Electronics Engineers (IEEE) focus on Local Area Networks, Software Languages, Test and Measurements Internet, focus on TCP/IP protocol and its Uses to Transport Information, Telnet, FTP protocols focus,

- Engineering Task Force (IETF) on Service and Network Management,

- Network Management Forum (NMF)

Standards and agreed specifications are clearly important, but manufacturers, operators and users will be confused if new specifications are introduced too frequently, are contradictory, or have not has enough practical validation and pre-service trailing.

Interoperability between different types of networks encompasses the following levels of inter-working:

- physical level (e.g. opto-electric-radio),

- network level (e.g. signaling and control functions in homogeneous and heterogeneous networks; inter-operability between fixed & mobile networks, and optical & electrical networks; interfacing with service-provider networks),

- application level (e.g. interfacing with content providers; user Quality of Services(QoS)),

- management level (e.g. inter-operability between network management systems; accounting schemes; guarantee and preservation of QoS).

Human interface design

Human (user) interface design (HID) is a central issue for the usability of a software product. Based on theoretical and empirical work in software ergonomics (human factors) in the seventies and the eighties, standards have been developed for defining the usability of software products. One of the structural basis standards has become the International Federation for Information Processing (IFIP) user interface reference model. The model proposes four dimensions to structure the user interface: the input/output dimension (the look), the dialogue dimension (the feel), the technical or functional dimension (the access to tools and services), and the organizational dimension (the communication and co-operation support). The model has greatly influenced the development of the international standard ISO 9241 describing the interface design requirements for usability

The dynamic characteristics of a system are described in terms of dialogue requirements contained in seven principles of the ergonomics standard. This standard establishes a framework of ergonomic ,,principles" for the dialogue techniques with high-level definitions and illustrative applications and examples of the principles. The principles of the dialogue represent the dynamic aspects of the interface and can be mostly regarded as the ,,feel" of the interface.

The seven dialogue principles are:

- suitability for the task: the dialogue is suitable for a task when it supports the user in the effective and efficient completion of the task,

- self-descriptiveness: the dialogue is self-descriptive when each dialogue step is immediately comprehensible through feedback from the system or is explained to the user on request,

- controllability: the dialogue is controllable when the user is able to initiate and control the direction and pace of the interaction until the point at which the goal has been met,

- conformity with user expectations: the dialogue conforms with user expectations when it is consistent and corresponds to the user characteristics, such as task knowledge, education, experience, and to commonly accepted conventions,

- error tolerance: the dialogue is error tolerant if despite evident errors in input, the intended result may be achieved with either no or minimal action by the user,

- suitability for individualization: the dialogue is capable of individualization when the interface software can be modified to suit the task needs, individual preferences, and skills of the user,

suitability for learning: the dialogue is suitable for learning when it supports and guides the user in learning to use the system.

The information presentation is described in the standard for the organization of information (arrangement, alignment, grouping, labels, location), for the display of graphical objects, and for the coding of information (abbreviation, color, size, shape, visual cues) by seven attributes. The ,,attributes of presented information" represent the static aspects of the interface and can be generally regarded as the ,,look" of the interface. The attributes are detailed in the recommendations given in the standard. Each of the recommendations supports one or more of the seven attributes. The recommendations for presentation of information also contribute to the application of the dialogue principles, mainly to the conformity with user expectations.

The seven presentation attributes are as follows:

- clarity: the information content is conveyed quickly and accurately,

- discriminability: the displayed information can be distinguished accurately,

- conciseness: users are not overloaded with extraneous information,

- consistency: a unique design, conformity with user's expectation,

- detectability: the user's attention is directed towards information required,

- legibility: information is easy to read,

- comprehensibility: the meaning is clearly understandable, unambiguous, interpretable, and recognizable.

The user guidance in the standard describes that the user guidance information should be readily distinguishable from other displayed information and should be specific for the current context of use. User guidance can be given by the following five means:

- prompts indicating explicitly (specific prompts) or implicitly (generic prompts) that the system is available for input,

- feedback informing about the user's input timely, perceptible, and non-intrusive,

- status information indicating the continuing state of the application, the system's hardware and software components, and the user's activities,

- error management including error prevention, error correction, user support for error management, and error messages,

- on-line help for system-initiated and user initiated requests with specific information for the current context of use.

Interoperable content management

The basis of interoperable content management is the unification and formalization of data definitions. This can be set up as interoperability at "data level". The interoperability can be defined in similar way at the level of data structures, at the level of electronic documents, etc. The tools for practical achievement of interoperability are well known- XML-repositories, clearing processes and so on.

In each country most of the legislative acts set up definitions of data and documents, used in administrations and by citizens. Those data and documents can be pointed out as a "core components", which represent the content created and processed by administrations. Additional data is needed, in order to manage this content. The suitable basis for defining this data is the service oriented administrative organization (SOAO)

The Content Management Interoperability Services (CMIS) standard defines a domain model and Web Services and Restful AtomPub bindings that can be used by applications to work with one or more Content Management repositories/systems.

The CMIS interface is designed to be layered on top of existing Content Management (CM) systems and their existing programmatic interfaces. It is not intended to prescribe how specific features should be implemented within those CM systems, not to exhaustively expose all of the CM system's capabilities through the CMIS interfaces. Rather, it is intended to define a generic/universal set of capabilities provided by a CM system and a set of services for working with those capabilities

In the common vision for an European Interoperability Architecture (EIA), a consensus is expressed on interoperability agreements that are needed at European level for cross-border and cross-sector interoperability between public administrations. Using the common vision for an EIA, EC projects and Member State administrations can benefit from reusing the interoperability

agreements and solutions that are provided or implemented at European level. The interoperability agreements that should be included in the common vision for an EIA represent a selection of the interoperability agreements of the Rich Internet Application (RIA). Such a selection was made based on a scoring exercise and a consensus discussion with all participants, leading to a working hypothesis of the common vision. This working hypothesis was revisited, by discussing whether these EIA agreements should be added, changed or removed.

Incident handling interoperability

In recent years, the use of public e-Communications networks has expanded rapidly to encompass a far wider range of services and applications. These networks have become critical infrastructure for Europe's Member States, public institutions, societies and economies.

The reformed Regulatory Framework for electronic communications networks and services further reinforces the policy commitment to incident reporting. The new framework addresses many different issues, but among the security and integrity provisions to be implemented by providers, there is one that establishes a legal obligation to report serious incidents to the competent authorities.

The Special publication 800-61 of National Institute for Standardization and Technology (NIST) define incident as follow: "A computer security incident is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices". Examples of incidents are as follows: - denial of service, - malicious code, - unauthorized access, - inappropriate usage.

Incident response has become necessary because attacks frequently cause the compromise of personal and business data. Incidents involving viruses, worms, Trojan horses, spyware, and other forms of malicious code have disrupted or damaged millions of systems and networks around the world. Heightened concerns about national security and exposure of personally identifiable information (PII) are also raising awareness of the possible effects of computer-based attacks. These events—and many more—make the case daily for responding quickly and efficiently when computer security defenses are breached. To address these threats, the concept of computer security incident response has become widely accepted and implemented in the government, private sector, and academia. The following are benefits of having an incident response capability:

- responding to incidents systematically so that the appropriate steps are taken,

- helping personnel to recover quickly and efficiently from security incidents, minimizing loss or theft of information and disruption of services,

- using information gained during incident handling to better prepare for handling future incidents and to provide stronger protection for systems and data,

- Improving properly with legal issues that may arise during incidents.

It is important that organizations have a formal, focused, and coordinated approach to responding to incidents. To effectively implement such a capability, an organization should have an incident response plan. The plan provides the organization with a roadmap for implementing its incident response capability. The plan should provide a high-level approach for how the incident response capability fits into the overall organization. The organization may need to communicate with outside parties regarding an incident.

Planning and implementing an incident reporting scheme are challenging goals. To achieve success, it is necessary to carefully and diligently proceed through many individual steps, working out a huge amount of detail in the process, while balancing the sensitivities of various

organizations and individuals with whom you will have to work and coordinate, and cooperate in both establishing and then managing the scheme. These numerous steps together form the lifecycle of the incident reporting scheme. The lifecycle could be depicted as a four-stage process. It begins with identifying the incident reporting need and setting the basic goals of scheme. The lifecycle then proceeds to engaging cooperation of the potential reporting parties – which in fact is an ongoing effort that shouldn't stop as long as the scheme is running. The reporting procedures are then defined, enabling the launch of the scheme. Finally, every scheme needs an ongoing management that would, on one hand, provide feedback that enables adjustment of the reporting procedures, and on the other hand enable longer-term improvement and evolution of the scheme. Thus the lifecycle may naturally flow into a re-assessment of the incident reporting needs and to establishing additional reporting arrangements.

Semantic aspects of interoperability

Semantics is the study of meaning. It's as old as the ancient Greeks. For most of us it was a deadly dull sub-discipline of philosophy, to be avoided. But it turns out that we can't avoid it. We are drowning in a sea of data which occasionally is generously referred to as "information." But the truth is that almost all of it must be interpreted by humans to be of any use. The growth and availability of data and, therefore, our need to consider it in decision-making and planning is growing exponentially, and our systems, rather than helping with this, are for the most part contributing to the problem.

Semantic technologies include software standards and methodologies that are aimed at providing more explicit meaning for the information that's at our disposal. This takes different forms depending on where in the information cycle the semantic technology is applied and which area of the problem it is addressing; as we'll get into later in this paper, there are some commonalities between the technologies but also many differences.

The semantic framework consists of the following:

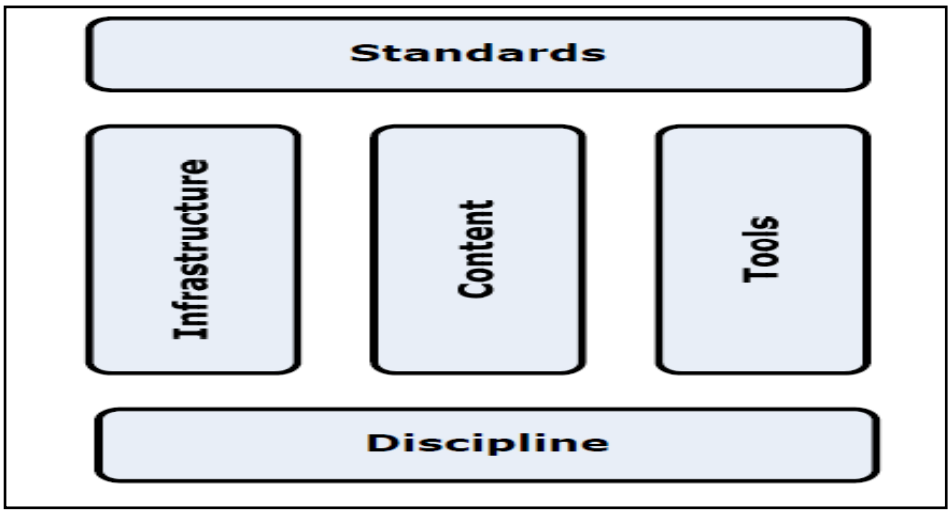


Figure 2-19

This aspect of interoperability is concerned with ensuring that the precise meaning of exchanged information is understandable by any other application not initially developed for this purpose. Semantic interoperability enables systems to combine received information with other information resources and to process it in a meaningful manner. Semantic interoperability is therefore a prerequisite for the front-end multilingual delivery of services to the user.

Semantic interoperability is a necessary component in achieving full interoperability since it is concerned with ensuring that the precise meaning of exchanged information is understandable by other parties. It is an essential design element for pan-European e-Government services, which will have to choose between a centralized architecture using single pan-European resources or a decentralized one supported by translation gateways.

It should be stressed from the beginning that semantic interoperability cannot be achieved separately from the other interoperability dimensions: sharing knowledge implies that the organizational environment makes it easy and desirable, hence addressing the two dimensions of technical and organizational interoperability as well as the semantic one.

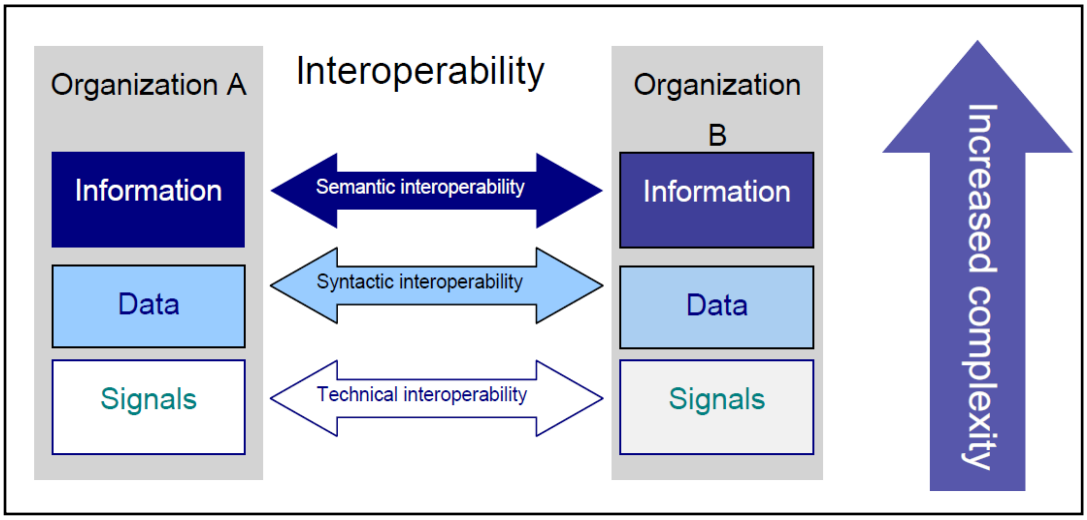


Figure 2-20

The main semantic conflicts are related to the structure of data and the meaning of data. The following categorization of semantic conflicts can be considered2:

- data-level conflicts are related to differences in data domains caused by the multiple representations and interpretations of similar data:
- data-value conflicts, e.g. the value “foreigner” in one database may mean that the person is not a citizen of the country, while in another database it may mean that the person is not a citizen of the European Union;
- data representation conflicts, e.g. a date can be represented as 06-30-2005 in one database, as 30-06-2005 in another one and as 30-Jun-2005 in a third one;
- data unit conflicts, e.g. building heights can be measured in centimetres in one database and in inches in another one;
- data precision conflicts, e.g. building heights can be graded as “high”, “medium”, and “low” in one database and as scale A, B, C or D in another one;
- data language conflicts, e.g. when information is retained in different languages.
- schema-level conflicts are related to differences in logical structures and/or inconsistencies in metadata:
- naming conflicts, e.g. the name “Citizen” in one database is used to capture the same information as the name “Beneficiary” in another database;

- generalization conflicts, e.g. when one database has a representation for "Citizens", while another database has two separate representations for "Males" and "Females".

The issue of semantic interoperability has very specific and challenging dimensions when it is considered in relation with setting-up pan-European e-Government Services (PEGS):

- Semantic assets are crucial in PEGS, both for achieving full interoperability, and also for achieving proper profiling of user interfaces given the large spectrum of European users;
- Adequate support of multilingualism is required for any existing or future PEGS deployed in Europe;
- Mapping rules between various semantic assets is sometimes the only, but difficult, way to achieve semantic interoperability, given that imposed uniform standards are often impossible to achieve.
- Properly addressing such challenges in the European Union implies to develop sophisticated semantic assets. Given that harmonization of the use of such assets is not possible in most cases, it also implies to deploy semantic gateways, which are services in charge of translating a message exchanged between two different actors, or adding useful contextual information to this message to help in its good interpretation by the recipient. To fulfill this role, semantic gateways need to discover and collect semantic assets from clearinghouses or other registries, or exploit those locally available.

The only way to provide semantic interoperability with sufficient reliability is to use controlled terminologies, and controlled mapping-tables and mapping-rules for any transformation. All those controlled terminologies, mapping-tables and mapping-rules that are developed and used for the purpose of enabling semantic interoperability in a distributed information system are called in the sequel Semantic Interoperability Assets (SIA). They may take several forms (thesauri, nomenclatures, ontologies, transcoding rules, etc.) and may be encoded using various technical standards.

Looking at all the national or international initiatives, which have produced semantic assets used by a large user community, we can identify a few success factors that should inspire a European policy aiming at facilitating the development of pan-European interoperable information systems. The most noticeable success-factors seem to be organizational, from which we can draw the following conclusions:

- long-term sustainability - a semantic asset is long and expensive to produce. It needs to be permanently updated. Developing a semantic asset cannot be handled through a short duration project without visibility on the follow-up. This is also necessary to motivate the partners in the Member States to invest energy and resources in the development and adoption of such assets;
- catering for users' feedback - user feedback is extremely valuable for the maintenance and the update of the semantic assets. The maintenance process must include mechanisms ensuring that these users will have the opportunity to provide feedback to those in charge of updating the asset;
- transparent and open process for updating - stakeholders exploiting a semantic asset for publishing or exchanging information must have immediate access to the manuals or publications documenting the process through which the asset evolves.

This transparency is important to build confidence in the process, and hence in the reliability of the organization which is responsible for governing it;

- quality policy - the process must include quality control mechanisms. This means that it should not only establish how the asset is modified, but also what happens exactly when an error is discovered and reported. Modifying an asset must be planned. Transition mechanisms must be defined;
- adaptation to expected use - an asset must be designed with sufficient understanding of its intended use. A good semantic asset is not abstract knowledge about a domain. The choice of the terms and the granularity of the concepts must be chosen according to the expectations and background of future users. This obviously means that the sectors must be involved and take on an important part of the workload;
- focus must be on the process, not on the standards - any existing nomenclature or thesaurus may quite easily be encoded in XML. There is no other reason to privilege a standard or another than ease of publishing and reuse;
- publish and distribute existing assets in suitable formats - several European institutions (EU Commission, EU Parliament, European Patent Office …) have developed or have funded the development of a large number of multilingual dictionaries e.g.: definitions of acronyms, definitions of terms used in legal publications, etc. These resources should be made available in formats and under terms and conditions that may facilitate their reuse by all those – including the private industry - developing pan-European applications. This may require the identification of reusable dictionaries, to encode and publish them in a convenient exchange format (XML), and distribute them through an appropriate clearinghouse;
- identify, reuse and extend existing assets - national public administrations and EU institutions have a long and established track record in the development of classification systems, i.e.: thesauri, nomenclatures, taxonomies which are produced in the national language.

A large number of public organizations in Europe also contribute to the work of international societies, which produce classification systems. Domains covered by such national or international efforts are extremely diverse from cultural heritage to healthcare or other scientific areas. PEGS should be able to reuse and extend existing assets.

registries should play a key-role - the document entitled “Technical description of target e-Gov infrastructure for delivering PEGS”, published on behalf of IDABC explains in some details, how semantic interoperability in open architectures may be obtained thanks to some semantic gateways. Such architecture requests that semantic assets must be machine-browseable. They must be available from online services, using protocols and coding standards that facilitate the implementation of the semantic gateways.

Finally the document proposes broad lines of an action plan for the European Commission and for concerned stakeholders in the Member States, based on the factual analysis. The central item of the action plan is the set-up of a Semantic Interoperability Clearinghouse, which will disseminate semantic interoperability assets developed and used by public administrations and organizations in the EU Member States, namely: Core components with companion terminologies, taxonomy of services and life-events, nomenclatures of public

services, etc. A second function of the clearinghouse will be to facilitate the implementation of the semantic gateways.

SEMIC.EU (Semantic Interoperability Centre Europe) is an EU-Project to support the data exchange for pan-European e-Government services. Its goal is to create a repository for interoperability assets that can be used by e-Government projects and their stakeholders. SEMIC.EU is offering the following services for the public sector in Europe:

- it will provides access to interoperability assets, which have been developed in previous governmental projects;
- a clearing process will safeguard certain rules and standards to assure the quality of published assets;
- community features will be available on the platform, e. g. a forum to discuss best practices for the use of assets;
- it will invite to seminars and workshops that are related to its activities and
- it offers coaching services for the creation and/or reuse of interoperability assets.

The SEMIC.EU platform is primarily intended as a cooperation and collaboration platform, which deals with semantic interoperability assets. The resulting assets may be of pan-European nature and enable a partly or fully interoperable communication between the different administrations of the Member States.

SEMIC.EU is targeted to provide the conceptual base, technical infrastructure and support services in order to establish a pan-European repository for interoperability assets. It is a major goal to freely include all interested and related parties in the development of interoperability assets using an open and community-based process.

However, SEMIC.EU is neither a governmental agency nor a standardization committee of any kind. The platform holds neither the political power or the political intention to develop and enforce binding communication regulations for semantic interoperability, nor the intention to create new standards for inter-agency communication. Therefore, the SEMIC.EU platform should not be mistaken to represent any standardization efforts of any kind but as an enabler for harmonization between the communication partners.

CHAPTER 2.4

EUROPEAN INITIATIVES

The main programs and projects

Interoperability has 3 main aspects – organizational, semantic, and technical - which must be taken into account when developing a public service.

The programs **IDA (Interchange of Data Between Administrations), IDA II, IDABC (Interoperable Delivery of European eGovernment Services to Public Administrations, Business and Citizens), and ISA (Interoperability Solutions for European Public Administrations)** should be considered as a chain of sequent continuous efforts directed towards improvement of Public Administrations sector in the EU.

Similarly, **ICT PSP program (2007-2013)** is the successor of **e-TEN program (2000-2006).**

Whereas:

- eCODEX - E-justice Communication Via Online Data Exchange (2010-2013);
- epSOS – European Patients – Smart Open Services (2008-2013);
- PEPPOL – Pan-European Public Procurement Online (2008-2012);
- SPOCS - Simple Procedures Online For Cross-Border Services (2009-2012) and
- STORK - Secure Identity Across Borders Linked (2008-2012)
- are large scale pilots projects.

The IDA and IDABC programs

The IDA and IDABC programs together have provided a forum for exchange of ideas and experience, and have lent support to the execution of Community policies through sectorial projects leading to the establishment of a wide portfolio of operational trans-European networks and services in traditional policy areas such as agriculture, fisheries, employment, as well as in newer policy areas such as home and justice affairs, communicable diseases, and health and consumer protection. They also provided administrative sectors and member states with infrastructure services, i.e. frameworks, common services, generic and complementary tools aiming at achieving interoperability between the back-office administrative systems and processes, as well as between back- and front-office services

Taking into account e-Government initiatives existing at that time, the IDA Program gradually profiled itself as an e-Government program. It was focused on ‘networks’:

- use of IT in public administrations and facilitation of transition from paper-based to electronic exchanges across Europe;
- measures and services to be applied and used to ensure seamless interaction within and across networks at the trans-European level.

The program main activities supporting interoperability include the preparation of the draft version of the European Interoperability Framework and an XML Clearinghouse feasibility study.

The IDABC program launched in January 2005. It was a Community program managed by the EC's Directorate-General for Informatics, working in close cooperation with the member states and the different EC's services concerned.

IDABC contributed to the i2010 initiative of developing of the European public sector and played a key role in reaching the e-Europe 2005 objectives, more particularly in the field of e-Government .The objective of the IDABC program was to identify, promote, and support:

1. The development and establishment of European e-Government services;

2.The underlying interoperable telematics networks supporting the European member states and the European Community in the implementation of their respective policies and activities, achieving substantial benefits for public administrations, businesses, and citizens.

To achieve its objectives, the program:

- issued recommendations,
- developed solutions,
- provided services that enable national and European administrations to communicate electronically while offering modern public services to businesses and citizens in Europe.

IDABC was designed to help to achieve targets set in the area of e-Government by:

- continuing to promote the introduction of information technologies to policy domains, especially where this is facilitated by legislation;
- building a common infrastructure for cross-border information exchanges between public administrations in order to ensure efficient communications;
- encouraging the emergence of novel services for businesses and citizens.

The program provided benefits to the following groups:

public administrations, in particular national authorities and European institutions, because by providing a forum for information exchange and funding for IT solutions IDABC helped the administrations to improve the efficiency of their existing networks, it also offered generic services, common tools and guidelines that facilitate interoperability across European borders;

- citizens and enterprises which had possibility to use directly some of the IDABC networks or more open and efficient public services;
- IT and service providers which had opportunity to participate in the open calls for tenders in the framework of the program.

The IDABC program worked through providing funding to actions under two headings:

- **Projects of Common Interest (PCIs),** which focused on the use of IT solutions for specific sectors. They were actions in the policy areas of the EU concerning the establishment or enhancement of pan-European e-Government services in support of public administrations, businesses, and citizens;
- **Horizontal Measures (HMs),** which covered cross-sector networks, services, and tools. These measures were actions designed to support PCIs but also e-Government in general. Firstly, they provided and maintained infrastructure services for public services in the Community. Secondly, they initiated, enabled and managed the provision of horizontal pan-European e-Government services to

businesses and citizens in Europe, including related organizational and coordination aspects.

The ISA program

The Decision on the program "Interoperability Solutions for European Public Administrations" was adopted by the European Parliament and the Council on 16 September 2009. The program addresses the following needs:

- support the implementation of Community policies and legislation: from the internal market through the Lisbon Strategy to the Services Directive;
- avoid e-barriers to cross-boundary interactions due to lack of interoperability and common and shared solutions.

The ISA program focuses on back-office solutions supporting the interaction between European public administrations and the implementation of Community policies and activities. The program will support and promote:

- creation and improvement of common frameworks in support of interoperability across borders and sectors;
- assessment of ICT implications of proposed or adopted Community legislation as well as planning for the introduction of ICT systems in support of the implementation of such legislation;
- operation and improvement of existing common services as well as the establishment, industrialization, operation, and improvement of new common services;
- improvement of existing reusable generic tools as well as the establishment, provision, and improvement of new reusable generic tools.

The ISA program is implemented by means of actions, i.e. studies and projects as well as accompanying measures supporting the implementation, and is structured in accordance with the activity clusters and accompanying measures defined in the European Interoperability Strategy. The program's actions are as follow:

- trusted information exchange,
- interoperability architecture,
- assessment of the ICT implications of new EU legislation,
- accompanying measures.

The ISA program is implemented by means of actions, i.e. studies and projects as well as accompanying measures supporting the implementation, and is structured in accordance with the activity clusters and accompanying measures defined in the European Interoperability Strategy (EIS). The program's actions are grouped at following clusters:

1. **Trusted information exchange** - the cluster tackles the challenges posed by the different administrative, technical and legal backgrounds of the MSs, which can hinder the smooth and secure transfer of data. The cluster deals with information that is exchanged cross-border, typically taking place in sector specific projects. The cluster addresses topics such as semantics, information availability and usage, trust and privacy, and the catalogue of services. An example of actions at this cluster are: - Improving semantic interoperability in European e-Government systems; - Methodologies for the development of semantic assets; Developing electronic procurement for Europe - PEPPOL sustainability.

2. **Interoperability architecture** - the cluster aims to further align cross-border and cross-sector IT infrastructures that are already available. The cluster addresses a broad range of activities:

- agreeing upon common architecture guidelines,
- creating the architecture itself,
- supporting the maintenance of the architecture,
- identifying and developing common building blocks.

An example of actions at this cluster are: Towards a European Interoperability Architecture; - Elaboration of a common vision for a European Interoperability Architecture (EIA); - Towards the full digitalization of EU document exchange; - Document repository services for EU policy support.

3. **Assessment of the ICT implications of new EU legislation** - nowadays almost all implementation of new EU legislation requires the support of IT systems, e.g. for the exchange of information between authorities across borders or for the delivery of online public services to citizens. Consideration of ICT implications early in the drafting procedure will ensure a timely implementation of legislation and offers the possibility of reusing and adapting existing solutions as much as possible. An example of action at this cluster are: - Contributing to efficient implementation of EU law; - Assessment of ICT implications of EU legislation.

4. **Accompanying measures** - in order to support the success of the other cluster actions, accompanying measures are set up. Typically, these are horizontal measures. Actions in this cluster address the sharing of best practice and supporting communities. This will be done by providing the necessary tools, platforms, campaigns and support to the communities. An example of actions at this cluster are: - Communication for increased program effectiveness; - Communication activities; - Evaluating progress in implementing the ISA Program; - Monitoring and Evaluation.

The e-TEN program

The European Community e-TEN program works by giving financial assistance to consortia consisting of public and private organizations, enabling them to make e-Services available across the European Union. It focuses particularly on the critical validation and launch phases of a service, when assumptions about the operating costs and the potential revenues, savings and public benefits are put to the test. It can provide:

Currently the main focuses of e-TEN are applications and generic services in the areas of e-Government, e-Health, e-Inclusion, e-Learning and Trust and Confidence.

The program made considerable progress in involving stakeholders from New Member States, SMEs and public bodies. Their participation strongly favors the further deployment and uptake of project outputs at a pan-European level and the competitive health of markets for these and related services. Activities in the latter stage of the program promise good impacts through the formation of sector-based value chain communities (especially in the public sector). The emphasis placed in the latter stages of activity on inclusion in projects of the full value chain including ‘sustaining partners’ and ‘sustaining revenue streams’ was fully validated and represents an important lesson for future programs.

The direct effectiveness of the program in achieving deployment was thus rather modest in all but its closing years. However, its indirect effectiveness arising from the exemplary nature both of the program itself and of its project activities was somewhat higher. Due in some measure to the leverage provided by an effective communication strategy, e-TEN made more

impact from 2003 onwards. Another significant component of the substantially improved effectiveness of e-TEN was its increased emphasis on involving the whole 'value chain' in project consortia. This provided significant benefits:

- the inclusion of end-users greatly increased the likelihood of eventual deployment;

- the greater diversity of participation provided links into the portions of the wider innovation deployment.

The ICT PCP program

ICT Policy Support Program (ICT PSP) is a major component of the EU's Competitiveness and Innovation Framework Program (CIP). Its main objective is to develop pan-European, ICT-based solutions and services, most notably in the areas of public interest.

In the past, ICT PSP and IDABC program complemented each other in relation to a number of activities. ICT PSP program launched pilot actions and the IDABC program delivered input in support of the pilot actions. Currently, actions launched under the ISA program are continuously coordinated and aligned with the work ongoing under the ICT PSP and/or with the EC's internal ICT strategy as well as with actions undertaken in the context of the European e-Government Action Plan 2011-2015. The ICT PSP program supports mainly pilot actions to show and validate the importance of ICT solutions in real settings, both pilot actions addressing innovative solutions or replication of best practices and pilot actions building on member states ongoing initiatives. The ICT PSP program does not support the implementation of solutions, which might require an EU layer. This layer can be supported by the ISA program which endeavors to establish common operational and reusable ICT solutions which respond to generic needs expressed by administrative sectors and member states. As a matter of fact, the ISA program aims at supporting the implementation of solutions whereas the ICT PSP program aims at identifying potential solutions.

MODINIS program

MODINIS had the following objectives:

- to monitor performance of and within member states and to compare it with the best in the world by using, where possible, official statistics;

- to support efforts made by member states in the framework of e-Europe at national, regional or local level, by analyzing good practices and establishing a mechanism of exchange of experiences;

- to analyze the economic and societal consequences of the information society with a view to facilitating policy discussions, particularly in terms of industrial competitiveness and cohesion as well as in terms of social inclusion;

- to prepare for the establishment of the future structure at European level for network and information security issues.

Considering the work programs available at

http://ec.europa.eu/information_society/eeurope/i2010/archive/modinis/index_en.htm, it is possible to see that every year it had some activities and actions related to e-Government. In the context of interoperability, the most important is the study provided in.

The project outcomes can be grouped under three main areas:

- exchange of experiences and case studies,
- local and regional interoperability study,

- dissemination and promoting progress and take-up of Interoperability, including workshops.

e-Justice communication via online data exchange (e-CODEX) program

In a Europe without borders, cross-border judicial cooperation is crucial to enable and stimulate the mobility of citizens and businesses. In an increasingly digital society, such judicial cooperation relies on e-Justice to facilitate the interaction between different national and European judicial actors. At a time when the physical barriers between countries in the European Union have been removed, the digital era poses new cross-border challenges. Challenges related to different standards, different protocols, the cross-border recognition of identities, mandates, electronic signatures, and so forth.

The e-Justice Action Plan

A European system of e-Justice should be accessible to citizens, businesses, legal practitioners and the judicial authorities, which will make use of existing modern technologies. In June 2007 the Justice Home Affairs Council of Ministers decided that it was time to develop, at a European level, the use of information and communication technologies in the field of justice. In November 2008 the European e-Justice Action Plan was launched. This plan basically states that the European e-Justice system must be designed while respecting the principle of the independence of the judiciary. From a technical viewpoint, e-Justice must take into account the more general framework of e-Government, especially on issues like secure infrastructure and authentication, e-Signature and e-Identity.
The European e-Justice Action Plan outlines numerous areas of activity for the support of the European judicial area at the service of European citizens. Examples are access to information in this field, dematerialization of proceedings and communication between judicial authorities. The realization of these goals calls for common solutions to potential digital barriers between countries. e-CODEX aims to develop the building blocks that can help realise this.

The goal of the project is to improve the cross-border access of citizens and businesses to legal means in Europe as well as to improve the interoperability between legal authorities within the EU. e-CODEX will develop building blocks that can be used in- or between member states to support cross-border operation of processes in the justice fields. These solutions, which will be developed in different areas from safe transportation to identity and rights management to document standards, should enable a safe environment for users (ranging from citizens and businesses to members of the different legal professions) to access a wide range of legal services across Europe and will contribute to the pan-European interoperability layer for electronic exchanges in Europe in the field of Justice. Therefore, e-CODEX is a functionality which provides an easier (digital) way to exchange legal information between EU-countries. One of the aims of the project is to achieve interoperability between existing national judicial systems.

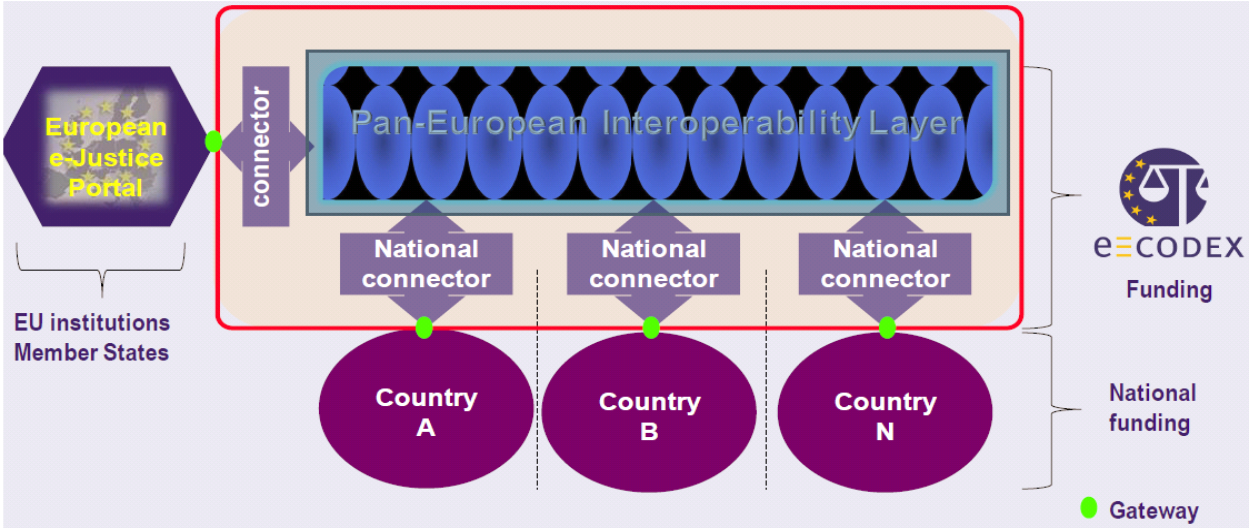


Figure 2-21

In the technical work packages (4, 5 and 6) of the e-CODEX project, the three main building blocks for cross-border e-Justice interoperability will be developed:

- identity; - transport/payment; - documents.

The seventh work package deals with integration of these building blocks. The activities carried out by the seventh work package to set up an architecture governance structure for the e-CODEX project and provides a description of such structure. It also presents a reference of the Standards and Architectural Guidelines to improve interaction, exchange, and cooperation among European public administrations across borders and across sectors for the delivery of e-CODEX services. Furthermore, this delivery sets the general framework for the e-CODEX methodology discussion. The actual methodology, which provides a framework and guidelines describing how to document the architecture and specifications, so that the necessary types and levels of documentation fit together, is provided. Lastly, the delivery presents e-CODEX high level scenario models of use cases, and discusses the e-CODEX security policy, which provides the basic principles for a secure operational environment and the development of a 'circle of trust' among actors, citizens, businesses, legal practitioners and the judicial authorities, specifying the obligations of the parties.

e-CODEX provide ready to use and tested solutions. The products of e-CODEX are available for everyone without any charge. Every country will be able to implement either all or just chosen modules and provide new functionalities for a wide range of use cases and not merely those piloted in the project. The e-CODEX solutions are built on the basis of existing solutions in Member States. E-CODEX will actively consult representatives from the IT industry, standardization bodies but also Member States and stakeholders not participating in the project to incorporate their views on the solutions proposed.

The European patients – smart open services (epSOS) project

epSOS is the European electronic Health ("eHealth") interoperability project cofounded by the European Commission and partners.

It focuses on improving medical treatment of citizens while abroad by providing health professionals with the necessary patient data in a secure electronic format. In particular, epSOS aims to offer seamless healthcare to European citizens by building and evaluating a service infrastructure.

The project aims to design, build, and evaluate a service infrastructure that demonstrates cross-border interoperability between electronic health record systems in Europe. It concentrates on developing a practical eHealth framework and ICT infrastructure that enables secure access to patient health information among different European healthcare systems

From a Legal and Regulatory (L&R) perspective, it is important to note that the epSOS services will be offered on a pilot basis.

As a pilot, the primary objective of the initiative is to gather information and evidence in order to facilitate subsequent full deployment. The mission of the L&R work area is to ensure that L&R challenges, which are critical to the realization of the epSOS pilots in real life situations, are appropriately recognized and addressed.

This work shall support and guide the epSOS Participating Nations in transferring this knowledge to a national level and shall support a close collaboration with the Data Protection Authorities of all Participating Nations.

epSOS Services are subject to extremely strict data security and protection standards. All personal medical data is protected at all times, and most importantly, patient data can only be accessed with the informed, explicit and specific consent of the patient.

The epSOS project is about people's cross-border healthcare and safety as well as all about trust. The project members emphasize this fact by setting up a high level of ethic standards as part of our project culture. These standards are based upon integrity, respect, consent and transparency of information and behavior according to national and European legal regulations. This aims at generating and maintaining confidence among all stakeholders and encouraging project participants to act in a fair and responsible way.

The main outcomes of EpSOS is providing following eHealth services:

- patient summary: access to important medical data for patient treatment;

- cross-border use of electronic prescriptions ("e-Prescription" or "e-Medication" systems);

- integration of the 112 emergency services;

- integration of the European Health Insurance Card (EHIC);

- patient access to their data.

The epSOS Patient Summary is a standardized set of basic medical data that includes the most important clinical facts required to ensure safe and secure healthcare. This summarized version of the patient's medical data gives health professionals the essential information they need to provide care in the case of an unexpected or unscheduled medical situation (e.g. emergency or accident). Though this data is mainly intended to aid health professionals in providing unscheduled care, it can also be used to provide planned medical care (e.g. in the case of citizen movements or cross-organizational care paths).

In general, the electronic Prescription Service (e-Prescription) consists of electronic prescribing and electronic dispensing:

e-Prescribing is defined as the electronic prescribing of medicine with the use of software by a legally authorized health professional and the electronic transmission of said prescription data to a pharmacy where the medicine can then be dispensed.

e-Dispensing is defined as the electronic retrieval of a prescription and the dispensing of the medicine to the patient as indicated in the corresponding e-Prescription. Once the medicine

has been dispensed, the dispenser is to report the dispensation information using the e-Prescription software.

The epSOS e-Prescriptions electronically transmitted to pharmacies in epSOS partner countries contain the currently available e-Prescriptions for the medications, i.e. all prescriptions that could also be dispensed in the patient's home country at that moment. If a prescribed medical product is not available abroad, the attending pharmacist may, depending on the circumstances, dispense a different brand or package size of a comparable product to the patient.

At national level various databases exist, various ways of representations exist, and different data models and coding systems have been used. Member States (MS) use different data models, terminologies, and coding systems to serve different purposes and so they cannot automatically exchange information.

Therefore, before any final recommendations can be made for development, one of the keys tasks to be undertaken is to obtain a comprehensive map of this situation in the MS. For the cross border setting it is clear that we need access to a common European terminology to describe a pharmaceutical product. However, it does not seem realistic to simply impose the use of a new single standard across Europe to describe medicines and/or clinical documents more generally because national interests must be looked at. However, current electronic prescription systems in some MS seem to suffer from poor availability of structured and coded information. In epSOS, it has proven to be difficult for each country to provide structured and coded data for unambiguous processing. Therefore the common European standard should facilitate and support MS and their development and should contribute significantly to interoperability between any European and existing national databases of medicines. Having such a European standard could perhaps also facilitate a pan-European development of Decision Support.

We need to address current issues, identified not just in epSOS but elsewhere including:

- unambiguous definition and description of medicinal and pharmaceutical products,
- including unique identification;
- handling of substitution.

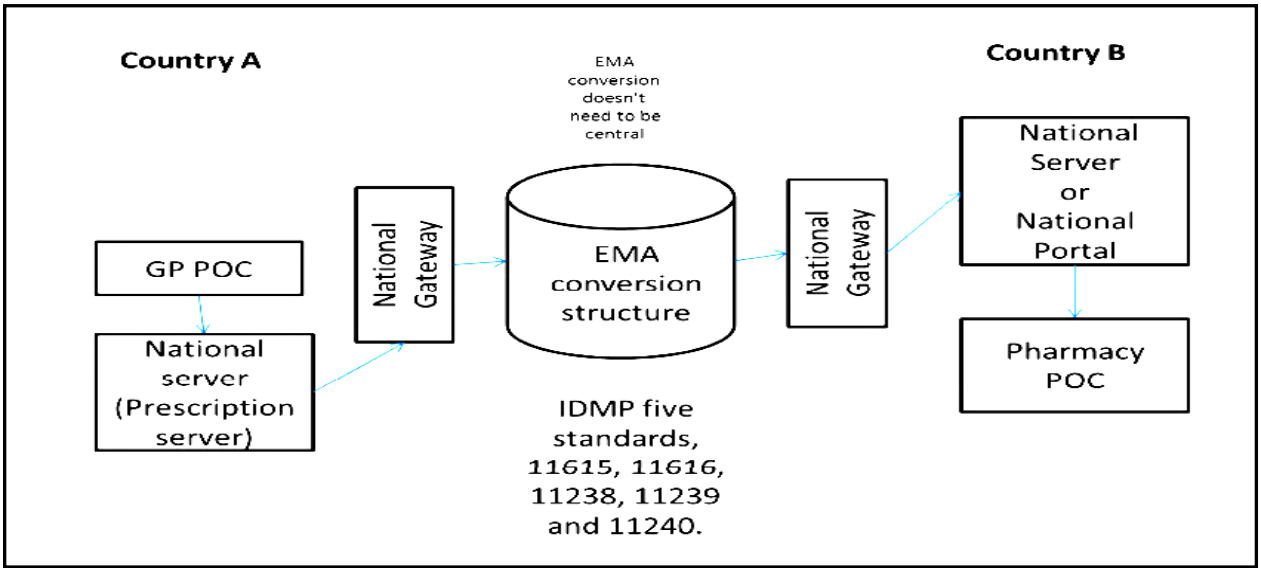


Figure 2-22

In the extended project phase, which started in 2011, the epSOS project team consolidates, scales up and operationalizes the services for ID management, security, semantics and standards. Additionally to the two core epSOS services Patient Summary and e-Prescription services like the patient access to their data, the Medication Related Overview (MRO), the Healthcare Encounter Report (HCER), the integration of the 112 emergency services and the integration of the European Health Insurance Card (EHIC) processes were analyzed and will be tested - if feasible. These services allows to reduce international barriers of healthcare such as different languages, health systems and IT infrastructures.

EpSOS facilitates the secure cross border exchange of patient data. This is done for example by communicating the necessary patient data to the treating doctor or automatic translation of relevant electronic data. Data are processed in a secure way and only with the consent of the patient.

The pan-European public procurement online (PEPPOL) project

The PEPPOL aims at expanding market connectivity and interoperability between e-Procurement communities. Project enables access to its standards-based IT transport infrastructure through access points, and provides services for e-Procurement with standardized electronic document formats (based on UBL and CEN/BII). It addresses electronic public Procurement (thus not any generic public procurement issue falls within its domain) and focuses specifically on interoperability in e-Procurement.

PEPPOL does not attempt to provide an integrated platform. It offers instead a modular set of IT specifications, and associated open source interoperable software solutions that any organization can easily install on its existing ERP systems to interoperate with others, exchanging specific business documents. The objective of the PEPPOL solutions is to facilitate cross-border transactions and to lower barriers for SMEs. The solutions have been designed to operate across European borders, regions, or business sectors.

At the heart of PEPPOL is an electronic transport infrastructure allowing governments and companies to connect their IT systems and reliably exchange data and business documents. A common agreement on cross border procurement processes, implemented through open standards, makes this possible. PEPPOL has developed the BIS and the BusDox (Business Document Exchange) as its principle standards. PEPPOL supports the use of UBL 2.0 documents and CEN/BII profiles. A CEN/BII (Business Interoperability Interfaces Profile) is a specification of how one or more business processes, such as ordering or invoicing, are executed. PEPPOL implements the CEN/BII profiles to define specific business scenarios. A PEPPOL Business Interoperability Specification (BIS) is a CEN BII Profile with additional legal, organizational and technical requirements to support pan-European use. The transport infrastructure of PEPPOL, based on BusDox, allows organizations to securely and reliably exchange electronic documents. BusDox is document agnostic, meaning users can transfer any kind of XML document between any network.

PEPPOL facilitates the pre-award and post-award procurement process with standardized components. In the pre-award phase, PEPPOL supports the public tender process with:

- validation of e-Signatures based on electronic certificates issued by authorities;
- a Virtual Company Dossier to submit standardized company information (evidence, certificates and attestations);
- an e-Catalogue to submit offers about goods and services in a standardized format.
- In the post-award process, PEPPOL covers:

- the e-Catalogue to exchange information about goods and services offered under the contract;
- e-Ordering and e-Invoicing providing the buyer and suppliers with defined procedures to share common business information;
- the Transport Infrastructure - the foundation of all PEPPOL post-award services, based on common, national IT compatible standards and interconnecting e-Procurement communities.

The PEPPOL Enterprise Interoperability Architecture (EIA) is a structured approach to present the PEPPOL artifacts (project documents, specifications, user guides, software tools, etc.) in a repository so that different stakeholders can access information relative to their specific needs, in a consistent and flexible way. The PEPPOL EIA is a 3 dimensional cube (the figure at the next slide). At the top, the cube comprises 4 interoperability communities, reflecting the PEPPOL components:

- e-Signature Validation Infrastructure – validates e-Signature certificates across EU borders;
- transport Infrastructure – enables pan-European e-Delivery of business documents between the e-Procurement communities;

PEPPOL project

Figure 2-23

- post-Award e-Procurement - enables the purchasing process consisting of e-Catalogue, e-Ordering and e-Invoicing and pre-Award e-Procurement – enables the tendering process currently consisting of e-Attestation (VCD) and e-Catalogue.

The above 4 communities are also linked to 6 dimensions: 1. ICT Architecture – providing the ICT scope, solutions and ICT architecture for the interoperability community; 2. Conformance and Test – comprising the requirements, processes and tools of conformance for the different interoperability stakeholders; 3. Life Cycle Management (LCM) – processes for LCM of business and ICT architectures; 4. Governance - comprising the governance structure, legal framework and processes for the business and ICT architectures; 5. Marketing – including processes and material for increasing awareness and recruiting new participants for PEPPOL

pilot projects; 6. Business – being the business scope and business architecture of the interoperability community.

Currently, three of the six dimensions have been put into operation: ICT Architecture, Conformance and Test, and Governance.

Furthermore, each community dimension is divided into 5 abstraction levels: - strategy; - framework; - models (guidelines and specifications of the different services and components); - services and components; - designs; - implementations.

Strategy, Framework, Models, Services and Components are generic artifacts where the Models can be instantiated into specific designs and implementations. The Services and Components can be used in the specific designs and incorporated into the implementations.

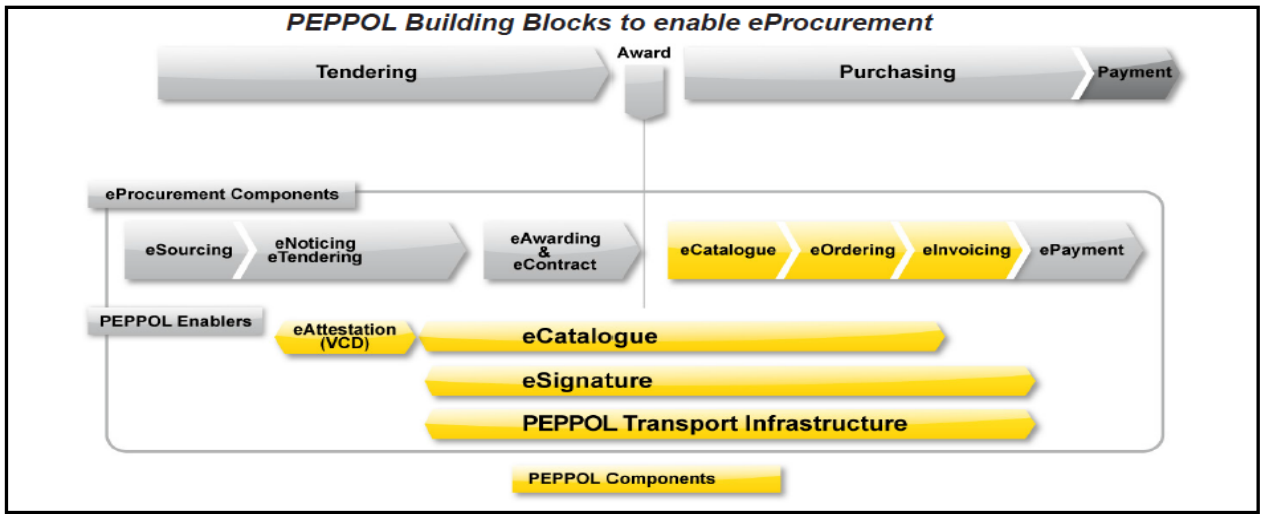


Figure 2-24

During its first year PEPPOL successfully specified and designed the infrastructure to enable cross- border public procurement in Europe. The PEPPOL infrastructure was released for beta test on 1 May 2009. Since then it has been possible to exchange business documents through the PEPPOL infrastructure for testing purposes. For the remaining two and a half years the project aims to construct and pilot the solution which will be operative after the project ends in late 2011. A plan for long-term sustainability is in progress. The pilot project will facilitate the electronic cross-border exchange of orders, invoices, and catalogues. It also includes the re-use of company information required for bidding. The mutual recognition of electronic signatures will also be addressed.

In order to enlarge the geographical coverage of PEPPOL, to strengthen specific focus areas and to ensure long-term sustainability, the project budget has been increased by EUR 11.2 million. It makes a total budget of EUR 30.8 million, half of which comes from the European Commission. Greece, Portugal, Sweden and the United Kingdom entered the project as of 1 November 2009. The PEPPOL consortium consists now of 18 partners from 12 EU countries. The project timeframe has been extended by six months, with completion by 31 October 2011.

Small- and medium-size enterprises will benefit from reduced costs through automated and simplified processes, and could ultimately see an increase in their sales thanks to access to new and larger markets. The higher maturity in eProcurement at both buyer and supplier side, will create new innovative IT projects for the software industry, by expanding optimization of business processes to the whole supply chain. EU governments at federal, regional and local level will see reduced costs through automated and simplified processes and reduced costs through

more competition in bids. Electronic processes ensure transparency and better control of funds, as well as possibility of facilitating green and sustainable procurement. PEPPOL can also contribute to the export of domestic products and support economy modernization.

Simple procedures online for cross-border services (SPOCS) project

The project is closely related to the Service Directive which implementation calls for setting up Points of Single Contact (PSC). The PSCs are acting as intermediaries between service providers and the national public administrations. SPOCS aims to build the next generation of online portals PSC, that every European country now has in place, through the availability of high impact cross- border electronic procedures. Therefore, the SPOCS pilots are using the SPOCS building blocks for Syndication, e-Documents, e-Delivery, e-Safe and e-Services in the national production environment of the Points of Single Contacts in member states.

The aim of SPOCS is to develop an interoperability layer to foster the services economy in Europe by facilitating the Service Providers to apply via the Points of Single Contact for businesses the EU member states have set up. Therefore, the aim of our pilot is to show that the building blocks developed within SPOCS composing this interoperability layer indeed do function in a real life environment.

The process followed within the SPOCS to reach live testing consisted in:

- specifying the SPOCS building blocks (Syndication, e-Documents, e-Delivery, e-Safe and e-Services);

- developing the SPOCS building blocks based on their specifications;

- deploying them in the SPOCS piloting countries;

- assessing the results and iteratively adapting the specifications and modules as needed;

- scaling and sustaining the SPOCS building blocks.

The work packages related to technical activities are the following:

- WP1: Content syndication, multilingual issues and glossary. Its objective is to enable content syndication related to glossaries and the multilingual reality. 27 different member states, 23 different languages, 3 different alphabets – content syndication + multilingual issues must be qualified. Syndication is used to supply SPOCS enabled PSC's the metadata on the available licenses, procedures and other relevant information available from competent authorities;

- WP 2: e-Documents. Its objective is to enable understanding and recognition of e-Documents and their authentication and validation processes. SPOCS will develop interoperability models and common specifications for documents to assist convergence and reduce heterogeneity;

- WP 3: Interoperable delivery, e-Safe, secure and interoperable exchanges and acknowledgement of receipt. The objective is to enable understanding and recognition of e-Delivery systems in different member states. SPOCS will provide solutions such that competent authorities and PSCs of one member state can effectively communicate the outcome of an administrational procedure (usually e-Documents) to a service provider or agency in another member state;

- WP 4: Interoperable e-Service Directories. Its objective is to enable definition and description of services to form a better understanding and recognition of e-Services that are provided in different national service directories. SPOCS will focus on structuring and seamlessly connecting resources and systems (i.e directory services/relational databases) containing information about authorities and services.

Such approach allow to achieve following main result of SPOCS:

- the completion of the open consultation and common specifications;

- providing seamless electronic procedures by building cross- border solutions based on your country's existing systems;

- creating four pilots: Real Estate Agent, Travel Agent, Master Builder and Architect,

The project's enlargement to 9 new countries (Lithuania, Luxembourg, Malta, Norway, Portugal, Romania, Slovenia, Sweden and the United Kingdom) pending final contractual arrangements, its collaboration with similar large scale pilots and further new projects to be launched.

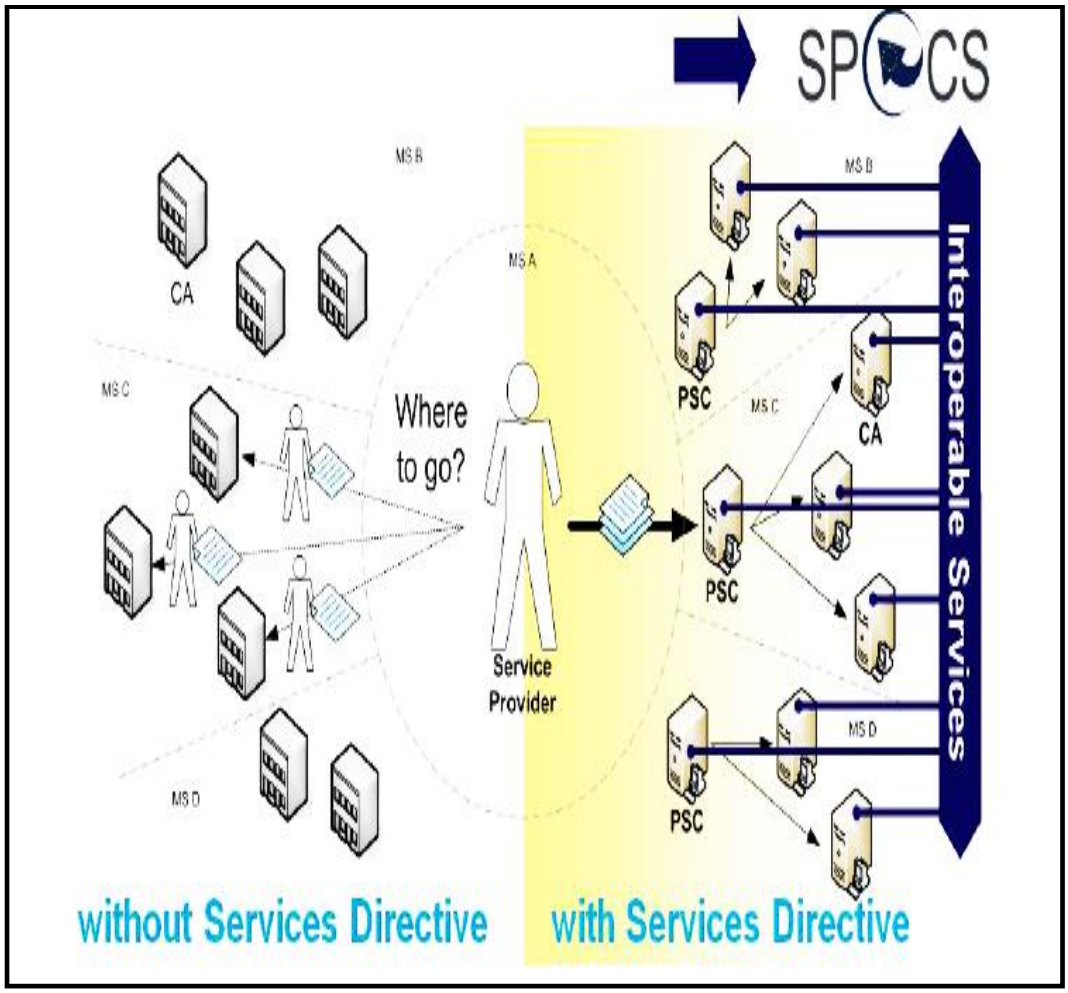


Figure 2-25

Figure 2-26

Secure identity across borders linked (STORK) project

The aim of the STORK project is to establish a European eID Interoperability Platform that will allow citizens to establish new e-relations across borders, just by presenting their national eID. Cross-border user authentication for such e-relations will be applied and tested by the project by means of five pilot projects that will use existing government services in EU member states.

The STORK project will make it easier for citizens and businesses to access online public services across borders by developing and testing common specifications for mutual recognition of national electronic identity (eID) between participating countries.

It will do so by:

- developing common rules and specifications to assist mutual recognition of eIDs across national borders;
- testing, in real life environments, secure and easy-to-use eID solutions for citizens and businesses;
- interacting with other EU initiatives to maximise the usefulness of eID services.

STORK will focus on pragmatic eID interoperability solutions, implementing several pilot cross-border eID services chosen for their high impact on everyday life.

STORK will test cross-border services in areas:

- a demonstrator showing that cross-border electronic services can operate in a number of member states;
- student Mobility, to help people who want to study in different member states;
- electronic Delivery, to develop cross-border mechanisms for secure online delivery of documents;
- change of Address, to assist people moving across EU borders.

The main achievements are as follows:

- establish a European eID Interoperability Platform that allows citizens to establish new e-relations across borders, just by presenting their national eID (created a set of common specification, a set of quality assurance level, a common code, six pilots in production);

- STORK sustainability action, which will address various legal and organizational barriers to widespread implementation of STORK supported by analysis of significant business cases and applications;

- minimization of time & cost & energy savings;

- functionality & openness of authentication components;

- reinforcement of European mobility in the Digital Single Market;

- proven variety of secure authentication dimensions to foreign e-Services;

- scalability overtime;

- easy and effective application of existing processes in cross-border context;

- trust and wide acceptance by various stakeholders.

National online services today with eID

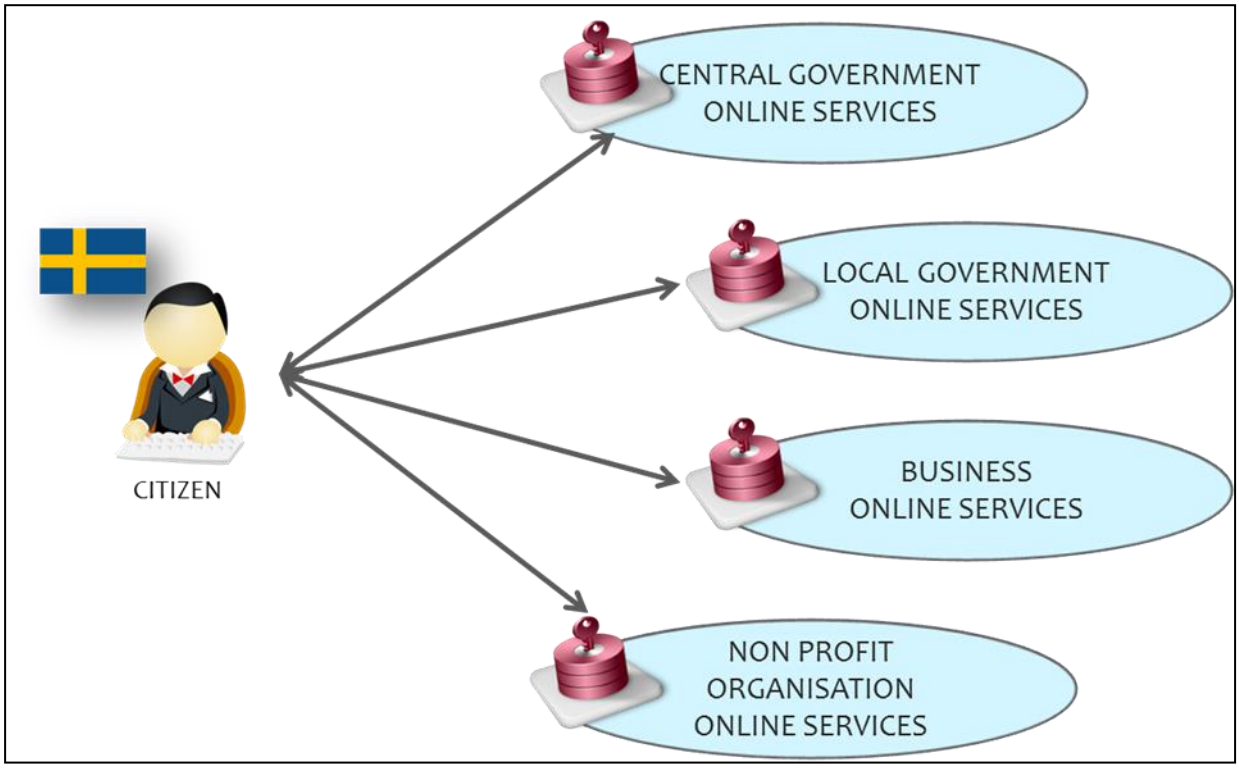


Figure 2-27

All MS have their own eID infrastructure

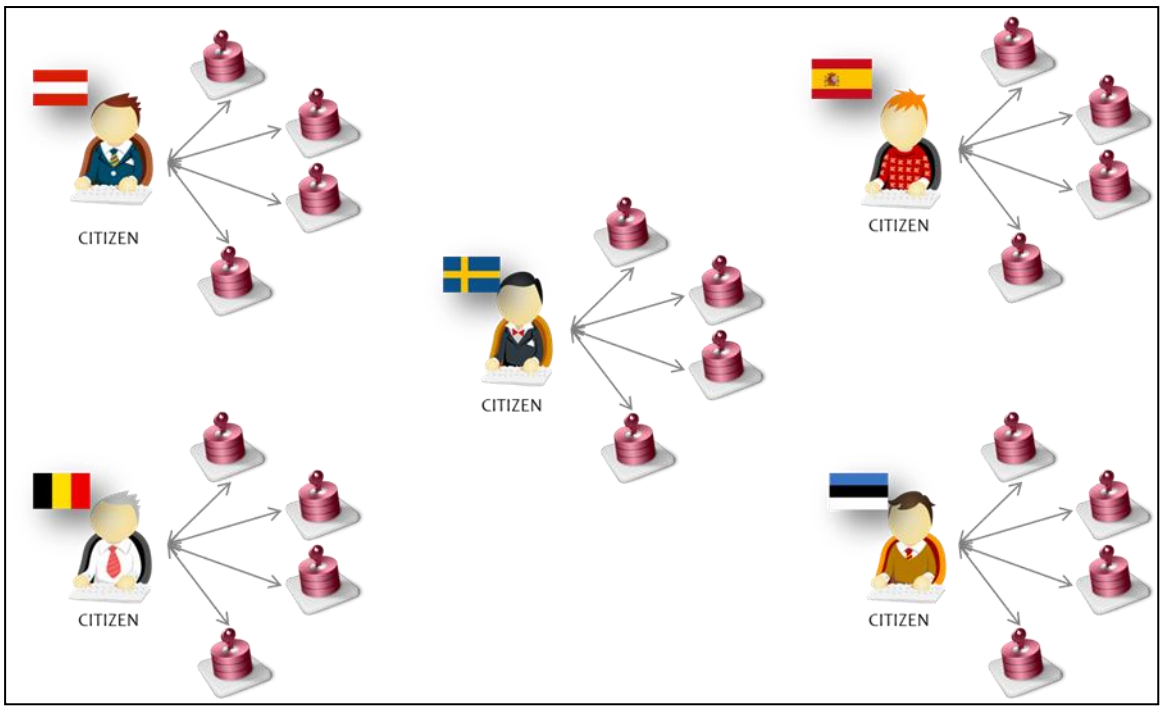


Figure 2-28

Borders will open & National online services will improve

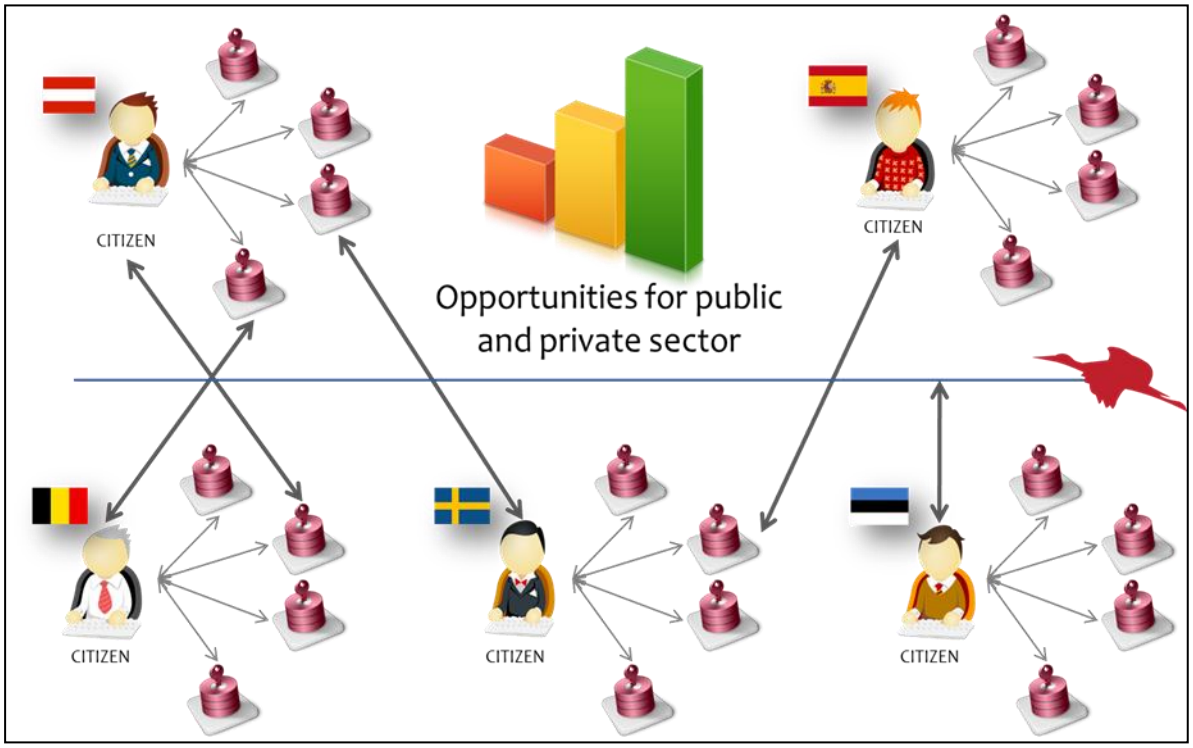


Figure 2-29

STORK: Communication structure

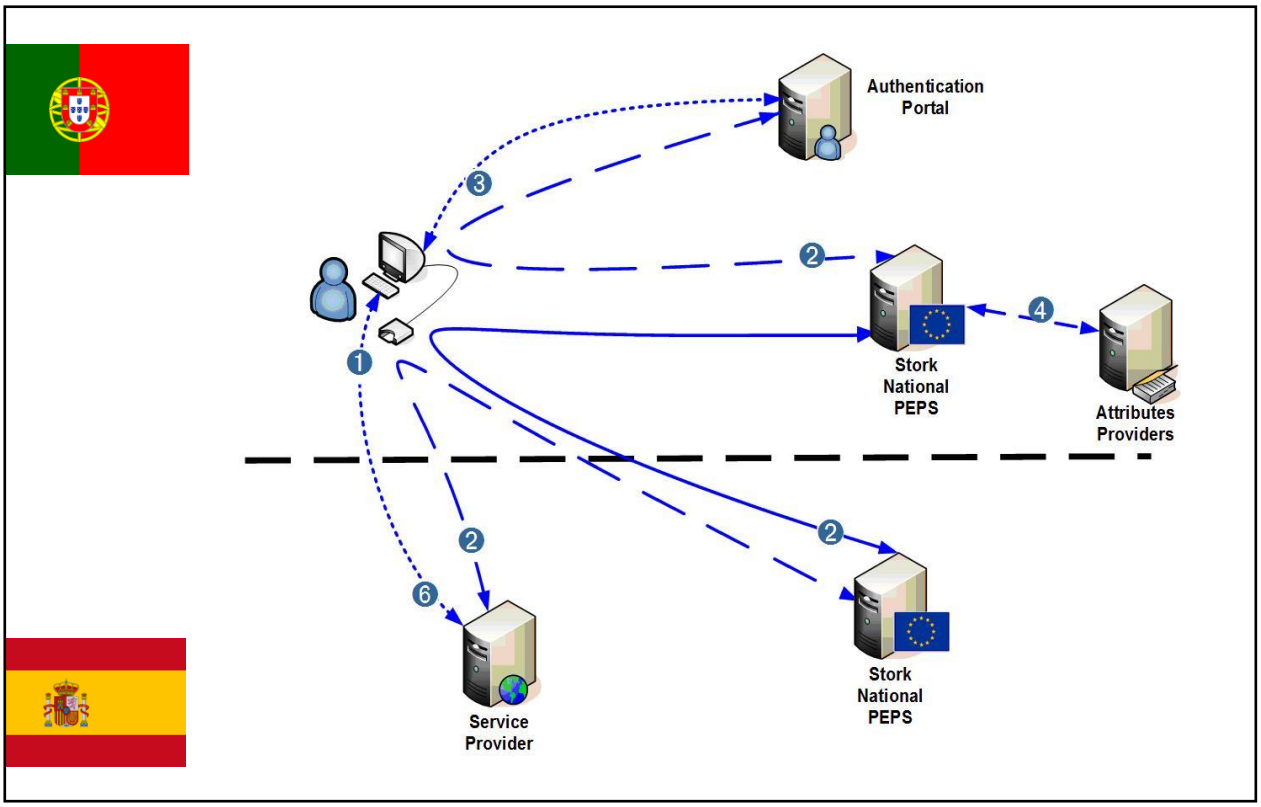


Figure 2-30

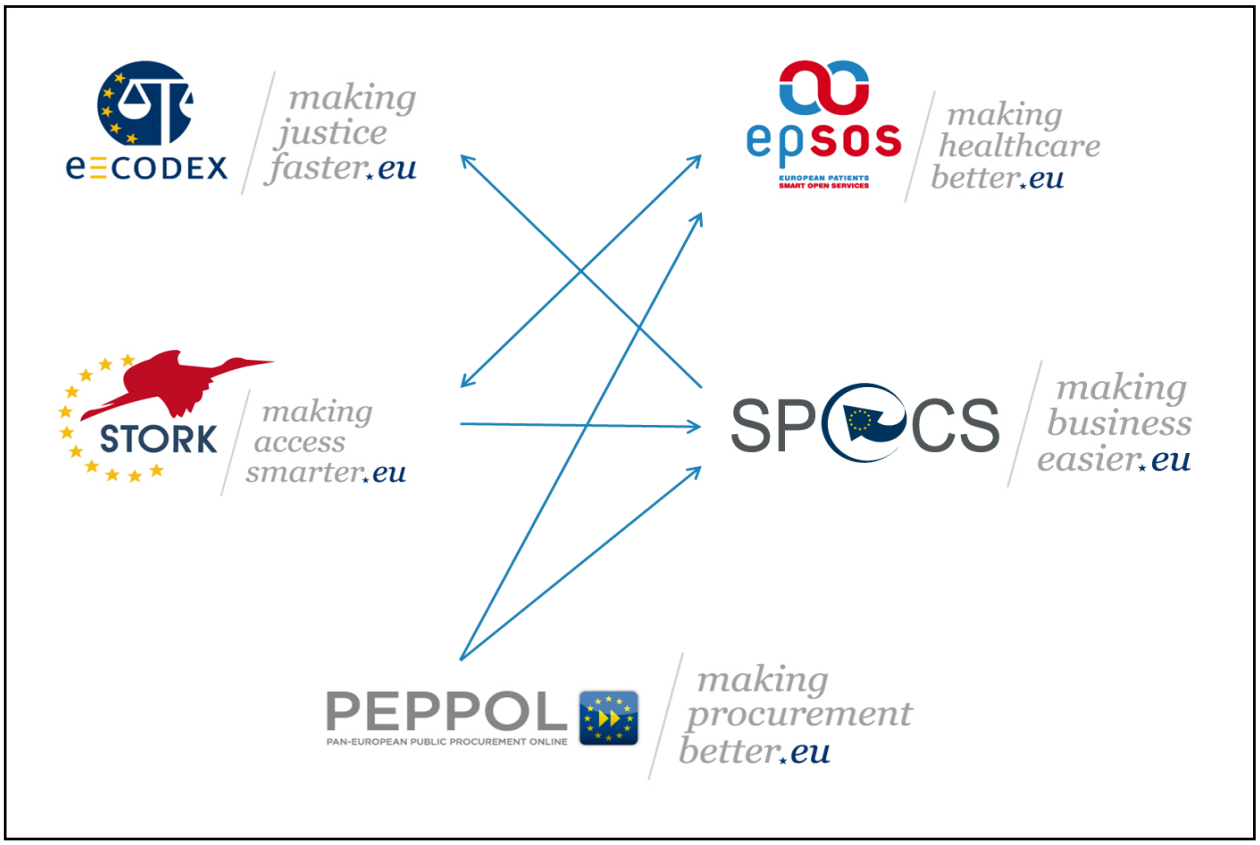


Figure 2-31

PART 3

NATIONAL ASPECTS

CHAPTER 3.1

NATIONAL INTEROPERABILITY FRAMEWORK

Introduction

The Bulgarian national interoperability Framework for Governmental information systems is adopted by the Council of Ministers with Decision Nr. 482 of 28 June 2006. This document is developed in compliance with the "European Interoperability Framework for pan-European e-Government Services" version 1.0 published in November 2004. The European framework has been created in pursuance of the initiative "e-Europe 2005", adopted at the Seville summit (June 2002). In accordance with its Recommendation Nr. 1: "Member State administrations should use the guidance provided by this European Framework to introduce a pan-European dimension into their own interoperability frameworks and administrative infrastructures".

The high priority of the interoperability problem has been underlined in the Communication of the European Commission COM (2006) 45 dated 13 February 2006, entitled "Interoperability for pan-European e-Government services". According to it, the interoperability is one of the four major challenges for the establishment of a Common European information space, as it is formulated in the Strategic initiative "i2010".

The IDABC Program (Interoperable Delivery of European e-Government Services to public Administrations, Businesses and Citizens) of the European Commission has proposed the following "road map" for the creation of a pan-European environment, ensuring system integration and interoperability of the information systems, passing through the following basic phases:

- development of an "Interoperability Framework for Information Systems";
- development of Guidelines and specific rules for System Integration and Interoperability of applications related to the e-Government;
- development of "Architecture Guidelines and Reference Models";
- setup of XML Clearinghouses - centralized storages of information resources, required for achieving Interoperability;
- development of a "pan-European Administration Orientation Map".

The interoperability framework cannot be a static document – it requires being permanently adapted to the changes in the technologies, the standards and the administrative infrastructures.

One of the most essential problems of the development of administrative information systems is the achievement of system integration and interoperability – both in the context of the information exchange between the systems of administrative bodies, and in the realization of e-Services for citizens and organizations.

The integration of the information systems (the so called "System-to-System Integration - S2Si") is facing a number of challenges:

- heterogeneity of the processes;
- heterogeneity of the system realizations;
- heterogeneity of the data structuring and presentation;
- requirements for security and reliability of the exchange.

Beside the discrepancies in software and technological aspect, the unregulated exchange between the partners also represents a problem.

While the heterogeneity is not having so serious consequences in the realization of e-services for natural persons, for the business information services where the problems of the different providers of e-services are transferred into the corporate systems of the companies-users, the situation is extremely serious. The problems become deeper also because of the requirements for integration of the national systems of the EU member states with the aim to organize cross-border e-services.

All this imposes the necessity for the development of the National Interoperability Framework in conformity with the internationally adopted standards and the practices in the EU member states.

Guiding principles

In accordance with Recommendation Nr. 2 of the European Framework, in order to reach a pan-European level of the services of the authorities the following main principles have to be adopted: - accessibility; - multi-linguistic character; - security;

- personal data protection; priority to the decentralized responsibility;

- use of open standards; - benefiting from the advantages of the open code;

- multilateral relations.

In accordance with Recommendation Nr. 3 of the European Framework, the interoperability contains three aspects:

- technical - enabling exchange between the applied systems in various computers;

- semantic - providing one and the same meaningful content of the exchanged data;

- organizational - creating organization for the management of the processes for data exchange and processing between different organizational structures.

Besides that, the technical interoperability is distributed on:

- the methods for data presentation;

- the methods of access;

- the methods for data integration;

- the architectures for distributed applications;

- the protocols for exchange of messages and files;

- the network services;

- the services for the security of the exchange and the storage of the messages.

The semantic interoperability is based on specific information resources of two types:

- resources providing for morphological compatibility (nomenclatures, thesauruses, ontologies, etc.).

- resources providing for syntactical compatibility (XML-schemes, models and schemes of metadata, etc.).

The maintenance of the Interoperability Framework is a permanent task requiring institutional structure and well-defined rules.

In accordance with the "Strategy of IDABC for interoperability of the content" the following conditions have to be observed for the successful application of the Interoperability Framework":

- continuous stability of the basic parameters of the Framework;

- feedback from the users;

- open and transparent process of changes of the basic documents;

- policy and mechanisms for quality management;

- adaptation to the expected new applications;

- focus of the changes on the processes and not on the standards;

- publication and allocation of the resources, oriented to the provision of the interoperability (definitions, terminologies, vocabularies, rules, etc.) in suitable formats;

- identification, enlargement and multiple use of the existing resources, oriented to the provision of the interoperability;

- key role of the registers with meta data.

Objectives of the National Interoperability Framework

The general objectives of the unification and rationalization of the Information infrastructure of the governmental information systems can be formulated as follows:

- social efficiency, minimization of the capital investments and the exploitations costs;

- equal treatment of the participants in the exchange;

- security, confidential exchange, personal data protection, intellectual property protection;

- homogeneity and interoperability of the information structures – basis for macro-management of the cybernetic principles;

- integration in the global and regional information structures.

From practical point of view the pointed out overall objectives can be achieved through:

- invariance of the access to the systems and their exchange with the environment;

- compatibility of the processes and the data flows;

- integration of the applications;

- automation of the processes of information exchange;

- multiple use of single input of data (data blocks);

- multiple use of already developed or bought software components and products;

- use of already built information systems;

- scaling of the decisions;

- transferability and independence from the platforms;

- possibility for flexible readjustment of the procedures after changes in the environment and the requirements.

Subject area

The interaction of the information systems in the governmental information systems in the Republic of Bulgaria is defined in the following documents:

- Strategy for the modernization of the State Administration – from accession to negotiation, adopted with a Decision of the Council of Ministers Nr. 465 dated 2003;

- e-Government Strategy of the Republic of Bulgaria, adopted with a Decision of the Council of Ministers Nr. 866 dated 28 December 2002;

- Plan for the implementation of the e-Government Strategy of the Republic of Bulgaria for the period 2003 - 2005, adopted with a Protocol Decision of the Council of Ministers dated 11 March 2004.

In essence these information systems (not depending on the common technical and telecommunication environment) perform comparatively autonomous functions – three basic and one auxiliary:

A. Function "Macro-management of the country" where analytic-synthetic procedures are predominating, related to the processing of unstructured information, with non-formalized preliminary exits and continuous time periods for generation of the decisions.

B. Function "Electronic services for the citizens and the business" where predominating are the formalized procedures for processing of structured information in a regime close to the real time.

C. Function "Exchange of information between the units of the administration" – data exchange predominantly connected to the technological processes in the administration itself. This covers: - exchange of structured data; - • exchange of unstructured data (including graphically organized data and multimedia); - exchange of meta-data.

D. Auxiliary function "Adaptation and upgrading" which on the basis of the information from the functioning of the three basic systems enables that analysis will be prepared for the effectiveness of the actions of the units of the administration branch and recommendations for their improvement.

The applications related to the e-Services are first and foremost critical for the integration between the information systems. This is stemming from the circumstance that the latter are most dynamic, they act in the most heterogeneous environment and include in themselves procedures with different degree of automation.

The functions of the information systems in the governmental information systems develop in the hierarchical environment of the public and the local administration, which from a system point of view represents a non-canonic hierarchy (because of some autonomy of some of the levels and the functional relations, leaping across several levels). Irrespective of this, the principles for obtaining integration and interoperability are invariant in respect to the levels of functioning of the information systems.

The modern infrastructure for complex e-Services supposes:

- realization of the services as a complex value added chains;

- centralized management of the process of provision of services in its whole "life cycle";

- requesting and receiving the services from "one-stop shop" (including territorially distributed ones).

However the exchange of data between the information systems (the applications respectively) is realized at four levels:

• transport (between the systems);

• transactional;

• syntactic (between the applications);

• semantic

The choice of fundamental standardization platform is of crucial importance, because of the exceptional diversity of the standards and the specifications related to the system integration and the interoperability. The evolution of the standardization process in respect to the system integration and the interoperability directs this choice towards the integration oriented to services. The latter allows not only for transfer of information from one application to another application in different information systems, but also the creation of complex application through services, maintained in remote systems through the distribution of common business logics between the applications.

The basic approach to the creation of the National Framework is a combination of:

- the classical Reference model for open distributed processing (international standard ISO/IEC 1076 : 1998), which defines the infrastructure for distributed processing of information between heterogeneous technological resources and multiple organizational domains;

- the last level in the evolution of the standards for system integration – the so-called "Service oriented architecture (SOA)" where "loose coupled" modules of applications are distributed, combined and used for the creation of new applications in the network.

The standardization of the information systems in the governmental information systems in the field of the system integration and the interoperability covers wider area than that of the so-called "formal harmonized standards" approved by official intergovernmental standardization bodies (such as ISO, ITU at a global level or CEN, CENELEC, ETSI – at European level). It covers informal and hybrid standardization processes – the production of sectorial consortia, such as: OASIS, IETF, W3Consortium, UN/CEFACT, OMG, etc.

The above mentioned standards can be divided into two main groups related to the fields of application,:

• horizontal standards – with general application (in all areas);

• vertical standards – with application in the specific area (branch, etc.). As an example for the objectives of the governmental information systems these can be: medical information, banking, geographic information systems, industrial product systems, etc.

The Bulgarian National Framework is treating thoroughly only the horizontal standards, ensuring system integration and interoperability in the information systems within the administration. The vertical standards from areas concerned with these systems will be maintained by branch groups and an information relation with the Register of the standards, object of the present document, will be realized.

Relying on the definition perceived in the European Union, the National Interoperability Framework is built on the hierarchical principle:

• the main directions are formulated from several basic principles;

• the principles are realized by procedures, formulated in the respective methodologies and instructions;

• the technical aspect of the interoperability is guaranteed by a dynamic series of standards;

• the whole application of the National Framework is ensured with respective organizational and technological events.

Basic principles

The document specifies the scenarios and the technologies for obtaining system integration and interoperability. Here, the principles, the observation of which ensures them, are supplemented by rules, definitions and recommendations which make them more detailed.

Principle Nr.1: **In accordance with Recommendation Nr. 14 of the European Interoperability Framework, the main factor ensuring system integration and interoperability is the application of open internationally adopted standards. This is guaranteed through the support of a Register of the standards with "on-line" access, containing standards of different degree of compulsory character.**

The basic criteria for choice of the standards are as follows: - openness; - level of accessibility and maintenance; - maturity; - potential; - applicability to the national conditions.

The term "Maturity of the standards" has been introduced in compliance with the so-called "Model of maturity of the standards" considering five levels of effectiveness and applicability of the respective standard.

The Registers treated in the present National Framework (Register of the standards, Register of the information objects, Register of the electronic services) are specific information resources, intended for the developers of information systems and providers of software products for the e-Government. This predetermines the technology and the instruments for their support.

The name "Register" in the present National Framework means both an information resource and the Registration body in the sense of BDS ISO/IEC 6523-2:2000.

The Register of the standards is a dynamic structure, reflecting the current situation of the standardization processes and the possibilities for their application in the current moment. The register is supported and updated by a double-unit structure containing expert and executive part through procedures regulated in the respective Instruction Manuals.

Principle Nr. 2: **The "Service oriented Architecture (SOA) is accepted as the basis for building of the information systems within the governmental information systems. In accordance with SOA all procedures related to exchange of information in the infrastructure of the governmental information systems (including: the information exchange between the systems of the different administration units; the information exchange between the administration and the citizens and the citizens and the companies when delivering e-services) can be represented, defined and parameterized as "services".**

On its part, every so presented "service" forms the following hierarchical structure: - complex (composite) service; - primary (elementary) services; - documents (information, official); elements of data (segments, composite elements, simple elements).

In the document the term "Electronic Service (e-Service)" is defined in accordance with the Directive of the European Parliament and the European Council Nr. 98/48/EC dated

20.07.1998 as “a public service, provided by the administration at a distance, in electronic way, called (activated), related to exactly defined transactions”.

The primary services provided by different units of the governmental information systems, can be of different degree of automation (they also can contain manual operations) but for the customer they represent an unified process with one entry and exit and with a possibility for “on-line” tracing of the phase of execution.

In order to realizing complex services with a single interface, integrating primary services provided by different units of the governmental information systems, all services (primary and complex) have to be mandatory registered in the Register of the e-Services.

The Register of the e-Services organizes an environment of complex e-Services including: standardized nomenclature and classification of the primary and the complex services, rules for joining the services in Value Added Chains and their provision to the customers.

The entry into the Register of e-Services can be done with examination of the conformity with the mandatory and recommended standards registered in the Register of the standards. The Register will be supported and updated by a double-unit structure analogous to that for the Register of the standards.

Principle Nr. 3: **All services are realized as transactions of formalized information objects – electronic documents**.

“Electronic document” in the context of the “interoperability” is: ”logically completed self-describing information structure, which can be visualized and at the same time processed by the information systems of the governmental information systems even without direct human intervention. Here, the electronic document contains mechanisms for undisputed authentication and protection against illegal access”.

In order to ensure traceability of the transaction process and demonstrability of the participants in its individual steps, the storage of copies has to be provided both of the electronic document filed by the consumer of the e-service to the provider of the service, and of the documentary confirmation for its receipt on the part of the provider.

Definition – The transaction realizes exchange of messages between two interacting processes, in such a way that they coordinate the performance of their functions. The transaction protocol guarantees either the complete performance of the functions or the recovery of the environment in the status in which it has been before the transaction in case of interruption or fatal error.

In accordance with the general recommendations of the European Interoperability Framework to the national frameworks of the member states, the e-Services have to be consumer oriented: thoroughly described, correct, understandable, clearly differentiated into anonymous, requiring identification, etc.

In order to ensure electronic documents exchange management in the governmental information systems, every administrative unit has to maintain a system for effective management of electronic content, consistent with: - the MoReg specification for management of electronic recordings, based on the European Regulation 94/C 235/03; - the IDABC Strategy for interoperability of the electronic content (document ENTR/02/21-MIDDLEWARE-XML).

Principle Nr. 4: **All data of the companies and the citizens, interacting with the governmental information systems, can be entered only once. The administration units are obliged to use the data already gathered on a multiple basis. The holders of the information resources are obliged to provide access thereto of all providers of e-Services using the respective information resource on the basis of regulated rights to access.**

The single entry of the data and their multiple uses as well as the semantic interoperability between the various applied systems of the e-Government is realized through the Register of the information objects.

It is obligatory to enter in the Register of the information objects every electronic document foreseen to be used in newly developed information systems as well as the segments composing it, composite and simple elements of data. In case of presence of already registered elements and segments from the composition of the newly proposed document, they are used in it synonymously without repeated registration.

Every information resource, referred to the e-Government, has to have an exactly specified owner (holder). The latter is obliged to coordinate with the Register of the information objects every change in the structure of the information resource.

The entry of the information objects in the Register is realized with examination of the conformity with the standards adopted to be mandatory and recommended, registered in the Register of the standards. The Register will be supported and updated by a double-unit structure, analogous to the Register of the standards.

The Register of the information objects has to contain a comprehensive specification of the organizations having different rights of access to the information resources (including entry, reading, corrections, etc.).

The management of the life cycle of the information in the e-Government systems has to be consistent with the Recommendations of the so called "Data Management Forum (DMF)".

"Management of the life cycle of the information" means the complex approach for management of the data flows and the metadata associated with them in the information systems from the formation and the initial storage to the moment of their falling into disuse.

Principle Nr. 5**: In order to ensure a common interface in the information exchange between:**

a) the units of the governmental information systems;

b) governmental information systems and consumers of complex e-services (physical persons and legal entities).

every exchange between the providers of information (units of the governmental information systems) and the consumers of information (units of the administration, citizens, companies) must be realized through "integration (intermediary) environment".

Definition – according to the "IDABC architectural principles": the intermediary environment organizes the communications between the applications and the objects (local and remote) by connecting different parts of the allocated IT-architecture and maintains the exchange between remote applications.

The intermediary environment is built-up of "Basic components" performing specific functions. The basic components are "complex autonomous, self-controlled modules of applications having clearly defined interfaces and functions in the context of the general architecture of the information systems within the administration".

In accordance with recommendation Nr. 5 of the European Interoperability Framework the transactions between the "integration environment" and the consumers should be based on conventions for exchange, forming so called "interfaces for business interoperability".

Principle Nr. 6: **In accordance with Recommendation Nr. 12 of the European Interoperability Framework the security aspects of the intersystem exchange cover the following levels:**

- analysis of the global and local environment; - analysis of the type of information during the design or enlargement of the functional capabilities of the network; - building of the public key infrastructure (PKI); - monitoring, diagnosis and measures for protection in a situation of threat for the information security; - controlled access to information; - ensuring of authenticity and completeness of the information; - measures for protection at the level of working stations, including at client's level (including "firewalls", antivirus protection; Trojan horses and other programs bringing the computer systems into undesirable status or results).

The permanent analysis of the type of information has to be performed in accordance with the classification levels for information security, defined in the European Security Regulation, adopted with a Decision of the European council 2001/264/EC.

The aspects pointed out cover the following areas of the definitions in the "Ordinance for the mandatory general conditions for security of the automated information systems or networks wherein classified information is generated, processed, stored and transferred": - documentary security;

- communication security; - cryptographic security; - computer security.

The exchange of electronic documents between the units of the administration should follow the policies of the European Union for authentication and authorization of the participants in the exchange of electronic documents and data, presented in the document "ENTR/01/67-CONSEC SA6/IDA_Auth_Pol". This includes: - coordinated authentication of the users; - single public key infrastructure (PKI); - unified services for the integration of the directories; - unified services for secure exchange with external systems.

The provision of conditions for trust services is an essential element from the "Integration environment". Here one has to follow the "European Trust Recommendations".

Principle Nr. 7: **The adequate application of the standards for interoperability (fixed in the dynamically supported register of the standards) in the information systems within the administration must be realized through conformity assessment procedures.**

Every software product or information system being developed or bought with the aim to be applied in the administration has to be certified for conformity in accordance with a special Instructions Manual.

The certification for conformity is based on conformity tests, carried out by organizations authorized for this. The test methodic is based on the ETSI (European Telecommunication Standardization Institute) Recommendations and are adopted by the Authority, empowered to support the Register of the standards.

Besides the conformity with the entries in the three registers mentioned, the certification procedure should include a testing for the minimum requirements for security, corresponding to the European recommendations mentioned above.

Measures for practical application

The practical application of the National Interoperability Framework requires the resolution of the following immediate tasks:

The document has to be an integral part of the e-Government strategy of Republic of Bulgaria adopted by Decision Nr. 866 of the Council of Ministers dated 28 December 2002 The

National Framework has to be obligatory for all newly introduced information systems in the units of the administration.

The documentation for participation and the technical specifications for all procedures for design, development or supply of departmental information systems in accordance with the Public Procurement Law should be consistent with the National framework.

"A Program for bringing the existing information systems in conformity with the National Interoperability Framework" to be developed in coordination with the ministries.

It is necessary to establish and ensure the maintenance of the centralized registers.

The registers, defined in the National Framework (Register of the standards, Register of the information objects, Register of the e-services) give practical guidance of the contracting authorities, the developers and the providers of information systems and software products for the administration, as follows:

a) minimum amount of requirements, which the contracting authority has to set in his specification;

b) minimum amount of requirements, which the contacting authority should set for the technology of the exploitation and organization of the realization of the services provided by him;

c) direction for the Contractor what kind of means to select for development. A barrier is posed to the requirements which in essence draw the developments back in technological aspect.

The creation and the functioning of the registers will be provided through the adoption of regulating instructions on the basis of the following documents developed as annexes to the National Framework: - "Methodology for maintenance and management of the working processes for identification, adoption, application and development of the standards, providing system integration and interoperability of the information systems within the administration of the Republic of Bulgaria".

- "Methodology for the building and support of a Register of the information objects, ensuring system integration and interoperability of the information systems within the administration of the Republic of Bulgaria"; - "Methodology for the building and support of a Register of the e-services provided by the administration of the Republic of Bulgaria".

It is necessary to adopt Instructions Manual for the order and the conditions for Certification of the departmental information systems in respect of their conformity with the present National Framework. In compliance with the European practice the so called "voluntary certification" realized by bodies of professional associations has to be introduced.

It is necessary to define and ensure the creation and the exploitation of basic components performing specific functions in the environment of the information systems within the administration. In compliance with the basic formulations in the "e-Government Strategy of the Republic of Bulgaria" and the analysis of the best practices in the EU member states the following "basic components" can be pointed out as part of the "the integration environment" of the information systems within the administration: - information intermediaries (messaging brokers); - authorization and validation module; - module for electronic payments to the administration; - virtual post office; - central portal;

- interfaces and adaptors to existing data basis; - server of application forms; - module for content management; - module of a public desk for e-services.

In this way the content of the Bulgarian National Interoperability Framework completely covers the definition adopted by the European Union: - the rules are defined in the basic document: - the required series of standards will be maintained dynamically in the current type in the respective register; - the instructions for building and support of the three registers as well as the Instructions Manual for certification of the information systems and products represent specific guidelines for action.

The main levels of the National e-Government Technological Infrastructure

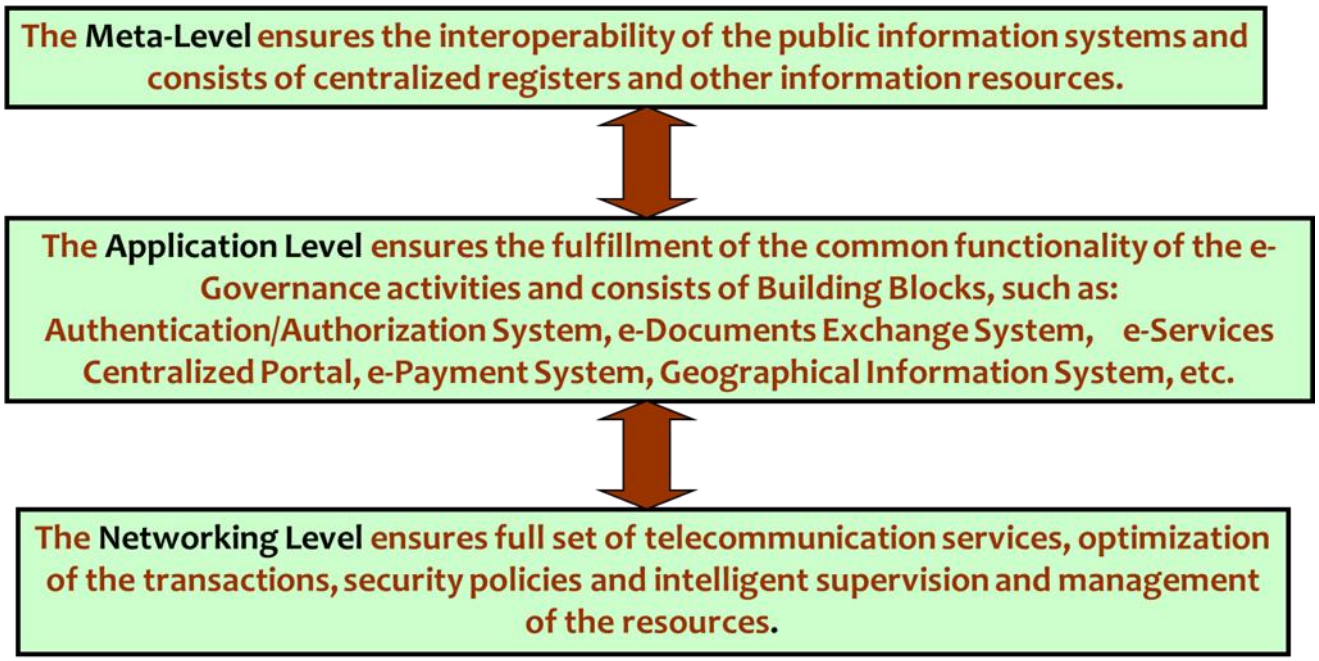


Figure 3-1

The National Document

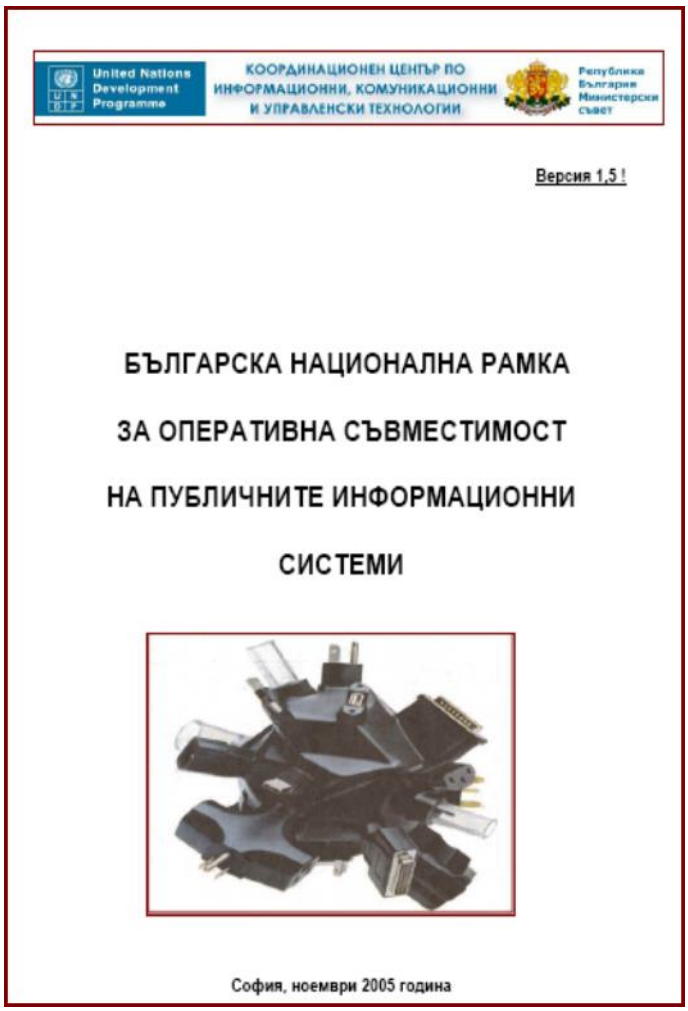


Figure 3-2

The Bulgarian e-Government Interoperability Framework (adopted by the Council of Ministers on the 26th of June 2006) is based on the European Interoperability Framework and the UN/CEFACT Recommendation No 33 named “Establishing a Single Window”.

Figure 3-3

The Interoperability Framework Environment

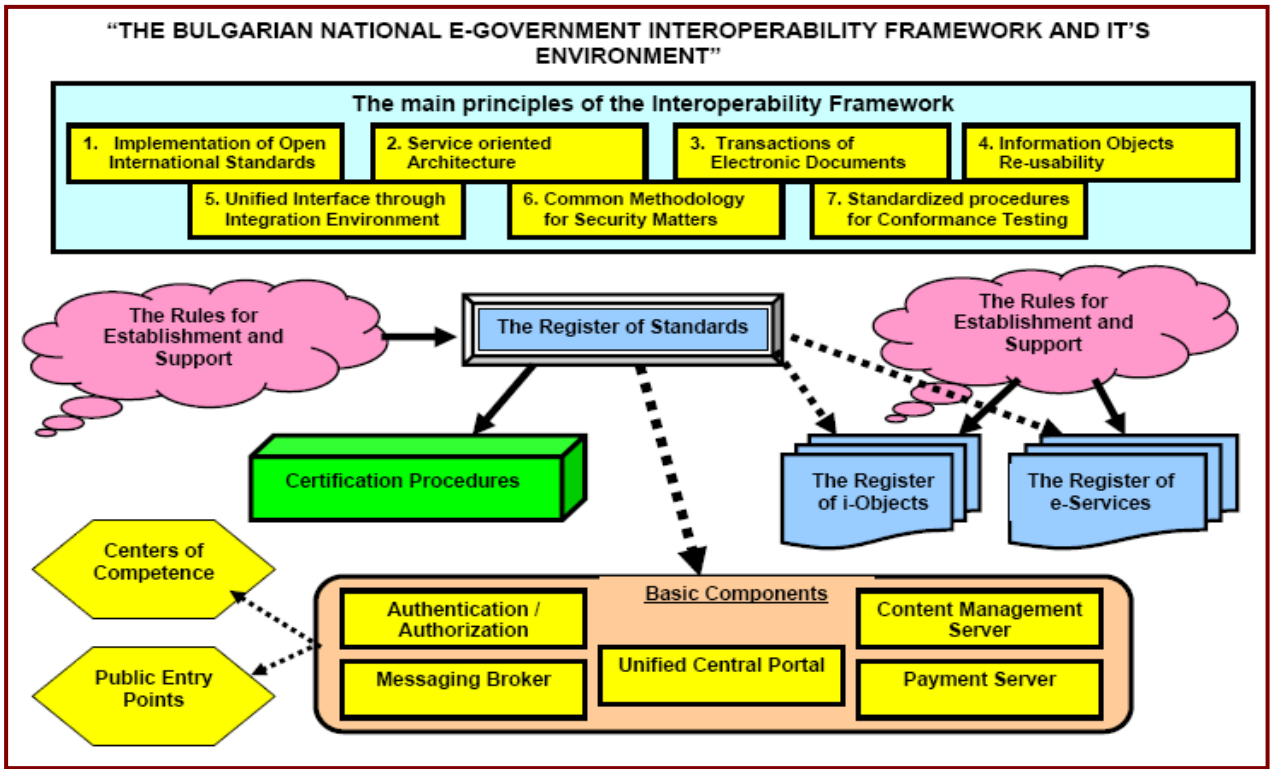


Figure 3-4

The general approach of Bulgarian e-GIF

1. Basis on Service-oriented Architecture (SOA).

2. Establishment of Registry-based environment of meta-data.

3. Realization of "active interoperability" through homogeneous exchange system between loose coupled heterogeneous systems.

4. Obligation for certification by accredited bodies.

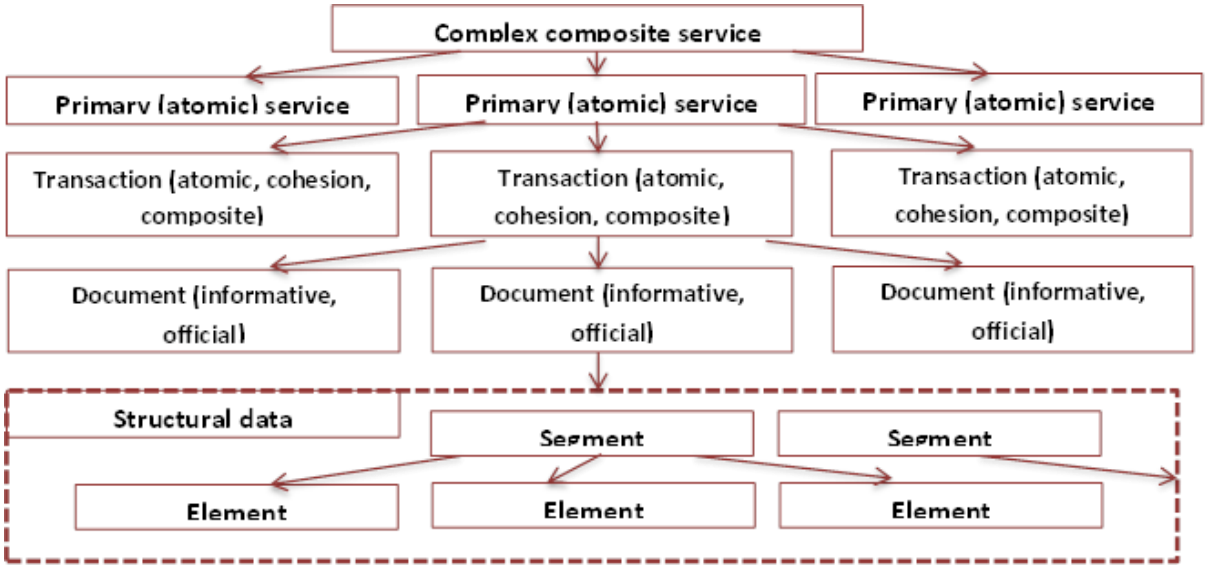


Figure 3-5

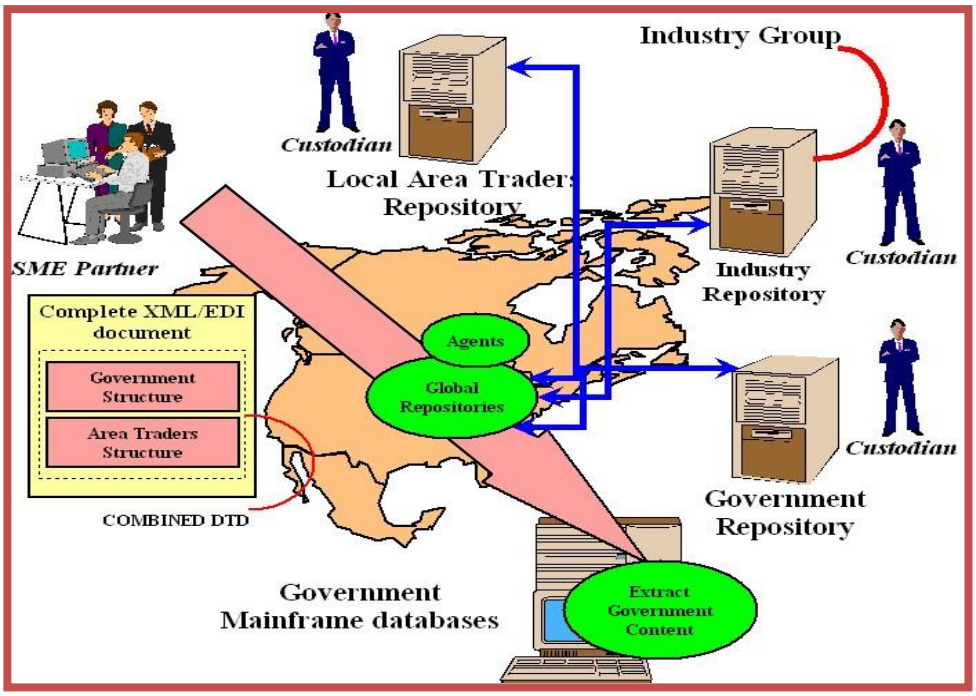


Figure 3-6

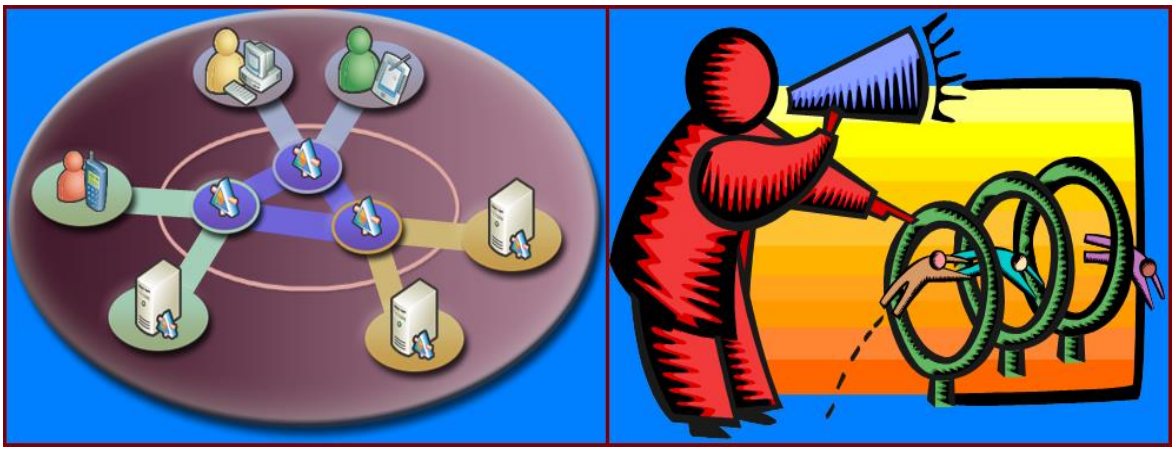


Figure 3-7

Basic consideration about three levels of the Interoperability:

Passive Interoperability - proceeding from the assumption that agents from different heterogeneous environments can reach Interoperability by exchange of standardized messages. However, this is not enough for meeting the requirements of the semantic and organizational Interoperability components.

2. Semi-active Interoperability - a “registry-oriented” form of the Interoperability.

3. Active Interoperability - proceeding from the assumption that agents from different heterogeneous environment can reach Interoperability only through the intermediation of homogenous environment with internal standardized exchange.

The Bulgarian e-GIF is based mainly on the second and the third levels:

A. Specifying three specialized registers:

the Register of Standards;

the Register of Information Objects;

the Register of Electronic Services.

B. Realizing common centralized solutions called “e-Documents Exchange System”.

The Register of the Standards

Now the “on-line” Register contains 108 internationally adopted standards and specifications.

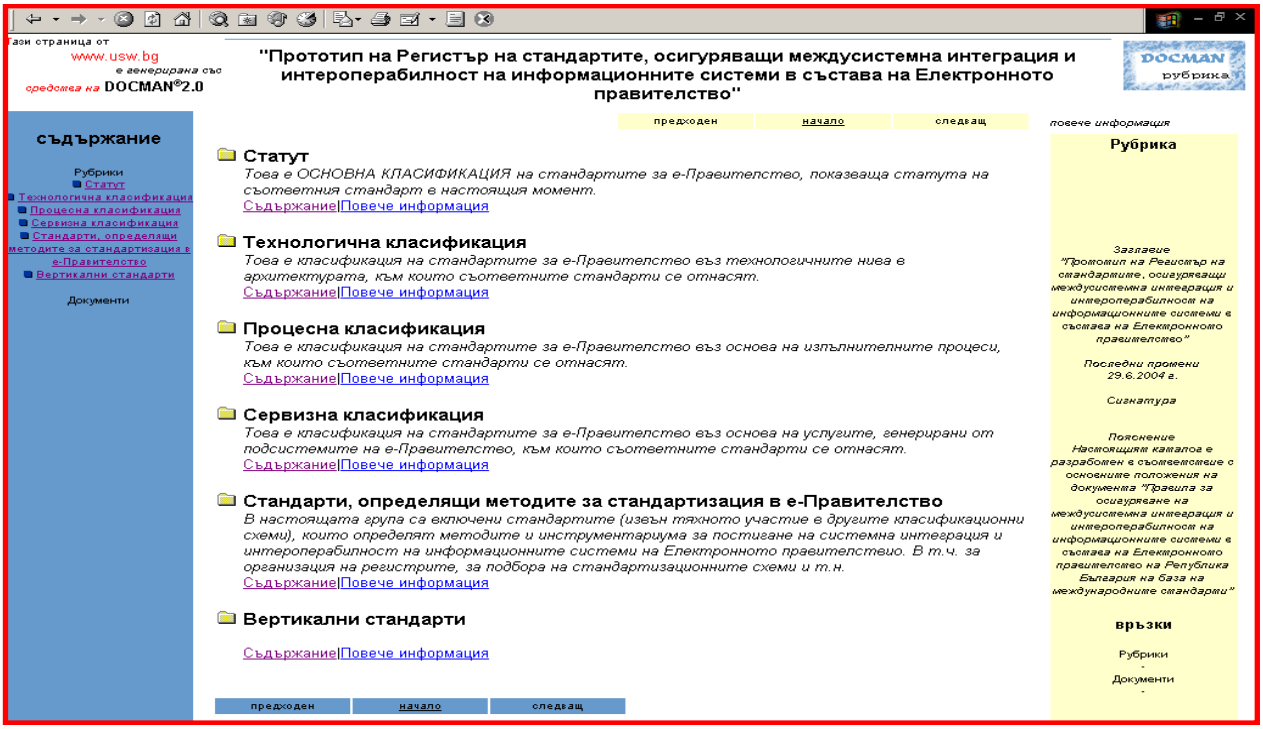


Figure 3-8

The Conformance Testing Procedures

The Bulgarian e-GIF provides Certification Procedure based on Instruction of the State Agency for Information Technology and Communications. In accordance with the European practice this can be a "Third Party Conformity Assessment" realized by accredited bodies.

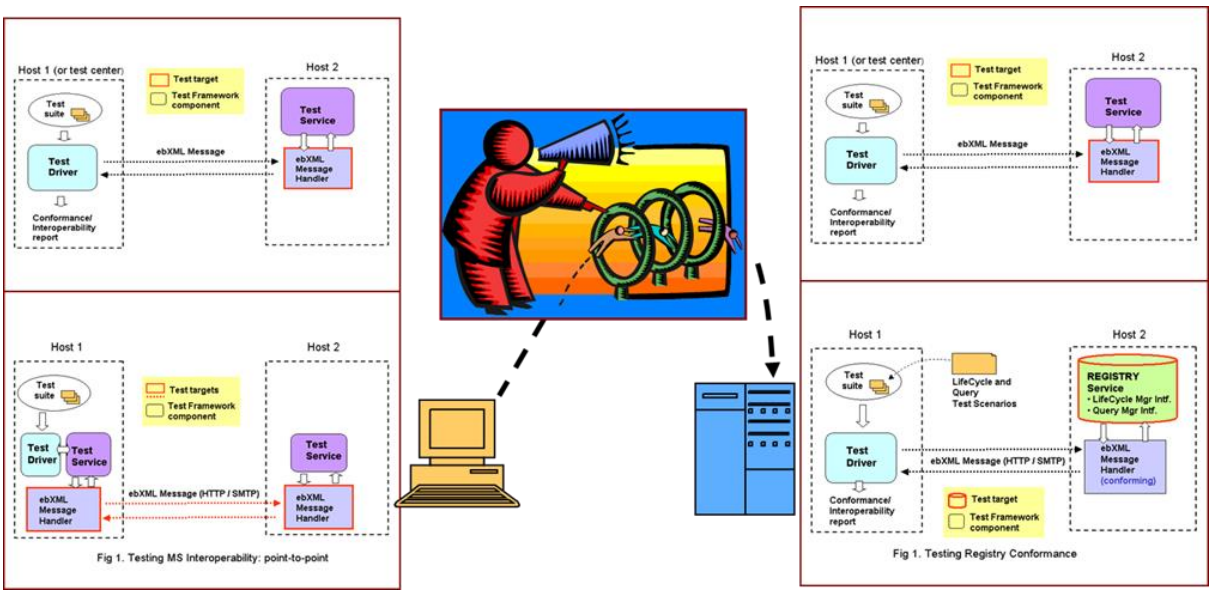


Figure 3-9

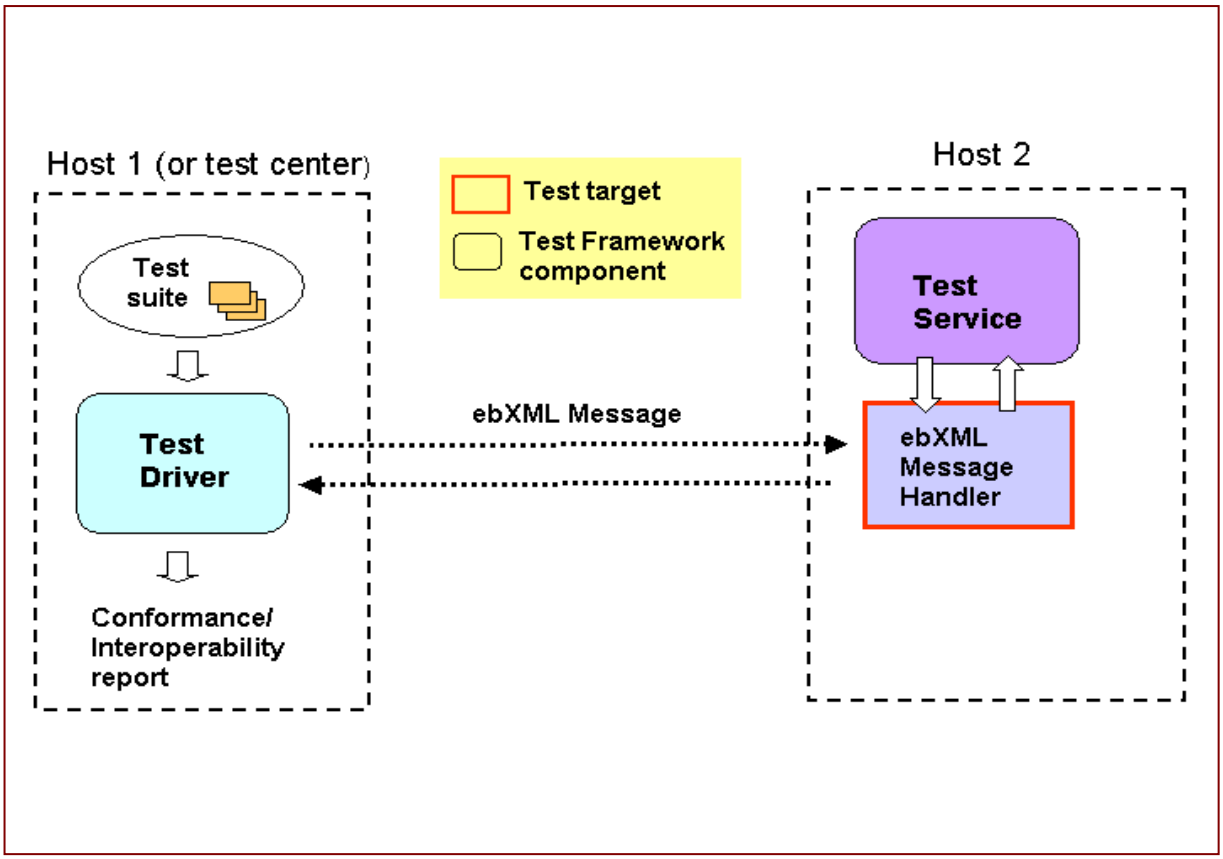


Figure 3-10

CONCLUSIONS

The “Bulgarian National e-Government Interoperability Framework” together with the attendant documents defines and regulates a consistent, functionally completed and efficient environment, which meets the requirements of the system integration and the interoperability.

CHAPTER 3.2

REQUIREMENTS OF THE E-GOVERNANCE ACT AND ORDINANCES

Regulatory and legal framework

The following legislative documents form the national legal framework for the electronic governance and, respectively, for interoperability:

1. The Law on e-Governance regulates three main groups of relations, namely:

- the ways of providing services to citizens electronically;

- the relationships related to the internal exchange of information and documents, simultaneous movement of paper and electronic documents, assigning them creation, storing and archiving of electronic documents;

- relations associated with the automated exchange of electronic documents between administrative authorities.

In its Chapter Four "Interoperability and Information Security" the Law enacts:

"Article 43 Requirement for Interoperability: Provision of internal electronic services and exchange of electronic documents between the administrative bodies shall be carried out in conditions of interoperability."

2. The Law on Electronic Document and Electronic Signature enacts that the legal implications of electronic form of the statements are identical with the ones of a written one, respectively, the electronic signature is equal to the handwritten one. The law established the legal foundation for the security of electronic exchanges with a view to validity and content integrity of electronic statements.

3. The Law on Electronic Communications regulates the public relations realized by provision of electronic communications. The objectives of this Law are: to create the indispensable conditions for the development of competition in the provision of electronic communications, to support the development of the internal market for electronic communications and to create conditions to ensure the integrity and security of public electronic communications networks.

4. The Law on Electronic Commerce regulates public relations connected with the implementation of electronic commerce. The e-Commerce within the meaning of this Act is to provide the services of the Information Society. The services of the Information Society are those services, which are usually onerous and which are provided at a distance by electronic means upon an explicit statement by the service recipient. The Service Provider is a natural or legal person providing services of the Information Society. The Recipient of services is a natural or legal person who uses services of the Information Society for professional or other purposes, including for purposes of seeking information or access to it.

5. The Law on access to spatial data aims to create conditions for access to spatial information, providing services and implementing Directive 2007/2/EC of the European Parliament and the Council of Europe on March 14, 2007 on establishing an Infrastructure for Spatial Information in Europe (INSPIRE)

6. The Law on Protection of Personal Data regulates the protection of the rights of individuals when processing their personal data. The purpose of this Law is to ensure the privacy through the protection of individuals against improper handling of related data in the free movement of data.

The personal data is any information relating to an individual who is identified or can be identified directly or indirectly by an identification number or one or more specific attributes.

7. The Ordinance on the general requirements for Interoperability and Information Security (in force as of 25 November 2008, adopted by the Council of ministers Decree No 279 of 17 November 2008) provides for:

- the general requirements for interoperability and network and information security for the needs of the provision of internal Electronic Administrative Services and the exchange of electronic documents between the administrations;

- the keeping, storage and the access to the Register of the standards;

- the manner of accreditation of the persons referred to in Article 57 (1) of the Law on eGovernance and the requirements for their activity;

- the methods for assessing the conformity to the requirements for interoperability and network and information security.

The scope of Law on e-Governance

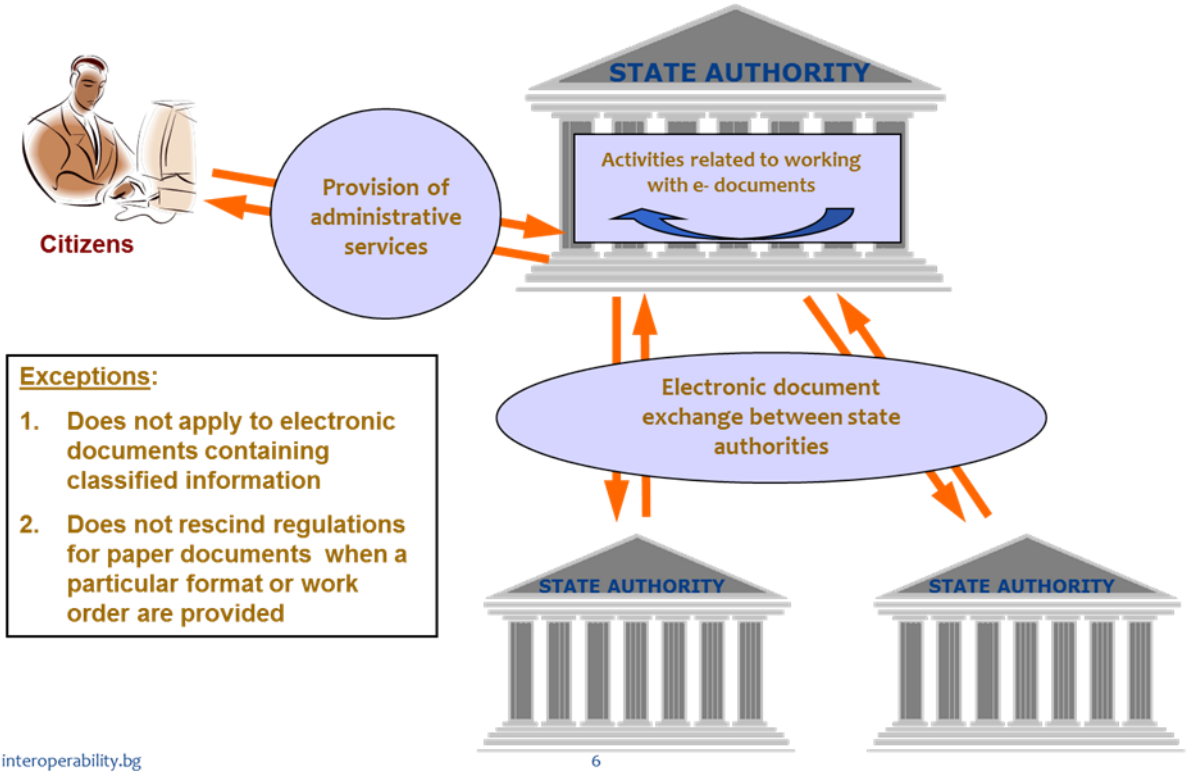


Figure 3-11

The important obligations

- One-off data collection and creation

Administrative authorities, persons performing public functions and organizations providing public services cannot require citizens and organizations to submit or prove such data as they should receive them ex officio from the original data controller[1]

- Official notification: The original data controller should send the data officially to all administrative authorities, persons performing public functions and organizations providing public services, which are required by law to retain the data and have requested to receive them
- Automated provision: The notification and request for data provision are carried out in an automated way, electronically
- Obligation for identification: The obligations arise if the citizen, the organization, respectively, have indicated a unique identifier

The architecture of e-Governance

The e-Governance Law and its ordinances define a new type of architecture in the organization of administrative activities. These regulations contain a set of instructions concerning the conduct of the interface of the administrations in their relation with citizens and businesses. For the most part, these instructions concern the provision of administrative services electronically.

The unification is the most important element in the transition to the new type of administrative organization, namely "service-oriented activity". In this regard:

a) all requests (external or internal) are treated similarly in respect to the start of administrative processes (in terms of their quality of "initiating documents");

b) all orders (external or internal) to the administration are treated similarly in respect to the launch of its processes (in terms of their quality of "initiating documents");

c) any process started by the initiating document is presented as a sequence of stages of processing of the respective activity;

d) each stage is defined in a unified form.

In this regard, the organizational and process-oriented aspects of the re-engineering of the Administrative Information System include:

- unification of the stages of the services and procedures;

- unification of internal administrative processes;

- unification of activities` executed by administration;

- formation of the status of implementation of service or procedure;

- providing an uniform means for control of all activities in the administration;

- preparation of internal rules for conduct of administrative activities.

The model of organization of administrative activities in accordance with the requirements for interoperability provides solutions to the following major problems:

[1] interoperability.bg

1. determination of the set of data which is present, organization of administrative activities, organized as a "business-oriented services";

2. determination of the structures and procedures that maintain the specified data;

3. definition of interface controls for receiving data from outside, in connection with the implementation of legal requirements and compliance requirements for interoperability.

The standardization of government business processes and enabling more efficient and effective connections across structural boundaries will result in a range of benefits for government service users and providers. To make government services and information more accessible and to improve the efficiency with which they are provided, government must build the interoperability capability of its agencies, harmonize policies and regulations, integrate programs and streamline business processes.

A more standardized and uniform set of processes will ensure that government is more responsive to both challenges and change. The ability of agencies to respond efficiently and effectively to policy or structural changes is enabled by interoperability between business processes and the people and systems which support them.

The practical realization of business process interoperability in Bulgarian administration is through creation and support of unified stages of services and procedures. Each procedure in AIS must be composed of unified stages. These unified stages must be registered in the Register of registers and data.

The base models for technological environment with interoperability are as follows:

1. Model of the procedures and data - this is a fundamental model, which is directly related to the creation of other models. To be able to ensure its use it is necessary to perform unification and formalization of the basic data set. According to interoperability, this set is called the Core components. That is, the creation of these Core components is an integral part of creating the model itself.

2. Model of organization of administrative activities in accordance with the requirements for interoperability. The model provides the solutions to the following major problems:

a) determination of the set of data which is present in the organization of administrative activities, organized as a "business-oriented services";

b) determination of the structures and procedures that maintain the specified data;

c) defining interface controls for receiving data from outside, in connection with the implementation of legal requirements and compliance requirements for interoperability.

3. Model for certification of IT resources to meet the requirements for interoperability. The most important task of the model is to regulate in detail the involvement of a third party to conduct the tests for certification.

4. Model for control of the administration in implementing the requirements for interoperability. The model provides a complete regulation of the administrative capacity and its use in control of the administration in implementing the requirements for interoperability.

5. Model for controllable and secure exchange of data between administrations. This model is the basis for establishing a technical resource that implements a secure and controllable exchange of data between administrations.

The requirements of the Law on e-Governance

Art. 17: The technical requirements for provision for access to electronic administrative services and the electronic administrative services providers' policies for graphic and other interfaces of the information systems used, as well as the types of electronic documents accepted by the providers of electronic administrative services shall be published on the website of the Ministry of State Administration and Administrative Reform and on the integrated portal for access to electronic administrative services and shall be compulsory for all persons during receiving, respectively transmitting electronic documents from and to the providers.

Art 20: The electronic documents submission by citizens and organizations shall be done:

1. on-line by using standard protocol by the means of publicly accessible web-based application;

2. through the Unified Environment for e-Documents Exchange;

3. by other means for electronic documents submission, as specified in the Ordinance

The interfaces must ensure the performance of the electronic statements and the creation of the electronic documents in accordance with the requirements of the Law on Electronic Document and Electronic Signature in simple and comprehensible way for operation by the users, including persons with disabilities.

Art 40: The administrative bodies shall be obliged to provide to each other internal electronic administrative services related to fulfilment of their competences and to the provision of electronic administrative services to citizens and organizations.

Internal electronic administrative services shall be provided compulsory through the Unified Environment for e-Documents Exchange.

Art 43 - 46: Provision of internal electronic services and the exchange of electronic documents between the administrative bodies shall be carried out in conditions of interoperability.

The general requirements to the interoperability and information security shall be laid down in an Ordinance.

The Minister of Transport, information technology and communications shall ensure integration of the national information systems with those of the European Union Member States with a view to create opportunity for provision of trans-border electronic administrative services.

The administrative bodies shall be obliged to use the established on the basis of this Law uniform standards and rules setting out technological and functional parameters, which are maintained by their information systems in order to achieve interoperability.

The semantic interoperability of the exchange of electronic documents between the administrative bodies shall be ensured through:

1. unification of the titles of the data subject to keeping in databases or registers;

2. formalization of the data and of the administrative services for ensuring technological opportunity for automatic exchange between the administrative bodies and the data processing;

The formalized data and formalized description of the electronic administrative services shall be entered in the register of the information objects, respectively in the register of the electronic services.

Art. 56 - 57: The administrative bodies shall use information systems, which have been certified for conformity with the requirements of this Law for interoperability and information security.

When organizing public procurement for introduction of information systems, the administrative bodies shall include compulsory requirement these systems to be certified for interoperability and information security.

The conformity of the information systems introduced by the administrative bodies with the established legal requirements shall be attested by the Minister of Transport, information technology and communications. The methodology and the rules for carrying out the assessment shall be laid down in an Ordinance.

Art 60: The Minister of Transport, information technology and communications may carry out inspections of the information security and interoperability of a given information system or of the measures taken by the administrative body by persons empowered by him/her, as well as may give prescriptions for their improvement.

Ordinance on the general requirements for interoperability and information security

Art. 1: The Ordinance shall provide for:

1. the general requirements for interoperability and network and information security for the needs of the provision of internal electronic administrative services and the exchange of electronic documents between the administrations;

2. the keeping, storage and the access to the Register of the standards;

3. ….;

4. the methods for assessing the conformity to the requirements for interoperability and network and information security.

Connectivity requirements

Art. 4-5: The administrations shall be obliged to send and to receive electronic documents among each other for the needs of provision of internal electronic administrative services through the Unified Environment for Electronic Document Exchange (UEEDE).

In cases when the electronic documents are sent by exception through open networks, the communication interfaces and the protocols for exchange should correspond to the compulsory standards and the legal acts specified in the section “Communication and exchange procedures” in the Register of the standards.

When the documents are sent on-line under a standardized protocol through a publicly accessible web-based application, the communication interfaces and the exchange protocols should correspond to the compulsory standards entered into the Register of the standards.

Interoperability of the data

Art 8: The presentation of figures, letters, punctuation marks and other symbols in the information systems of the administrative bodies must be done through the standards entered in the section “Data integration” of the Register of the standards.

The presentation of illustrations, photos and multimedia must be done through the standards entered in the section “Consumers interfaces” of the Register of the standards.

For compressing of the transmitted data when an electronic administrative service is provided the following methods corresponding to the standards entered into the Register of the standards must be used:

1. for text files – methods of compression without loss;

2. for illustrations, photos, multimedia, etc. - methods for compression with a loss can also be used.

Art 9 - 10: In their activity the administrations shall use only unified descriptions of data, registered in the respective sections of the Register of the registers and the data.

In cases of presence only of a non-unified description of data, the respective administration shall create unified description of these data and shall start to use them after registration in the Register of the registers and the data.

Interoperability of electronic documents

Art. **11 -19**: The formalized electronic documents exchanged between the administrations and issued by them towards other persons and organizations must have data organization corresponding to the information objects entered into the Register.

The visualization applications of electronic documents and the editing applications of electronic documents must be certified for conformity with the interoperability requirements .

The applications that ensure only visualization of electronic documents must visualize their content, while:

1. the content of all data shall be visualized according to the instructions entered during their registration in the Register of the information objects;

2. the name with which the data have been entered into the Register of the information objects shall be visualized for all data;

3. access to the text of data definition with which they have been entered into the Register of the information objects through a suitable interface shall be provided for all data;

4. indication for the name of an error in accordance with their registration into the Register of the information objects if the verification for their validity is unsuccessful shall be made for all data;

5. access shall be provided to the text of its definition with which it has been entered into the Register of the information objects through a suitable interface for every error found.

The applications ensuring editing of electronic documents besides the functions for visualization of content of an electronic document must contain also functions for:

1. recording and reading of file content of an electronic document in and out of the file system environment, being directly under the control of the consumer of the editing application, including when situated on a portable physical carrier;

2. introduction, correction and deletion of value for all data in an electronic document.

The applications must ensure an opportunity for establishing unconformities in the content of a visualized or edited document with its registration into the Register of the information objects.

Interoperability of information systems

Art 20 -23: The administrative information systems referred to in Article 4 and the subsequent of the Ordinance on the internal flow of electronic documents and documents on a paper copy in the administrations must correspond to specific requirements. These rules also to

the specialized information systems ensuring fully or partially the functions of an administrative information system as far as they create electronic documents regulated in the Ordinance on the internal flow of electronic documents and documents on a paper copy in the administrations.

In case of automatic creation of electronic documents by an information system, verification for the implementation of the requirements shall be performed during the creation. In case of unsuccessful verification the creation is terminated and this shall be communicated to the employee performing functions for processing in a non-automated regime or controlling the automatic execution of a stage of a service or procedure, whereat the creation of the document is being done.

The verification shall be performed by a certified application for verification for interoperability of electronic documents integrated into the information system. The availability of the application is an obligatory prerequisite for certification of an information system.

The information systems must ensure portability of all data contained in them in cases of unforeseen circumstances while allowing for the transfer of the data from them into the content of an electronic document of the type "Data for transfer between information systems" and their introduction into another information system.

The data subject to transfer shall be identified as composition and content in the Ordinance on the internal flow of electronic documents and documents on a paper copy in the administrations.

The information systems must visualize the data they keep, while:

1. the content of the data shall be visualized according to the instructions entered during their registration in the Register of the information objects;

2. for the relevant data the name with which they are entered in the Register of the information objects shall be visualized;

3. access for the relevant data shall be provided through a suitable interface to the text of their definition with which they have been entered into the Register of the information objects.

Compliance verification

Art 98 -101: The administrations shall be obliged to use only information systems and program applications which are certified for conformity with the interoperability and information security requirements established by the Law on E-Governance and the implementing regulations.

No certification shall be made using the procedure of the Ordinance for:

- information systems intended for processing and storage of classified information;

- information systems with special purpose (national security, defense, etc.);

The certification shall be made while observing the principles of lawfulness, independence, impartiality, publicity and equality.

The information systems and the program applications certified using the procedure of the Ordinance shall be entered into a public list of the certified information systems kept

The specification for the development of information systems should contain explicit and clear indication whether it falls into the scope of the administrative information systems.

Certification of applications for e-Documents

Art. 108 – 111: For every type of electronic document registered in the Register of the information objects the interested person shall present a set of documents of the same type

containing test data for performing tests for conformity with the registration in the Register of the information objects. In the set of documents only one document should not contain deviations from the registration of the respective type of document.

The tests shall be created in a way that permits the wrong values specified in them and the irregularities in the organization of the data to present all possible deviations from the registration of the respective type of document in the Register of the information objects. For every document containing the test data the interested person shall present a document of the type "Registered errors in a content of a document" which contains a description of the errors in the test document in accordance with the nomenclature of the errors for the information objects contained in the documents that has been entered into the Register of the information objects.

The certification for interoperability and information security of an application for visualization or editing of electronic documents should cover the following:

1. reading and visualization of a content of an electronic document from file recorded in the information system being under control of the consumer or recorded on an external carrier;

2. compiling of an electronic document of the type "Registered errors in content of a document" containing the results from verification of the stored electronic document for conformity with its registration in the Register of the information objects;

3. availability of functionality for true and correct visualization of all errors – a result from tests with the set of documents containing test data in performing the verification;

4. availability of functionality for true and correct visualization of the messages containing the names and the descriptions of all errors caused during the tests with the set of documents;

5. availability of functionality for true and correct visualization of the content, the name and the description of all data in accordance with the registration of the visualized electronic document in the Register of the information objects.

Certification for interoperability and information security of an application for verification of electronic documents for conformity with their registration in the Register of the information objects

It is necessary to realize following verifications in order to establish the technical functionality of the application for:

1. reading the content of an electronic document from a file recorded in the information system being under control of the consumer or recorded on an external carrier;

2. creation of an electronic document of the type "Registered errors in a content of a document" containing the results from the verification of the stored electronic document for conformity with its registration in the Register of the information objects.

Certification of administrative information system

An interested person can request certification for interoperability and information security of information systems. This person shall present an installation package along with a detailed manual for installation and use.

The interested person shall be obliged to specify:

1. the data related to the certification of an application integrated in the information system when making verification for interoperability of electronic documents;

2. the technical requirements regarding the environment in which the information system will be installed and tested.

For every document created by the administrative information system referred to in Annex 1 to the Ordinance for the internal flow of electronic documents and documents on a paper copy in the administrations, verification shall be made for:

1. the possibility for entering of the values of the data in the composition of a verified document in manual or automatic regime;

2. the possibility for generation in manual or automatic regime of a valid document of the verified type containing the data.

The verifications for the implementation of the requirements 2 shall be made in the following sequence:

1. the electronic documents created during the tests shall be entered into the information systems;

2. a document "Data for transfer between information systems" shall be created;

3. the availability in the document referred to in p. 2 of the documents referred to in p. 1 and the data accompanying their entry shall be verified;

4. they shall be entered into the information system according to three values for every type of data supported by it and their availability in the document referred to in p. 2 shall be verified.

The set of data for the verification shall cover all data described in the Ordinance for the internal flow of electronic documents and documents on a paper copy in the administrations,.

For all these data verification shall be made for:

1. true and correct visualization of the name of the data;

2. true and correct visualization of the definition of the data.

Register of certified systems and products

In the register of the certified systems and products, circumstances about information systems and products shall be entered. This register is a data base managed by an information system containing the descriptions of the composition and the organization of the data. History of the entries shall be kept in the lists.

The following circumstances for objects of the type "certified systems" shall be entered into the section "Certified systems" from the Register of the certified systems:

1. data identifying the certified system such as model, version, configuration, etc.;

2. data identifying the interested person;

3. data for the accredited person who has made the certification;

4. scope of certification including the types of electronic documents which are maintained by the system;

5. number and date of the issued certificate.

The following circumstances for objects of the type "certified application" shall be entered into the section "Certified applications" from the Register of the certified systems:

1. data identifying the certified application such as model, version, configuration, etc.;

2. type of certified application - application for visualization and/or editing or application for verification of electronic documents for conformity with their registration;

3. data identifying the interested person;

4. data for the accredited person who has made the certification;

5. scope of certification including the types of electronic documents maintained by the application;

6. number and date of the issued certificate;

7. hyper connection for access to the installation package of the application when the certified application has been entered as circumstance in the Register of the information objects or in the Register of the electronic services.

The following circumstances for objects of the type “certified specification” shall be entered into the section “Certified specifications” from the Register of the certified systems:

1. data identifying the certified specification;

2. data identifying the interested person;

3. data for the accredited person who has made the certification;

4. number and date of the issued certificate.

CHAPTER 3.3

REALIZATION

Introduction

Unlike most current practice of autonomous development of information systems in each administration, the requirement of the Law on Electronic Governance for single input of data concerning citizens and businesses causes need for intense information exchange between the administrative systems.

Therefore, the achievement of interoperability for the purpose of this exchange and a certain acceptable level of the network and information security for administrative information systems at all becomes a requirement for their interaction.

The impending inclusion of the Bulgarian administrative information systems for pan-European cross-border electronic services is also linked to these conditions. Therefore, the Law and its regulations provide requirements and measures to achieve them.

The six ordinances to the law constitute some kind of second level of regulation. These ordinances as a whole create consistent and functionally complete environment of requirements for information systems of the administration.

These requirements are aimed primarily at ensuring the smooth exchange of so called internal electronic administrative services and the opportunity that the electronic administrative services provided by each body can be included in the value-added chains without special action by its supplier.

The requirements set out in the six ordinances mentioned above affect both "external" behavior of information systems of administrative authority (having a direct bearing on the interoperability) and "internal" behavior (relevant for the organization of administrative processes, the data model and the network and information security).

Unlike the Bulgarian National Interoperability Framework, which has actually a "framework" nature, the Ordinance on interoperability and information security introduces a layer of requirements capable to be objectively checked in and to be underlid in the procedures for certification of information systems and products.

The implementation of these requirements is objectified consequently the operation of the systems composing so called "Meta-level of e-Government”:

- the Unified Environment for e-Documents Exchange (UEEDE) and

- the six registers making up the "National Administrative Data Model”.

Besides these requirements, which are included in the certification procedures, the ordinances define a number of requirements, which are liable to subjective control.

3.3.1
STANDARDIZATION

The selection of the standards

The choice of the fundamental platform for standardization is crucial because of the diversity of standards and specifications relating to interoperability.

The evolution of the standardization process in terms of system integration and interoperability refers this choice to the so called SOA (Service-Oriented Architecture). This architecture not only allows the transfer of information from application to application in different systems, but also the creation of complex applications through services supported in remote systems by sharing a common business logic between applications.

The standardization of administrative information systems in the area of interoperability and information security covers a wider area than that of the so-called "Formal harmonized standards" enforced by the official intergovernmental standardization bodies (eg ISO, ITU - globally or CEN, CENELEC, ETSI – at the European level). This includes informal and hybrid standardization processes - production of the sector consortia as: OASIS, IETF, W3Consortium, UN / CEFACT, OMG and others.

In terms of the fields of application the standards are divided into two main groups:

- horizontal - for general application (in all areas);

- vertical - with applications in a specified area (industry, etc.). As an example, for the purposes of administration that can be: medical informatics, banking, geographic information systems, industrial product systems, etc.

The evolution of the standardization process follows the paces of the evolution in the system integration.

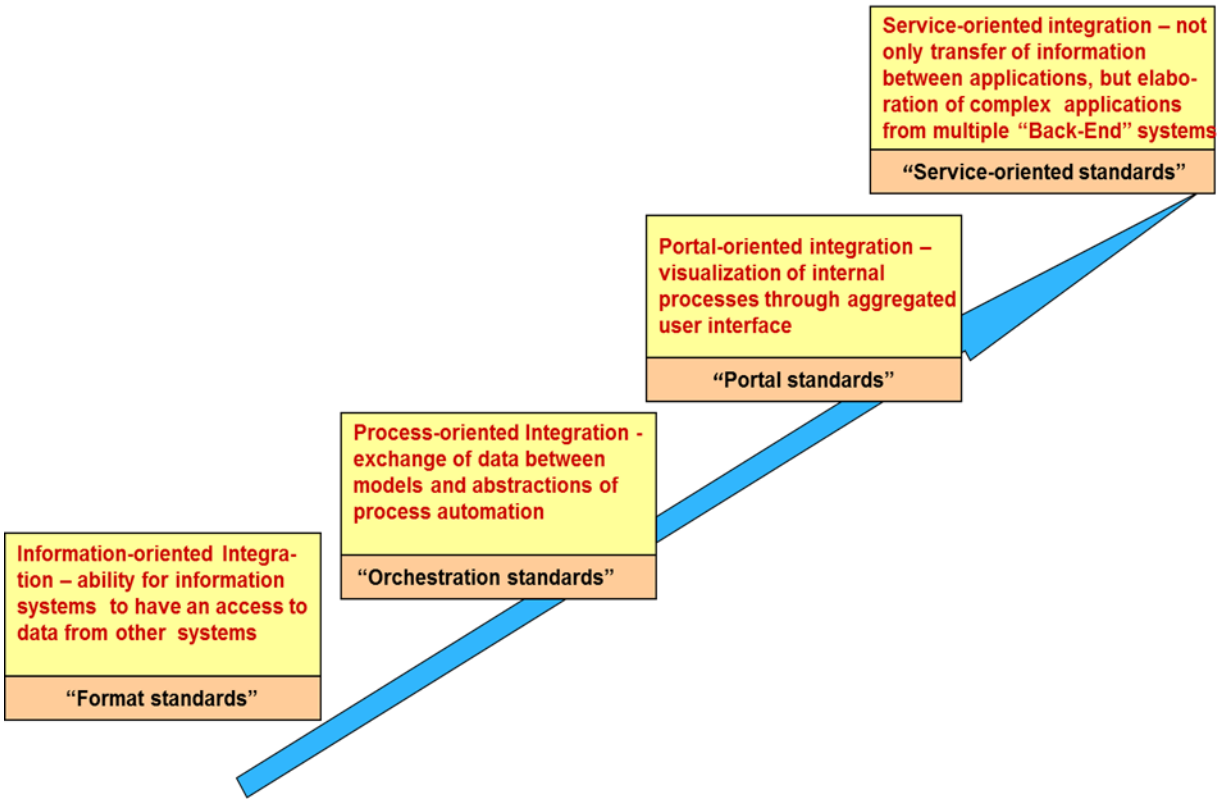


Figure 3-12

Vertical components of interoperability

Each vertical (or sectorial) interoperability can be seen as an upgrade over the common (or horizontal) interoperability provided by the National framework.

Some examples:

- in e-Health - standards developed by CEN / TC 251, ISO / TC 215, HL7, DICOM and IEEE;

- in e-Banking - the standards developed by SWIFT, FIX, ISO 15022;

- in e-Learning – standards developed by ADL (SCORM), IEEE-LTSC (LOM), etc.

The Register of standards

The Register of the standards is a database managed by an information system containing technical standards and specifications which have to be applied by the administrative bodies for the provision of electronic services as well as for ensuring interoperability and information security.

The Register shall be updated in compliance with the dynamics of the international standardization processes and the possibilities for their application in the current moment.

The new versions of the standards entered into the Register must not create obstacles for the functioning of the already realized solutions unless the standards used in these solutions could lead to violation of the requirements for information security.

Standards in the meaning of the Ordinance are as follows:

1. formal harmonized technical standards in the field of the information technologies, the electronic communications and the information security, approved by the intergovernmental standardization bodies such as ISO, ITU – at international level, or CEN, CENELEC, ETSI – at European level;

2. internationally adopted non-formal and hybrid technical standards and specifications in the field of the information technologies, the communications and the information security – a result of the standardization processes of the sector consortia such as OASIS, IETF, W3Consortium, UN/CEFACT, OMG.

The following circumstances shall be subject to entry in the Register of the standards:

1. Standard title – the full title of the standards established by the international organization that has drafted the standard and maintaining shall be entered translated into Bulgarian language and in original in English language;

2. Identifier of a standard – a code identifier of the standard established by the international organization that has drafted the standard and is maintaining;

3. Clarification for the standard – a brief text clarification for the standard;

4. Version – the last internationally accepted version of the standard;

5. Date – the date of the adoption of the last internationally accepted version of the standard;

6. organization – the data for the organization that has drafted the standard and is holding;

7. text – text of the standard shall be entered if the standard is published with free access by the organization that has drafted the standard and is maintaining it;

8. URL of a publication – the electronic address (URL) is entered on the Internet site from which access is realized to instructions for supply of the standard if it is not with free access;

9. degree of applicability – a characteristics which can have values: “compulsory”, “recommendable”, “under control”, “white list”, “grey list” and “black list” is entered;

10. thematic belonging – a characteristics which can have values: “communication and exchange procedures”, “web-services”, “data integration”, management of the content and definition of meta-data”; “consumer interfaces”; “working stations”; “internal organization of the activity and working processes”, “management of the electronic identity” and “information security” shall be entered;

11. scope of applicability – the possibility for application of the whole standard shall be entered or only the respective parts of it shall be enlisted;

12. URL batch – the automatically generated electronic address (URL) of the Internet site from which access is realized to the content of the batch of the standard in the Register shall be entered.

The procedure for initial entry of a standard or for changes for the entered circumstances shall include:

- acceptance of the application for the entry;

- verification for admissibility and reasoning of the entry;

- verification whether the standard or the new circumstance has been already entered;

- making the entry or issuing of a motivated refusal for making the entry;

- information to the applicant for the refusal for the entry to be made.

In case of initial entry of a standard a batch shall be created for it.

For every created batch a unique register identifier shall be generated consisting of:

1. unique register identifier of the Register of the standards –the unique register identifier created in the Register of the registers and the data during the registration of the Register of the standards in it shall be entered;

2. batch number –the number in turn of the batch in the Register of the standards shall be entered.

The Register of the standards shall be kept unlimited in compliance with the requirements of the Ordinance as a system with a class of information security 3 or A.

The Register of the standards shall be accessible through the Internet site of the Ministry of Transport, Information Technology and Communications. The Minister shall provide opportunity for review of the actual status of the batches of the standards towards the moment of the check-up as well as of their state towards a specific date back in time. Anyone can request and can make a check-up for the entries in the Register through the Internet site of MTITC. The checks in the Register shall be free of charge.

A Council for the standards for interoperability and information security shall be established under the Minister of Transport, Information Technology and Communications. This Council shall be an assisting consultation body and shall include experts assigned with an order of the Minister of Transport, Information Technology and Communications.

The Council for standards for interoperability and information security shall take decisions about the admissibility and the grounds for making entries in the Register of the standards. It can hold meetings if more than the half of its members are present. The Council approve methodology for assessment and preparation of standards in compliance with the document “Common assessment method for standards and specifications” (CAMSS), developed within the framework of IDABC Program of the European Commission.

The structure of the Register of standards

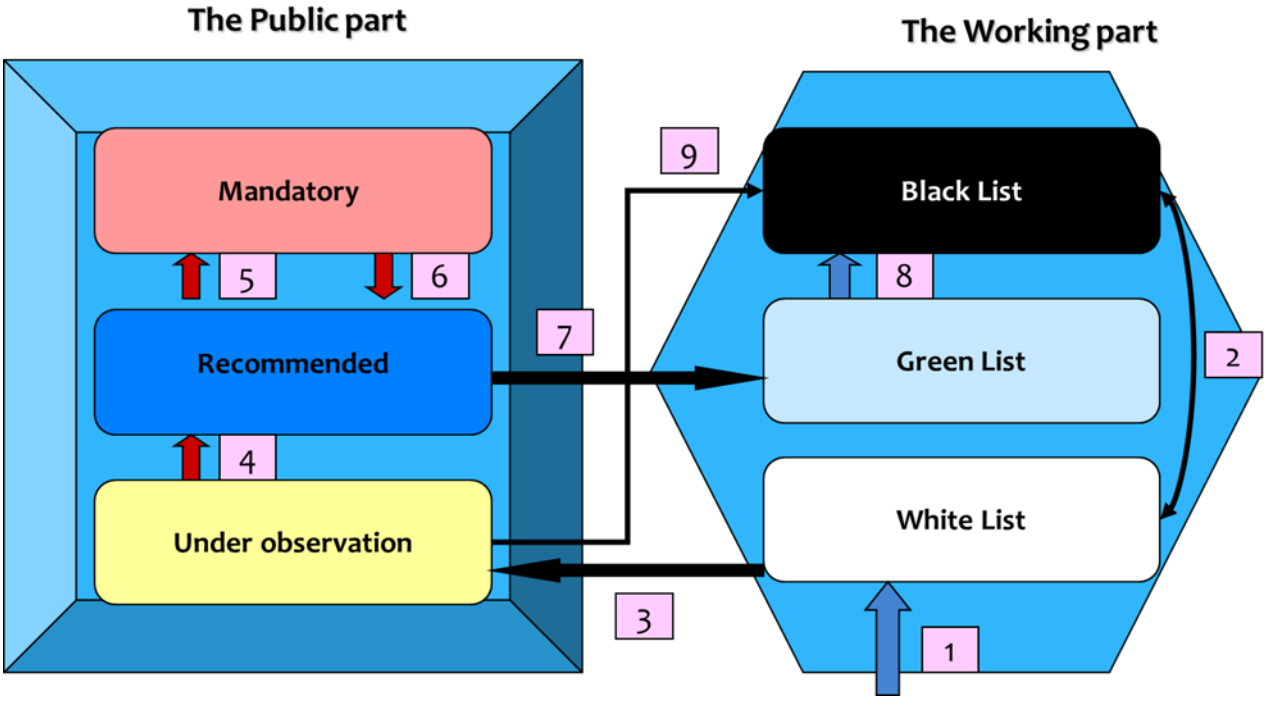


Figure 3-13

The Classification of the Standards in the Register

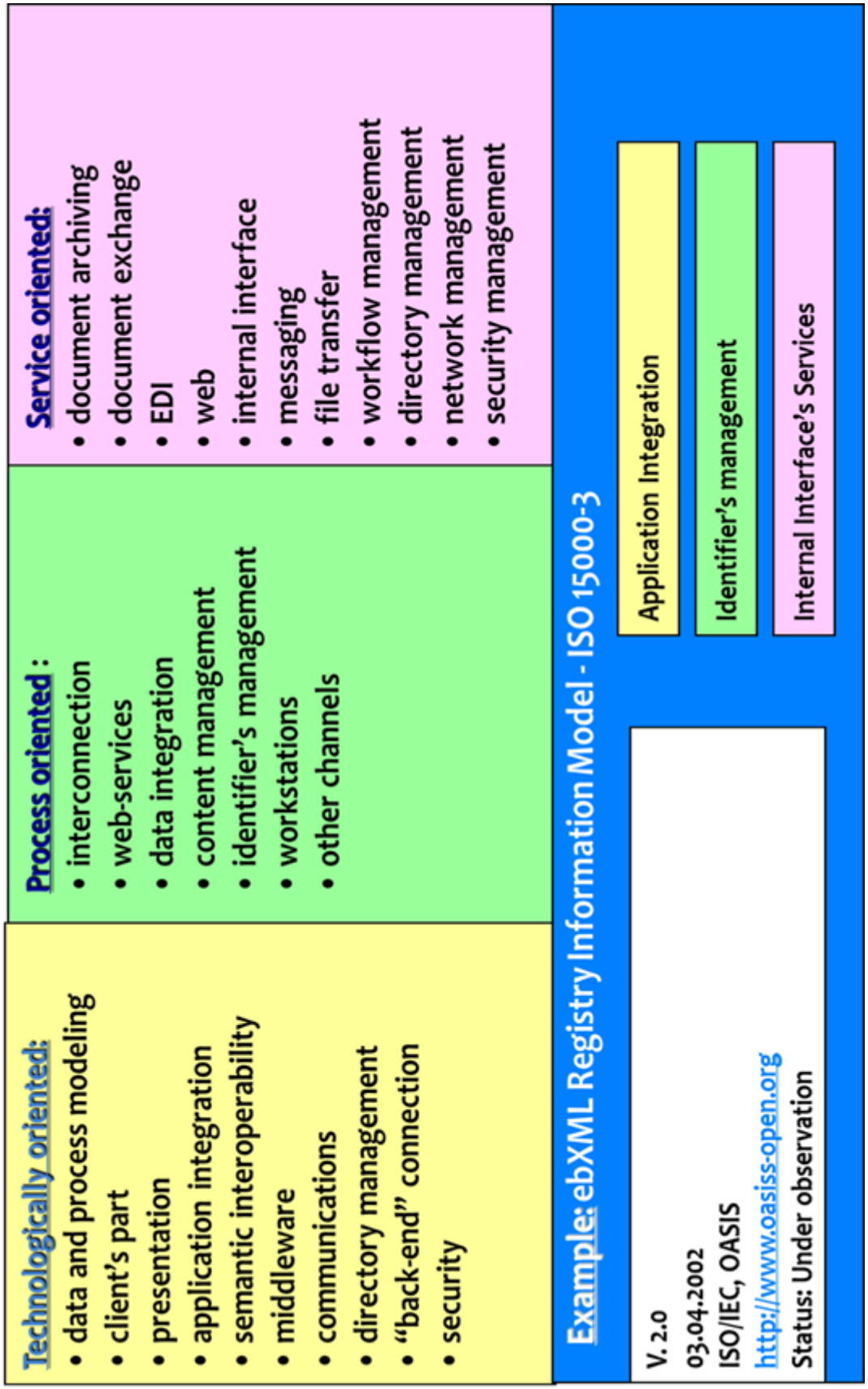


Figure 3-14

The home page

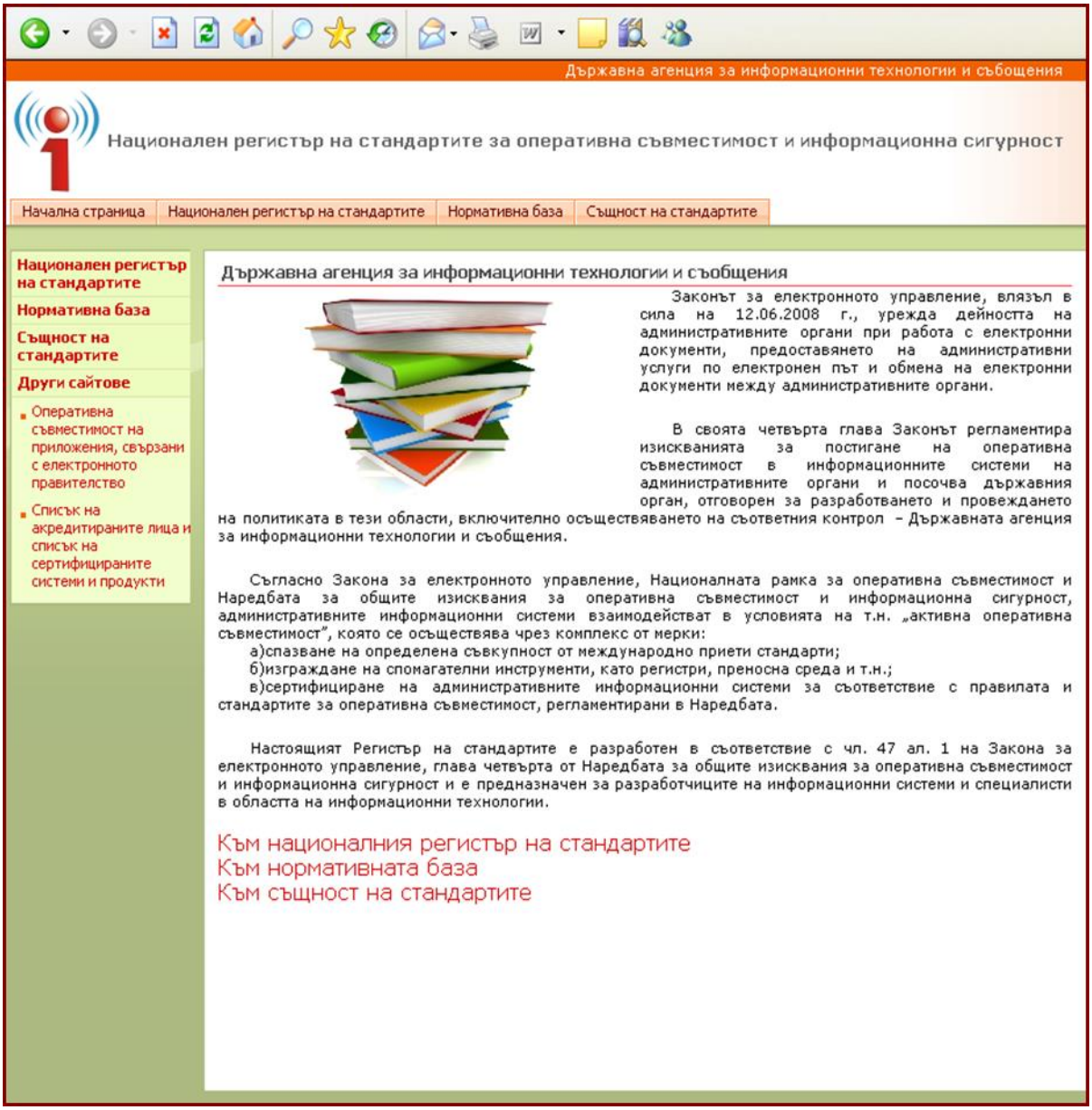


Figure 3-15

Description of standard

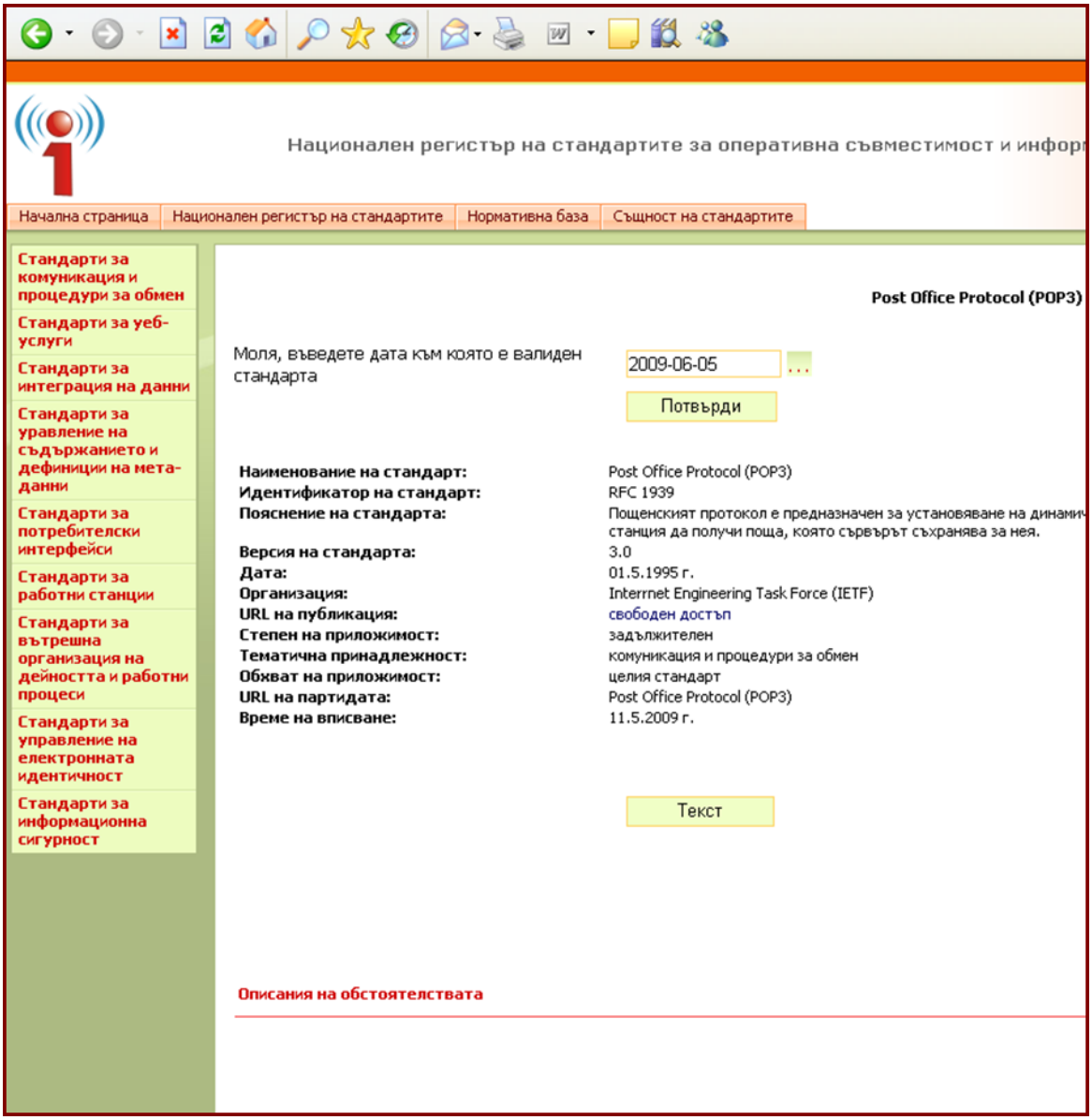


Figure 3-16

Characteristics of standard

Figure 3-17

Concrete characteristic

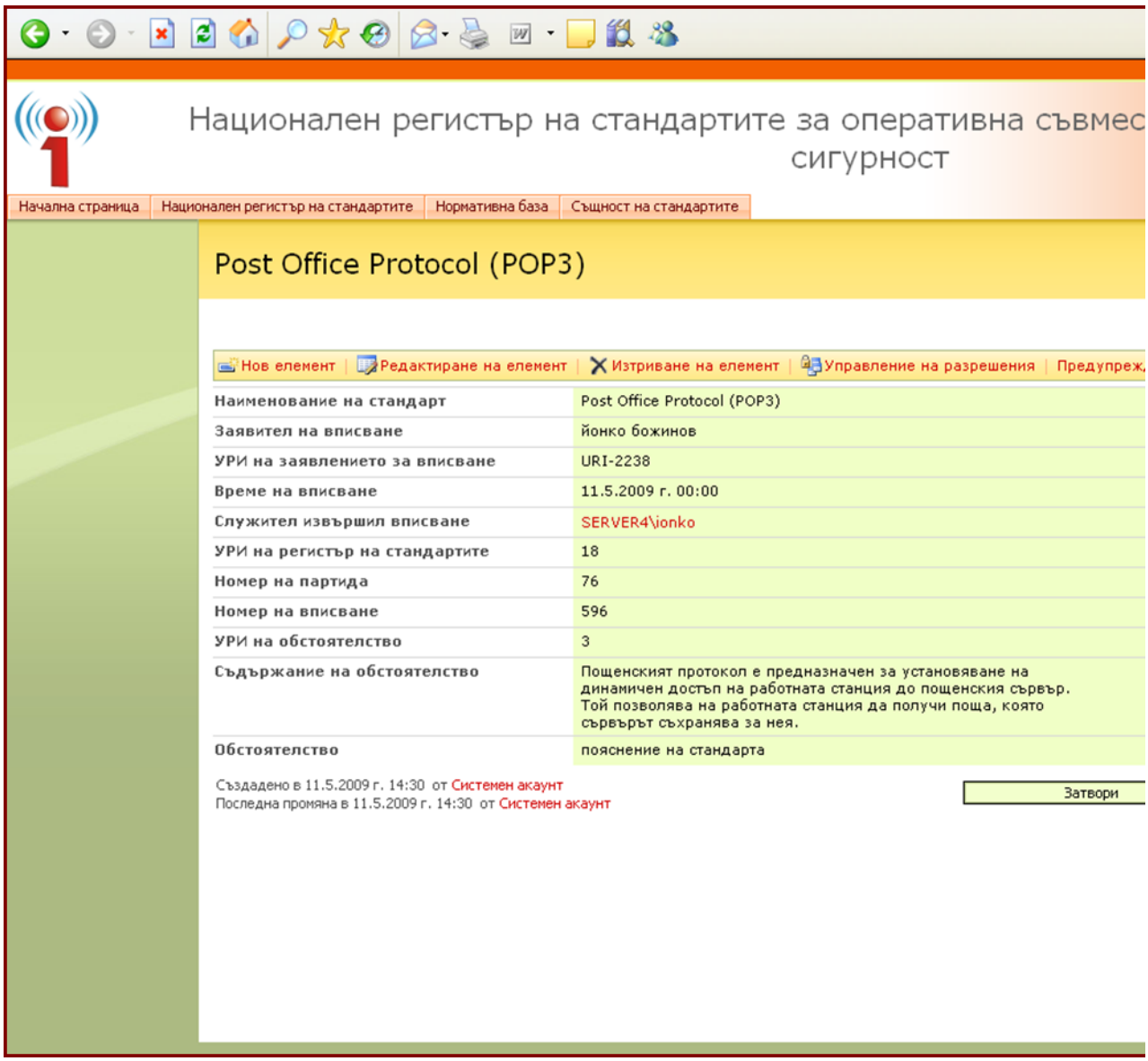


Figure 3-18

3.3.2
NATIONAL DATA MODEL
REGISTERS

e-Government National Data Model

For the purpose of providing electronic administrative services across the entire Bulgarian Public Administration, a National Data Model is required to ensure semantic interoperability of data. Therefore, all data requires a unified definition that includes:

- Data Name and

Extended Data Explanation.

The inclusion of the 'Extended Data Explanation' component in the descriptions of unified data definitions is a precondition for establishing the context in which they are used. Once qualitative good unified data definitions are developed, they provide a sufficient basis for making the relevant formalized definitions in XML format. Further, data unification by using the scheme ‘Data Name / Extended Data Description’ enables standardization of interfaces for editing and virtualization purposes.

The next figure shows the National Data Model with its interrelationships of Registers, which will be explained in more detail further.

e-Government National Data Model

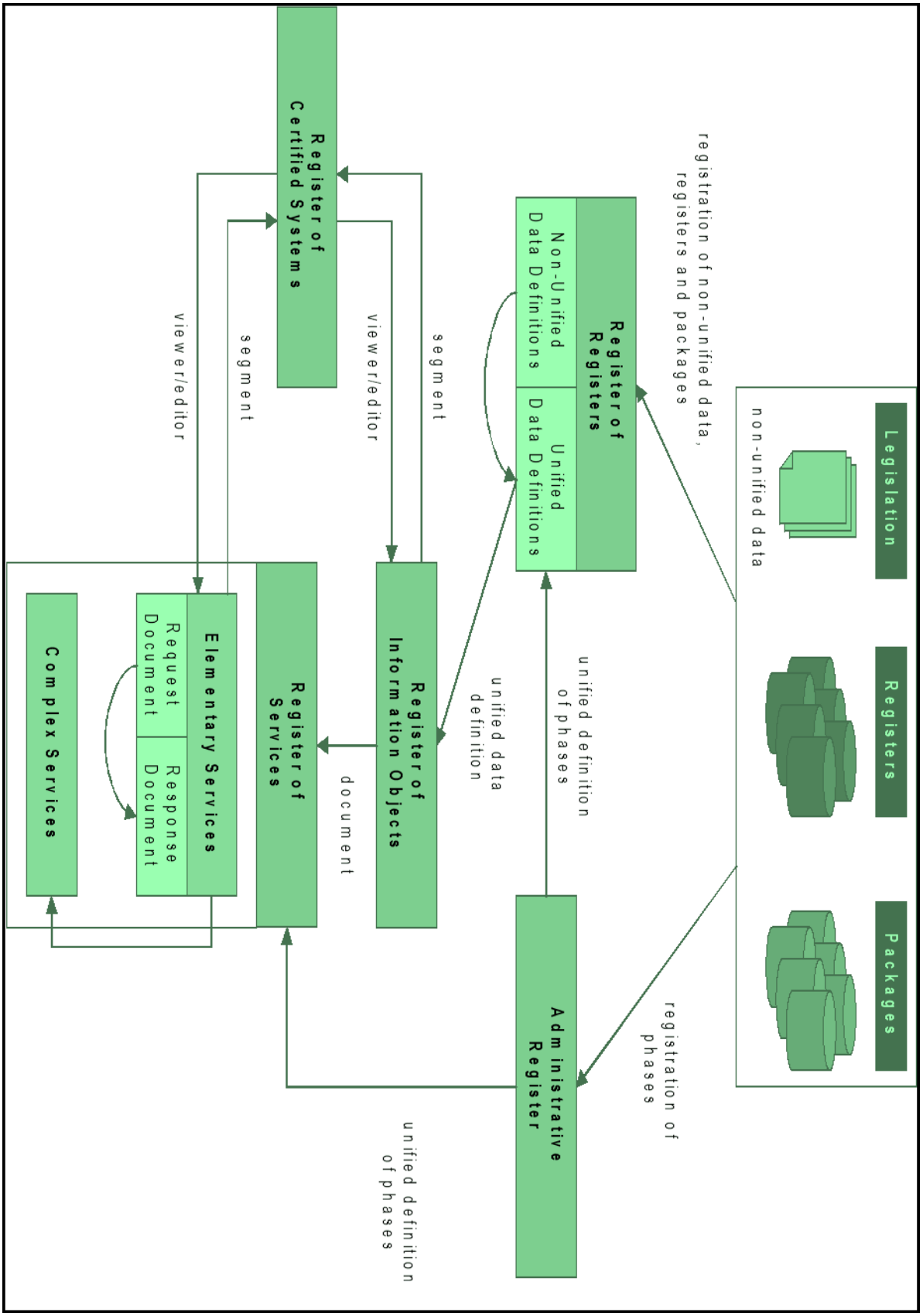


Figure 3-18

Interoperable Content Management

The basis of interoperable content management is the unification and formalization of data definitions. This can be set up as interoperability at "data level". The interoperability can be defined in similar way at the level of data structures, at the level of electronic documents, etc. The tools for practical achievement of interoperability are well known- XML-repositories, clearing processes and so on.

In each country most of the legislative acts set up definitions of data and documents, used in administrations and by citizens. Those data and documents can be pointed out as a "core components", which represent the content created and processed by administrations.

Additional data is needed, in order to manage this content. The suitable basis for defining this data is the service oriented administrative organization (SOAO).

The electronic services can be represented by the definitions of service request, service response(s) and service workflow description. The service requests and response(s) are electronic documents, consisting of a set of data types, registered in the e-Government XML-repository, named by the Law on e-Governance as Register of information objects.

Each type of electronic documents used by administrations has to be registered in the Register of information objects. The purpose of this registration is to legalize the XML-construction of the type of document and the availability of free of charge certified viewer for document's content.

The availability of a certified viewer guarantees the interoperability related to the user's understanding of the document's content.

The interface of electronic services has to be registered in the Register of electronic services. The main component of registration is the service interface definition represented by documents transferring the content of service request and service response(s). Those documents have to be legal, which means that they have to be already registered in the Register of information objects.

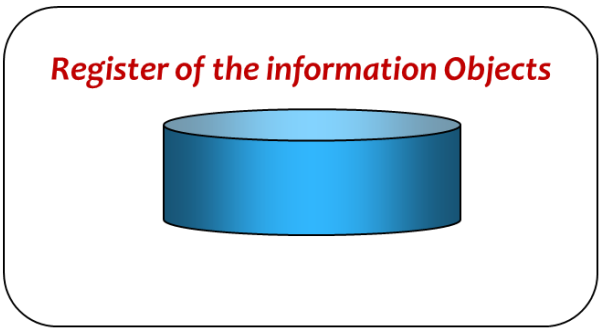
The second component of registration is the service workflow. The legalization of service interface and service workflow guarantees the interoperability related to usage and execution of electronic services.

The "heart" of interoperability

The Bulgarian meta-data model consists of definitions for:

- Terms
- Values
- Nomenclatures
- Segments

The main part of the definitions for values, nomenclatures and segments is the corresponding XML- construction.



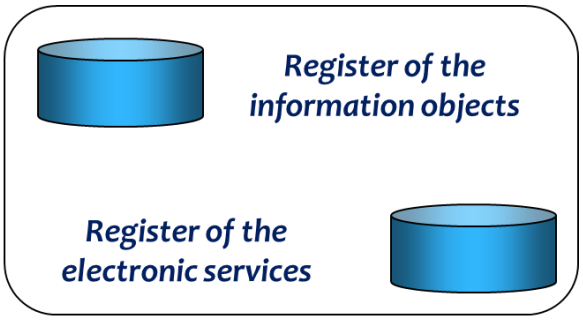
The e-documents are the 5-th type of information object, liable to registration. This registration guarantees that for every e-document is available free of charge application for viewing or editing.

The process of registration and the Register of the information objects itself are under regulation of the Ordinance on the Registers of the information objects and the electronic services

Figure 3-19

A matter of fact

The process of registration and the Register of the electronic services itself are under regulation of the Ordinance on the Registers of the information objects and the electronic services

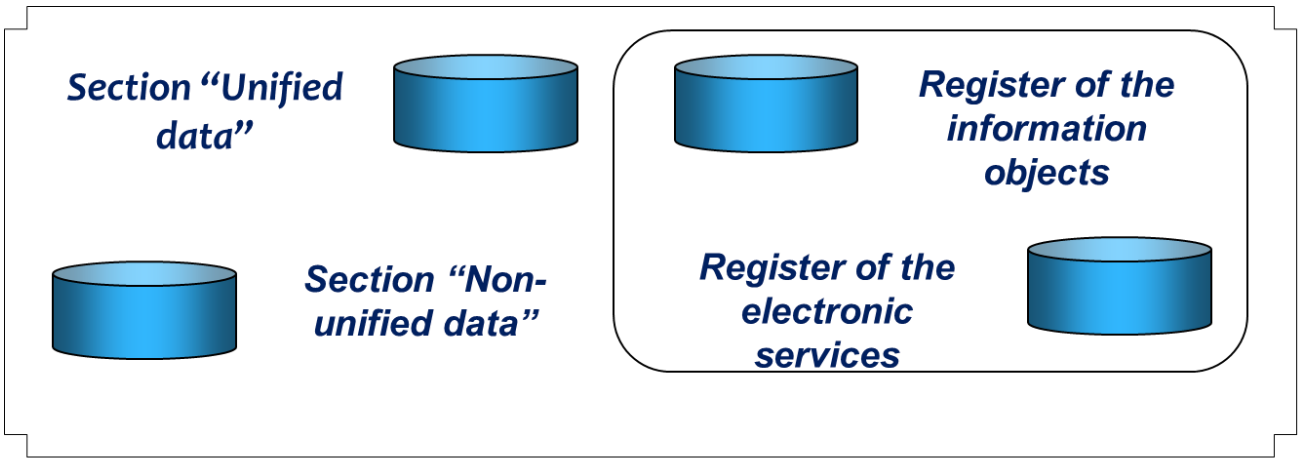


Two type of electronic services are under registration: "Primary services" and "Complex services". The Complex services are "services invoking other services", in accordance with DIRECTIVE 2007/2/EC – INSPIRE.

The main subject of the registration is the services interface, represented by e-documents for service request and e-documents for service response(s).

Figure 3-20

Two important sections of the Register of registers and data

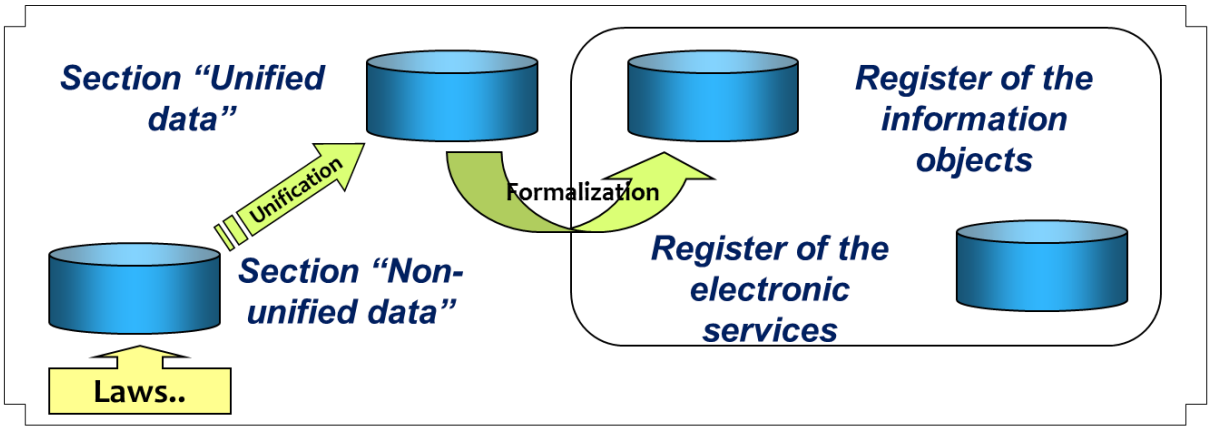


Section "Non-unified data" consists of data definitions accepted directly from law-texts. Section "Unified data" consists of unified data definitions, corresponding to one or more non-unified data definitions.

The process of registration and the Register of registers and data itself are under regulation of the Instruction on the Register of registers and data

Figure 3-21

The "clearing process"



Tree steps to "produce" formalized data definition:

1. Extraction of data definition from law texts and registration as non-unified data definition
2. Unification and registration as unified data definition(s)
3. Formalization (XML- construction building) and registration as formalized data definition

The steps are under regulation of the Ordinance on the Registers of the information objects and the electronic services

Figure 3-22

The "clearing house"

- The ordinance establishes the frame of the rules of clearing process. The Council for entries creates the full set of rules for unification and formalization
- The Council for entries consists of external experts in IT and Law
- The administration of the Ministry of TITC is supporting the clearing procedures
- The Ministry of TITC is responsible for building of IS, supporting the Registers of the information objects and the electronic services and Register of the registers and the data

Figure 3-23[2]

Structure of the data model 1

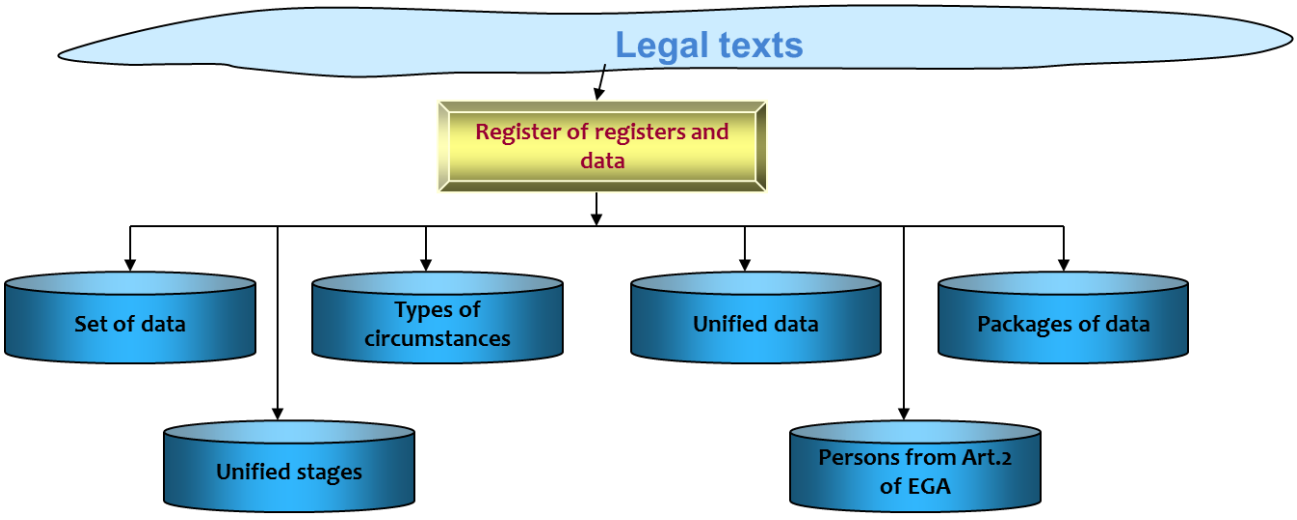


Figure 3-24

[2] interoperability.bg

Structure of the data model 2

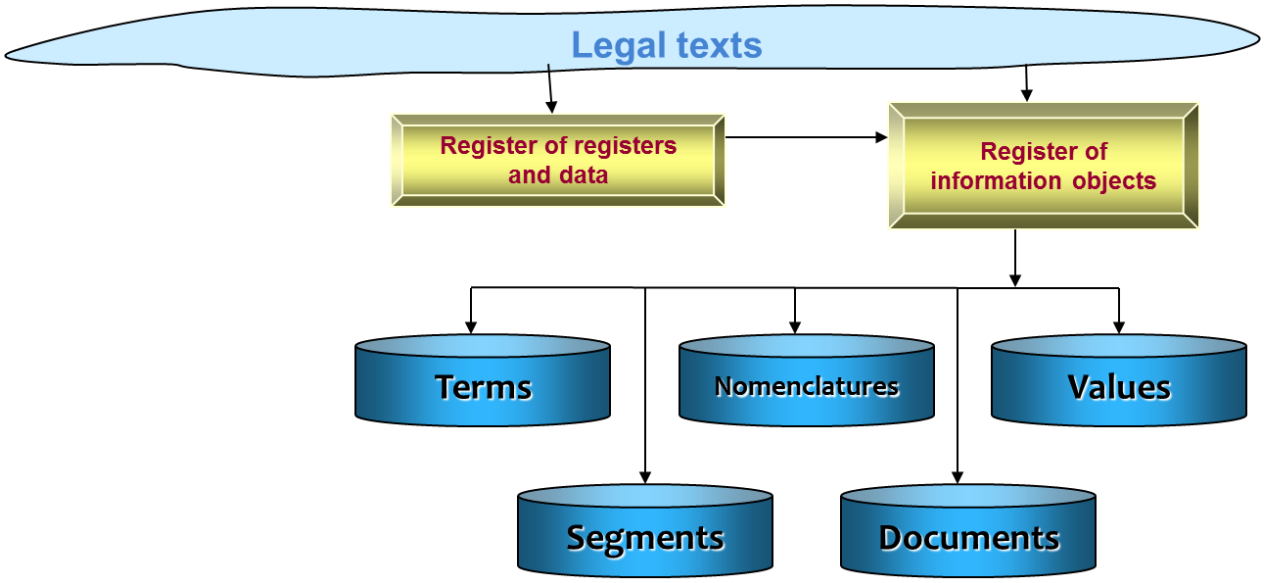


Figure 3-25

Structure of the data model 3

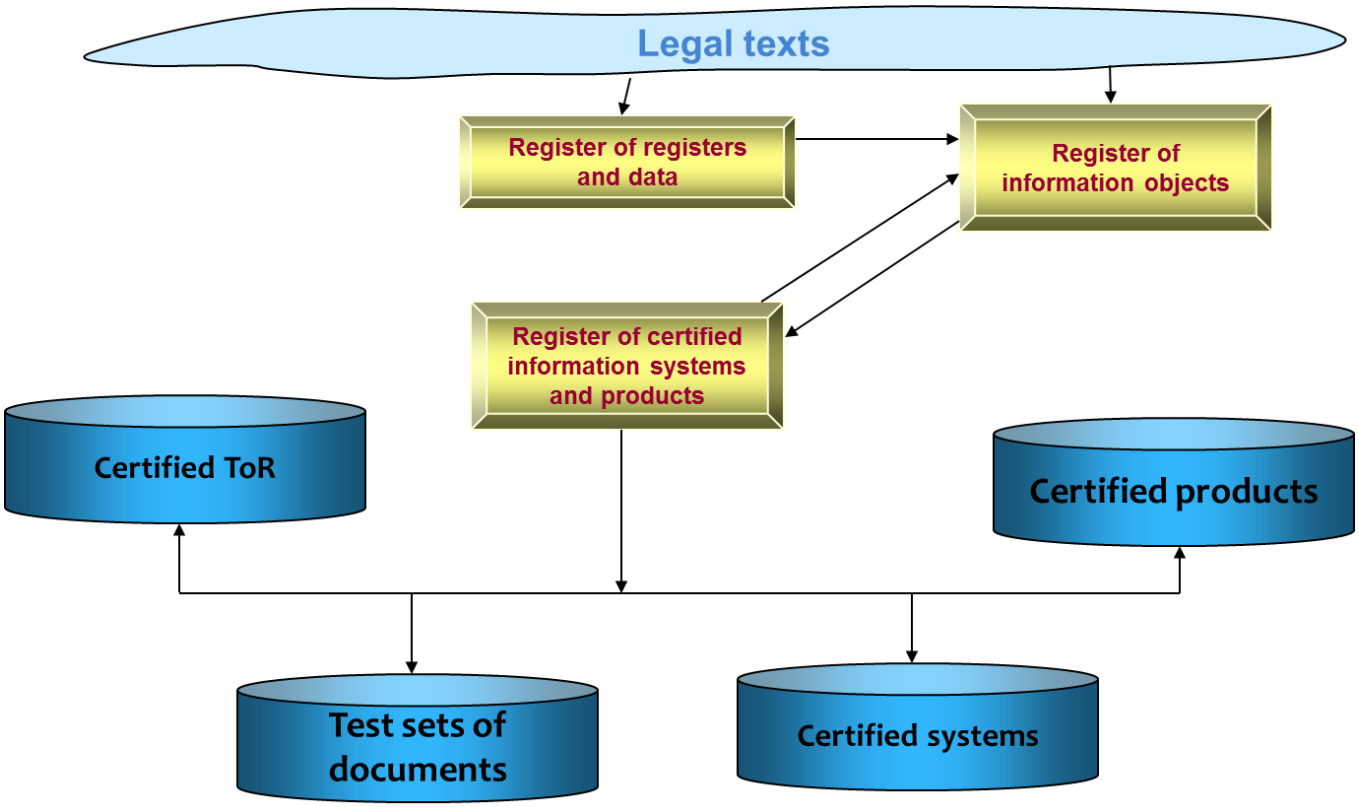


Figure 3-26

Structure of the data model 4

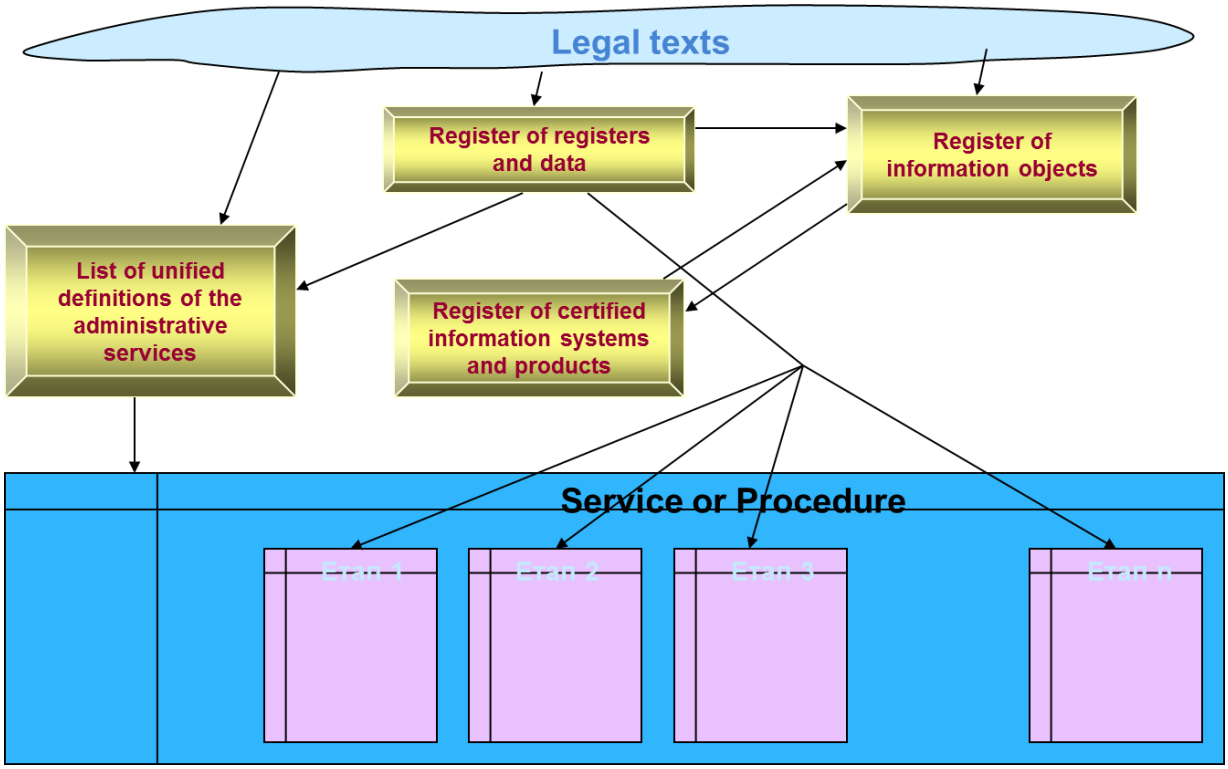


Figure 3-27

Structure of the data model 5

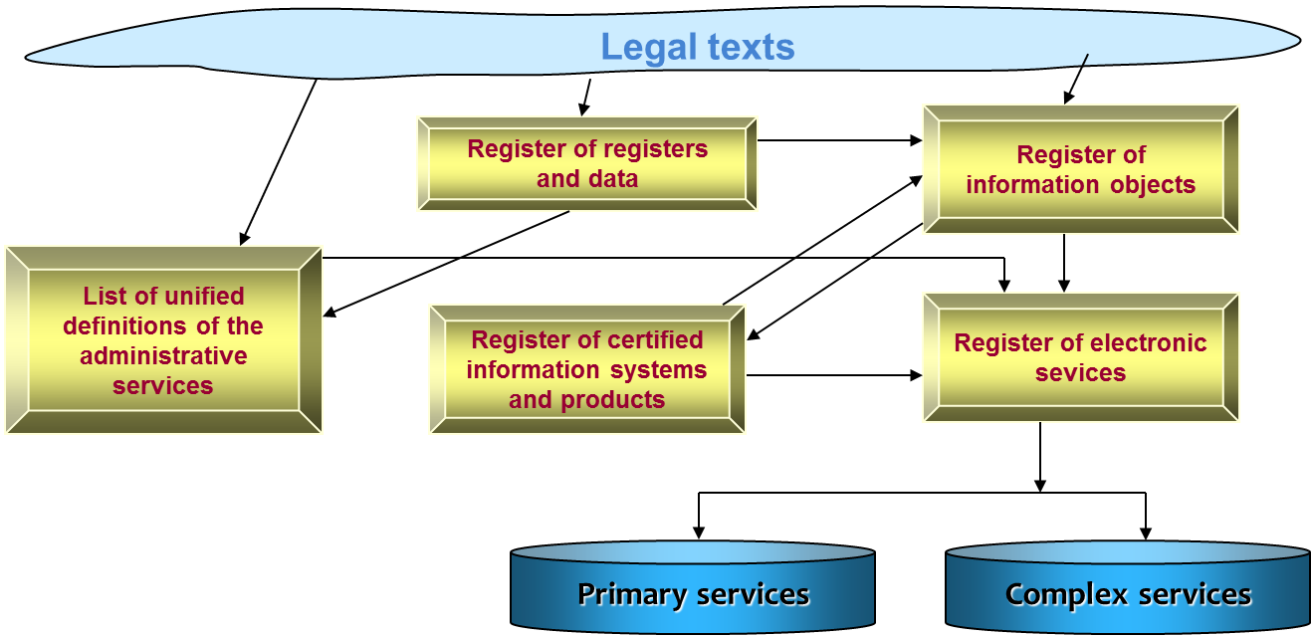


Figure 3-28

Structure of the data model 6

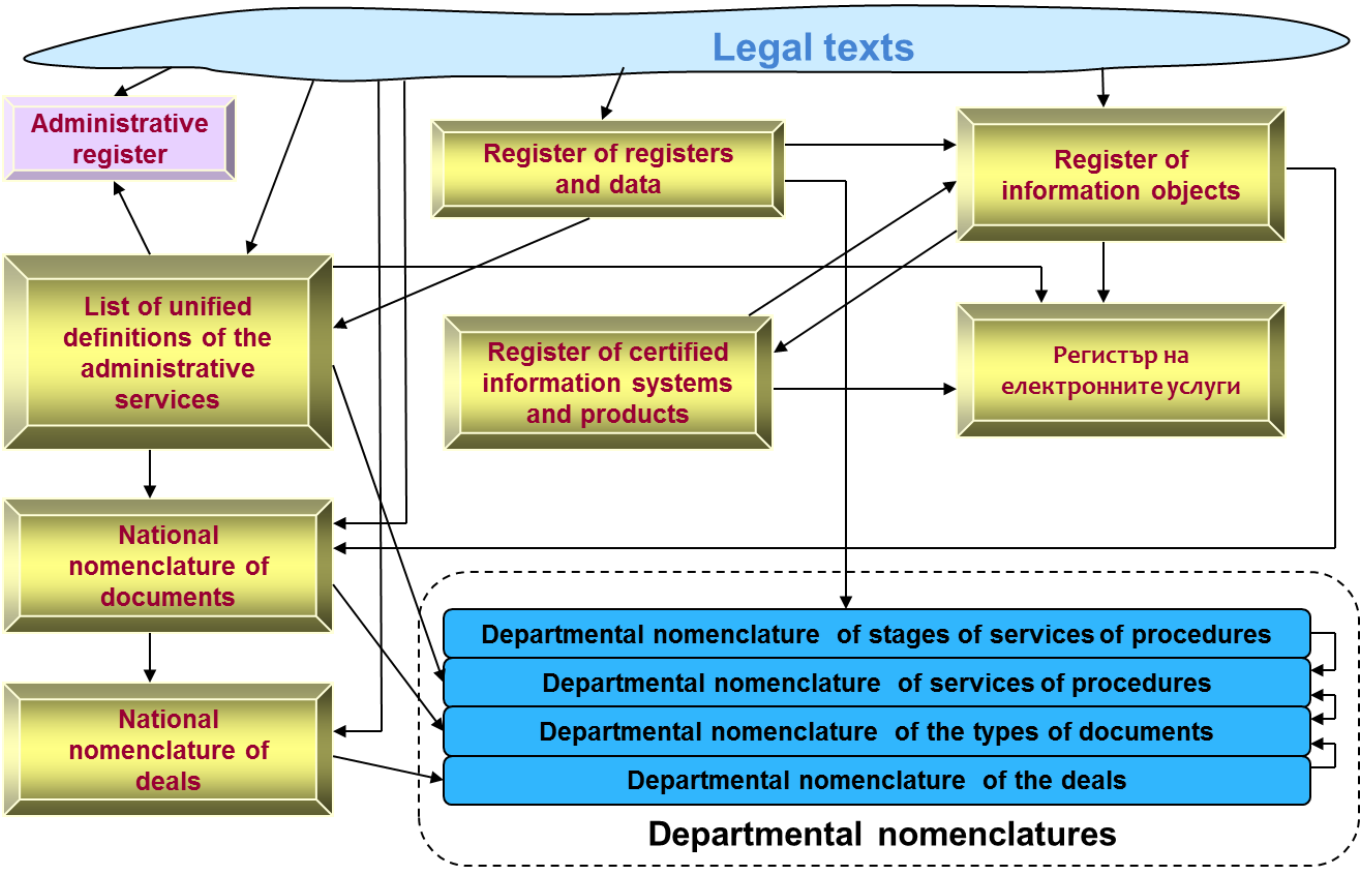


Figure 3-29

The Register of information objects

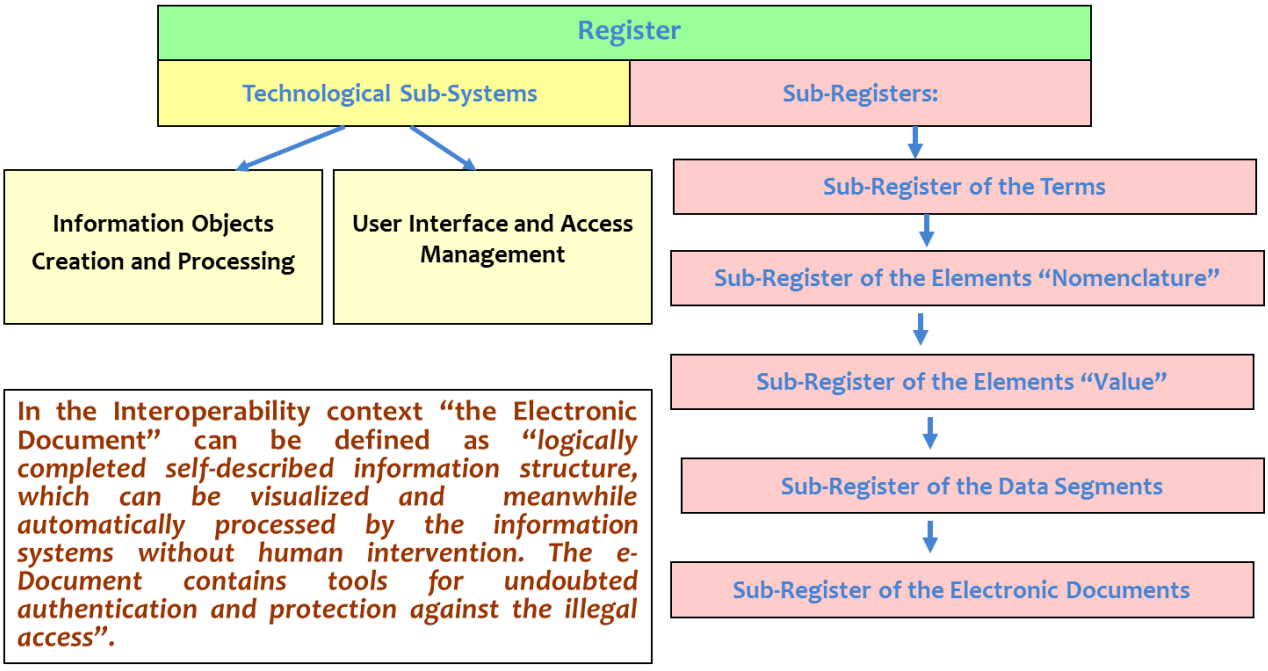


Figure 3-30

The Register of the information objects is a data base, managed by an information system and containing formalized technological descriptions of the information objects collected, created, stored and processed by the administrative bodies within the framework of their competence.

The information objects shall be:

1. “term” - a notion, which is interpreted unequivocally by all participants in the administrative process;

2. “nomenclature” – a final list of thematically related terms, entered into the Register;

3. “value” – constitutes a quantity and is described by a final number of meanings, determined by formal restrictions;

4. “segment” – a structure made up of terms, nomenclatures, values and/or other segments, already entered into the Register;

5. “document” – a segment for which a program application is ensured, enabling full, precise and true visualization of the data contained.

The content of the information entered for different information objects is almost similar. As an example - the circumstances concerning an information object of the “segment” type, subject to entry into the “Segments” section shall be:

1. name of an information object - the full name of the information object of the “segment” type shall be entered, whereby the object is unambiguously individualized; the name shall be unique;

2. purpose of an information object - a brief text explanation of an information object of the “segment” type shall be entered;

3. unique register data identifier - unique register identifier of the entered into the “Unified data” section of the Register of the registers and the data of a unified definition of data, corresponding to an information object of the “segment” type;

4. status of an information object - an indication shall be entered concerning the possibility to use the object in regulations, including in the definitions of other information objects; the possible values shall be “usable” or “unusable”;

5. Internet site for access to an information object - the electronic address (URL) of the Internet site shall be entered, from which access to the content of the segment batch is taking place;

6. instructions on the handling of an information object - entered in free text or in computer-executable descriptions, which unify the creation of procedures for revising, visualization and other types of processing, related to the information object;

7. XML definition of a segment – the object structure shall be entered – a definition in XML format with a name, which is unique for the Register of the information objects, containing other information objects of the “term”, “nomenclature”, “value” or “segment” types, which have already been entered into the Register of the information objects;

8. instructions on checking the validity of the segment - rules shall be entered for checking the validity of the segment content in formalized type according to a standard, entered into the Register of the Standards or by way of exception in free text;

9. nomenclature of the errors - a set of errors, defined under point 8, shall be entered and in accordance with their entry as terms in the “Terms” section.

The information object under may be entered into the Register only if an entry exists in connection with it in the "Unified data" section of the Register of the registers and the data. In this case the circumstances shall be entered with content, similar to that entered into the Register of the registers and the data.

To the content of each entered circumstance shall be maintained a description, containing:

1. the entry number – an automatically generated serial number of entry in regard to a circumstance in the batch content shall be entered;

2. unique register identifier of a circumstance - a unique register identifier of the type of the circumstance/the data shall be entered into the "Types of circumstances" section or the "Unified data" section of the Register of the registers and the data;

3. content of the circumstance – the data shall be entered, forming the content of the circumstance, subject to entry;

4. unique register identifier of the application for entry – the unique register identifier of the application shall be entered, whereby the entry had been applied;

5. applicant of the entry - the name, BULSTAT code, respectively UIC Code, e-mail address and telephone exchange of the administrative body, having applied for the entry, respectively – of the individual under Article 14(2) shall be entered;

6. time of entry – automatically generated data for the time of the performed entry into the register shall be entered;

7. employee, having performed the entry – data shall be entered automatically, identifying through the information system, maintaining the register, employee who performed the entry into the register.

One example – information object "segment"

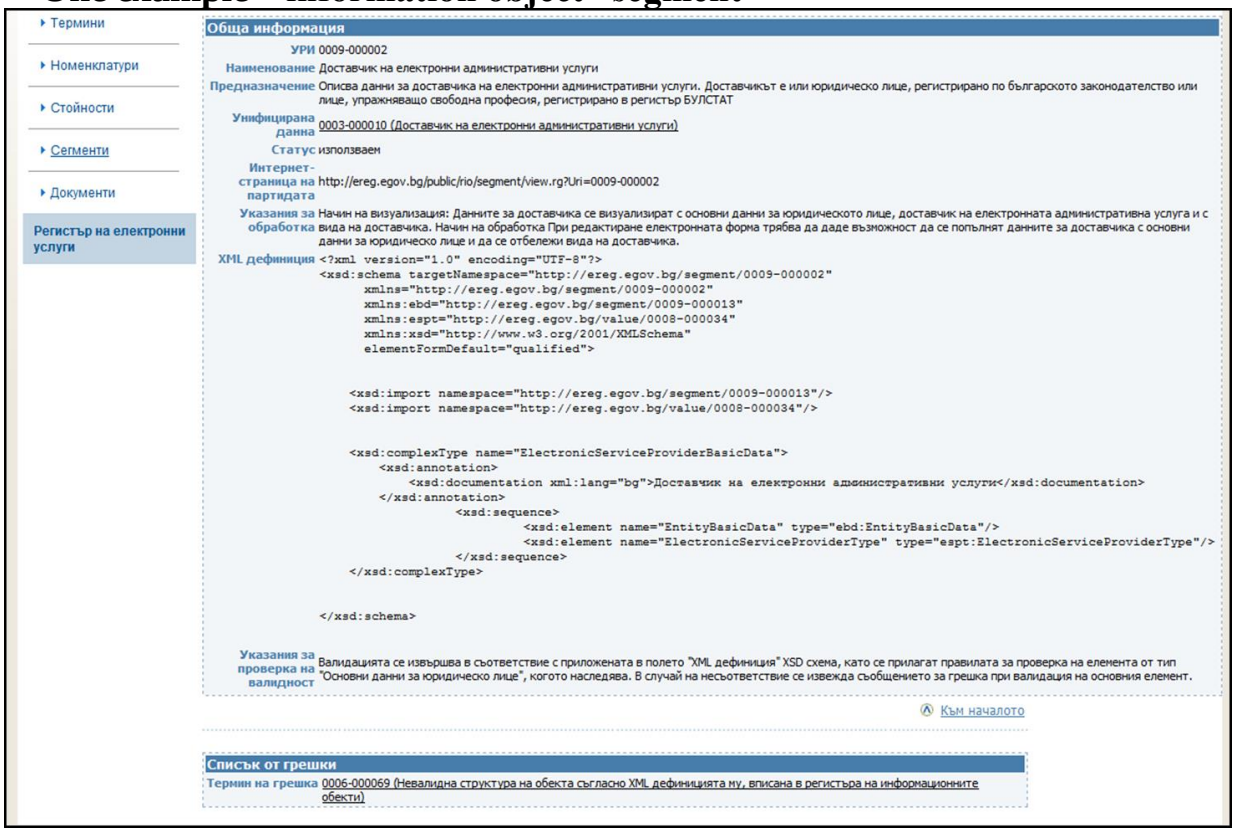


Figure 3-31

The Register of electronic services

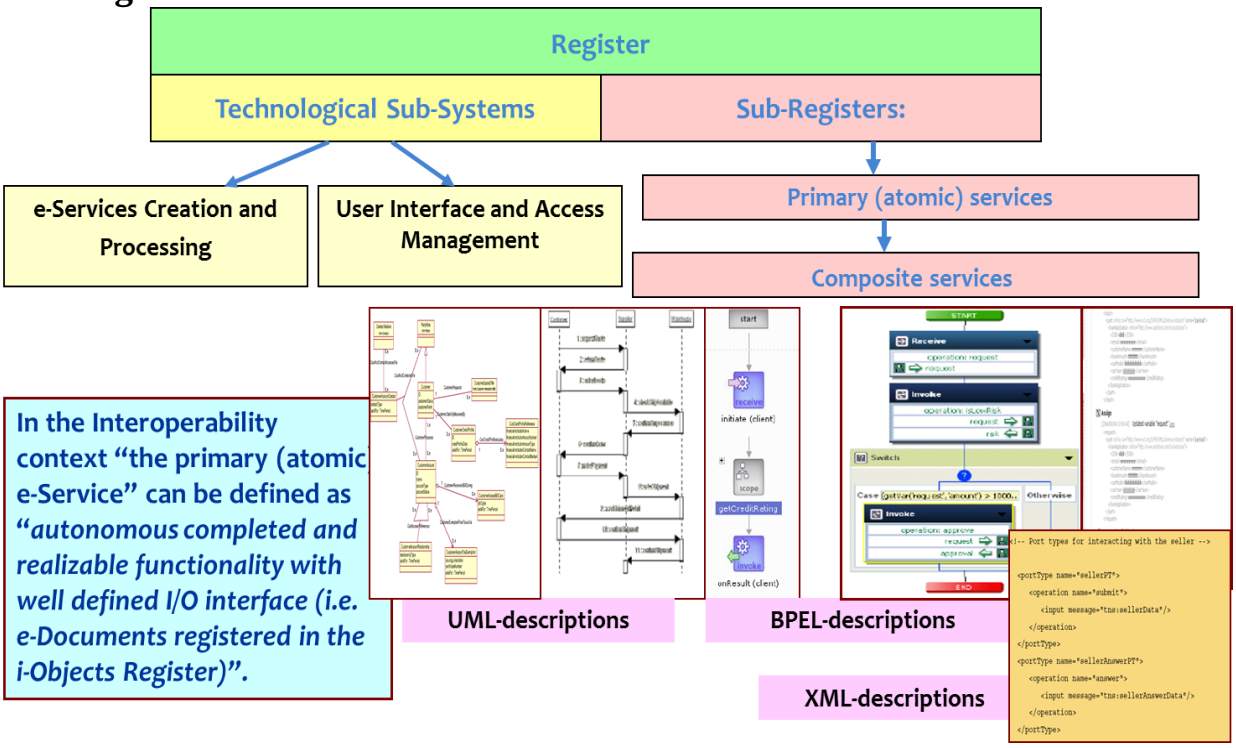


Figure 3-32

The Register of the electronic services is a data base, managed by an information system and containing formalized technological descriptions of the electronic administrative services and of the internal electronic administrative services, provided through the uniform document exchange environment.

Electronic services within the meaning of the Ordinance shall be the electronic administrative services and the internal electronic administrative services.

The following types of electronic services shall be entered in the Register of the electronic services:

1. primary services, which are performed within the framework of a single administration, differentiated in geographical or functional terms, as a single process, starting from application for the service and ending by provision of the service or statement of refusal;

2. complex services, which are performed as a process, where the access to data, maintained by the administrations, shall take place by using primary or other complex services.

The circumstances concerning an electronic service of the "primary service" type, subject to entry into the "Primary services" section of the Register of the electronic services, shall be:

1. name of the electronic service – the full name of the primary electronic service shall be entered, whereby it is unambiguously individualized; the name shall be unique for services with "usable" status;

2. purpose of the electronic service – a brief text explanation of the purpose of the electronic service shall be entered;

3. status of the electronic service – indication shall be entered concerning the opportunity for the primary electronic service to be provided by the administrative bodies, by the organizations, providing public services and by the individuals, discharging public functions and

to be used in regulations, including in the definitions of complex electronic services; the possible values are “usable” or “unusable”;

4. Internet site for access to the electronic service batch - the electronic address (URL) of the Internet site shall be entered, from which access to the content of the batch of the primary electronic service is taking place;

5. unique register identifier of administrative service – the unique register identifier shall be entered, issued upon entry of the administrative service, which corresponds to the electronic service in the list of unified names of the administrative services, kept in accordance with the Ordinance under Article 5a, paragraph 1 of the Law on Administration; this fact shall be entered, where the electronic service is provided by administrations;

6. unique register identifier of application - the unique register identifier shall be entered, under which the segment, whereby the data in the application for the electronic service is presented, is registered in the Register of the information objects;

7. unique register identifier of reviser - the unique register identifier shall be entered, under which an application is registered in the lists of certified information systems, enabling full, precise and true revising of the content of the data in the application for the electronic service;

8. list of unique register identifier of responses – a list of unique register identifiers shall be entered, under which the documents, whereby the data is provided in response to an applied electronic service, are registered in the Register of the information objects, and where the result of the service provision is an administrative act, manifested in an act of entry into a public register, the unique register identifier of the register shall be entered;

9. unique register identifier of refusal – the unique register identifier shall be entered, under which the document, whereby provision of the electronic service was refused, had been registered in the Register of the information objects;

10. list of providers - a list shall be entered of data on the administrative bodies, the organizations, providing public services and of the individuals, discharging public functions, who provide the electronic service;

11. list of recipients of internal electronic administrative service - a list of data shall be entered for the administrative bodies, the organizations, providing public services and of the individuals, discharging public functions, who by virtue of regulation are entitled to access to the data, provided by the internal electronic administrative service and the conditions, under which they may obtain it.

The electronic service, when it is provided by an administrative body, may be entered into the Register only if an entry exists in regard to it as an administrative service in the list of unified names of the administrative services

3.3.3
UNIFORM ENVIRONMENT FOR E-DOCUMENTS EXCHANGE

Nature of UEEDE

The Electronic Control provides all internal administrative services to be provided by mandatory single environment for the exchange of electronic documents.

UEEDE shall be constructed and maintained by the Minister of Transport, Information Technology and Communications in accordance with the Ordinance on the requirements for integrated environment for exchange of electronic documents adopted by the Council of Ministers Decree № of and promulgated in the State Gazette number.

The Uniform Environment for Exchange of Electronic Documents (UEEDE) is manageable environment for standardized exchange of documents, entered in the Register of the Information Objects, among the information systems in the administration for the purposes of the e-Governance.

The compliance between application and answer in an electronic service, ensured by the entry of the service in the Register of the Electronic Services, shall not be subject to inspection by the UEEDE.

The exchange of unstructured documents through UEEDE shall be performed through their inclusion in the content of electronic documents, registered in the Register of the Information Objects.

No processing of the content of the transmitted electronic documents shall be performed in UEEDE.

The exchange of electronic documents among the information systems of the participants in the exchange through UEEDE shall be performed through a Communication Server.

The connection between the information systems of the participants in the exchange and the Communication Server shall be realized through a specialized program application for connection (Communication Client).

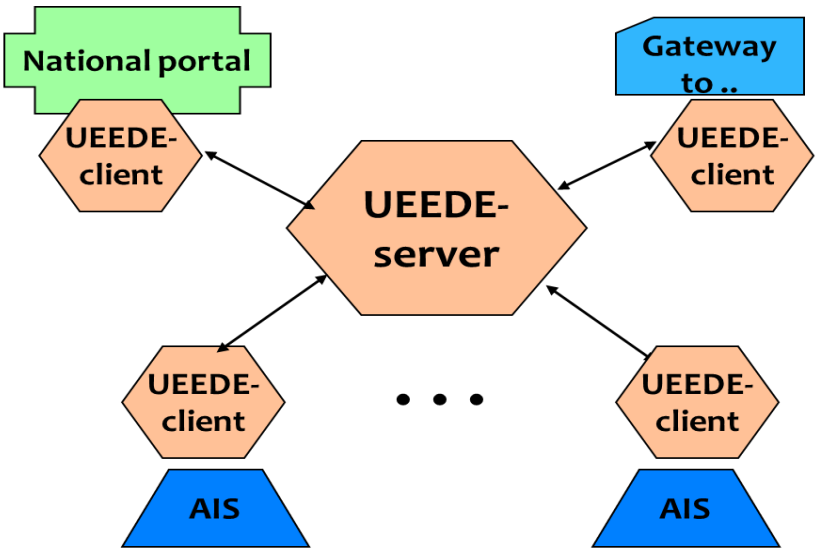


Figure 3-33

The registration of participants includes:

1. Data identifying the administration

2. Name of participant

3. IP-address

4. Unified registry identifier (URI) of the registration

5. Digital certificate

6. Other data

The addressing in the ESOED forms three levels:

- the level "release" - via IP;

- the level "transfer of document" – via URI of the registration of participants;

- the level “service or procedure” – via URI of the registration of the application document.

The document exchange is protected by encryption / decryption procedure through asymmetric public key cryptography using digital certificates of the UEEDE - server and UEEDE -clients. These transport certificates will be issued by the internal public key infrastructure for all administrations, maintained by the Minister of Public Administration and Administrative Reform.

The transfer protocol is based on the German standard “OSCI Transport” recognized informally for now as pan-European one.

Transfer of documents

The transfer of an electronic document between two participants in the exchange shall be performed through the Communication Server, within the framework of a single procedure of document exchange under the following conditions:

1. one exchange procedure shall transfer only one electronic document;

2. the document under may consist of and contain an unlimited number of other electronic documents, including unstructured documents.

A single information system may start several parallel exchange procedures.

Every document exchange procedure has two sessions as follows:

1. exchange session where the Communication Client of the sending participant sends a communication to the Communication Server;

2. exchange session where the Communication Server sends a communication to the Communication Client of the receiving participant.

The communications under contain the document to be transferred and they are part of the protocol specification.

The communications are created as types of electronic documents and are registered in the Register of the Information Objects.

The session under point 1 shall be terminated after return of communication on end of session from the Communication Server to the Communication Client of the sending participant.

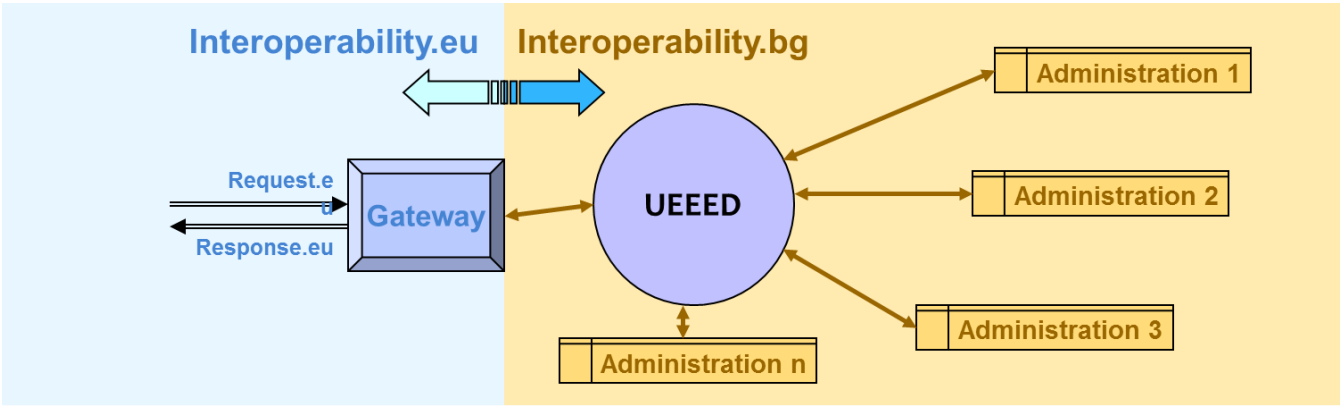
The session under point 2 shall be terminated after return of communication on end of session from the Communication Client of the receiving participant to the Communication Server.

The sessions have the maximum permissible time of realization indicated in the protocol specification.

Administration "A"		UEEDE	Administration "B"	
AIS: Service procedure "A"	UEEDE Client "A"	UEEDE Server	UEEDE Client "B"	AIS: Service procedure "B"

Figure 3-34

Cross-border services



A specialized Gateway will connect Bulgarian environment of administrative services with European. The Gateway will support:

- Protocol compatibility with eu-requirements
- Translation from eu-service specification to bg-service specification and vice versa
- Control of execution of services, including complex type, in Bulgarian environment of administrative services

Figure 3-35

Fulfilment of complex services

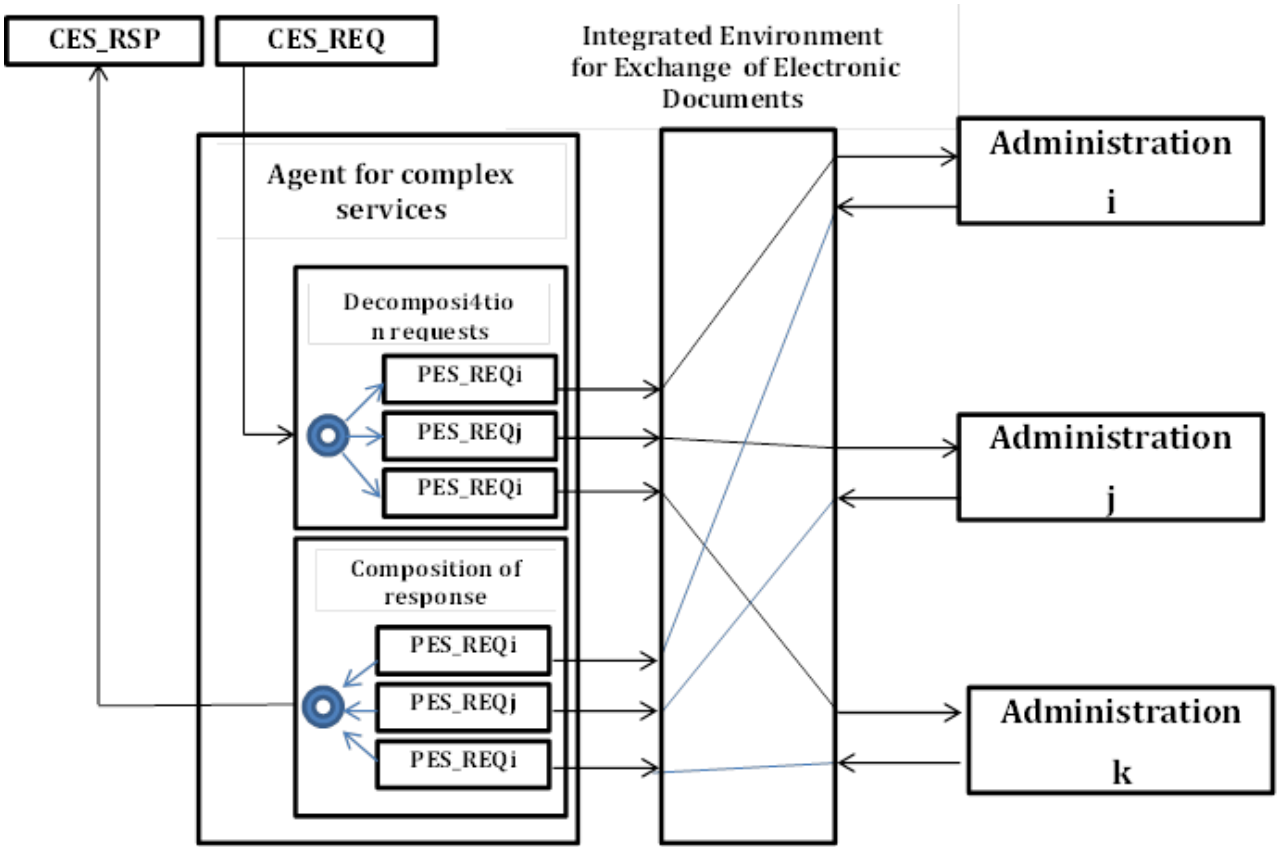


Figure 3-36

Decomposition of orders

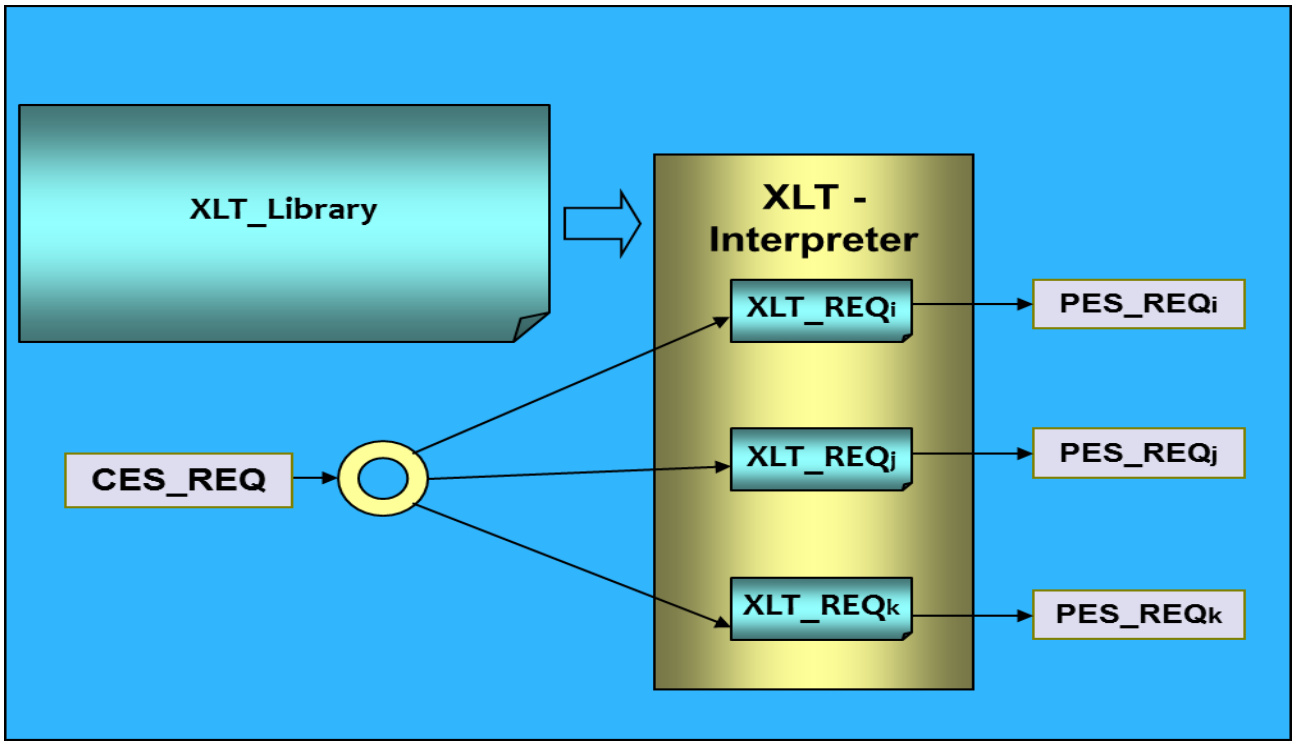


Figure 3-37

Decomposition of answers

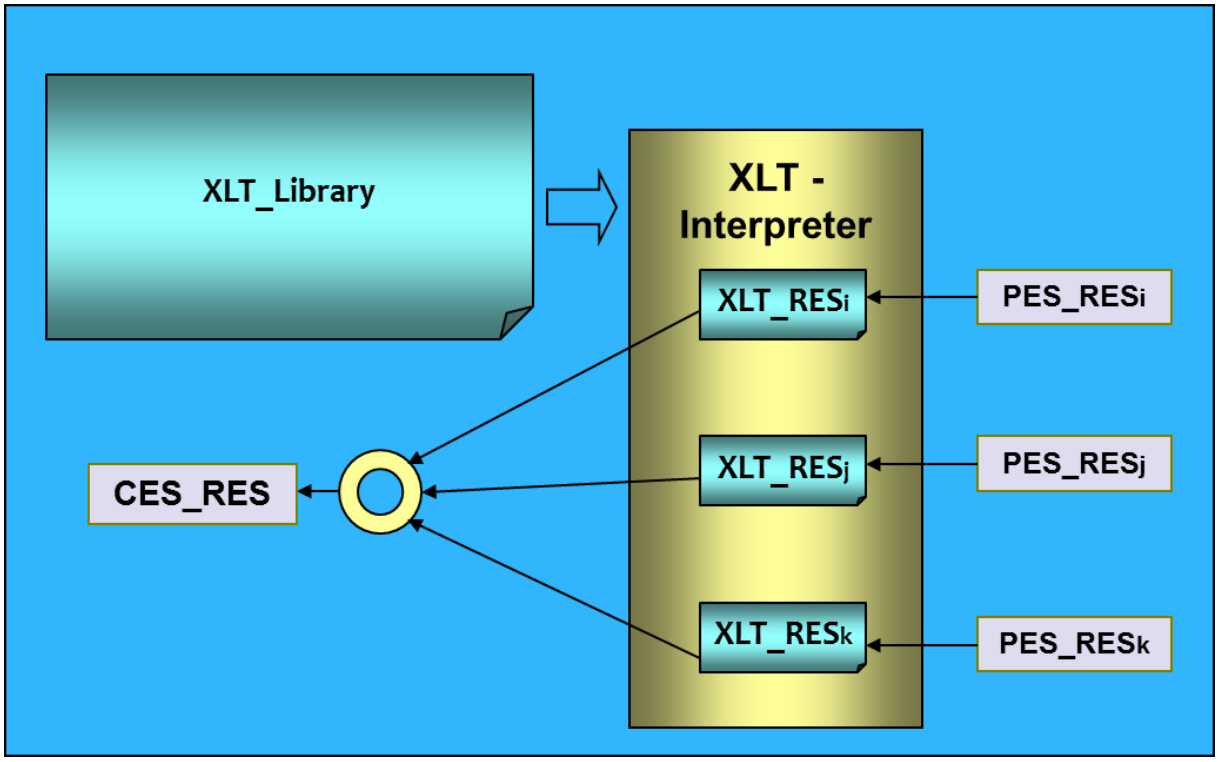


Figure 3-38

Complex service management

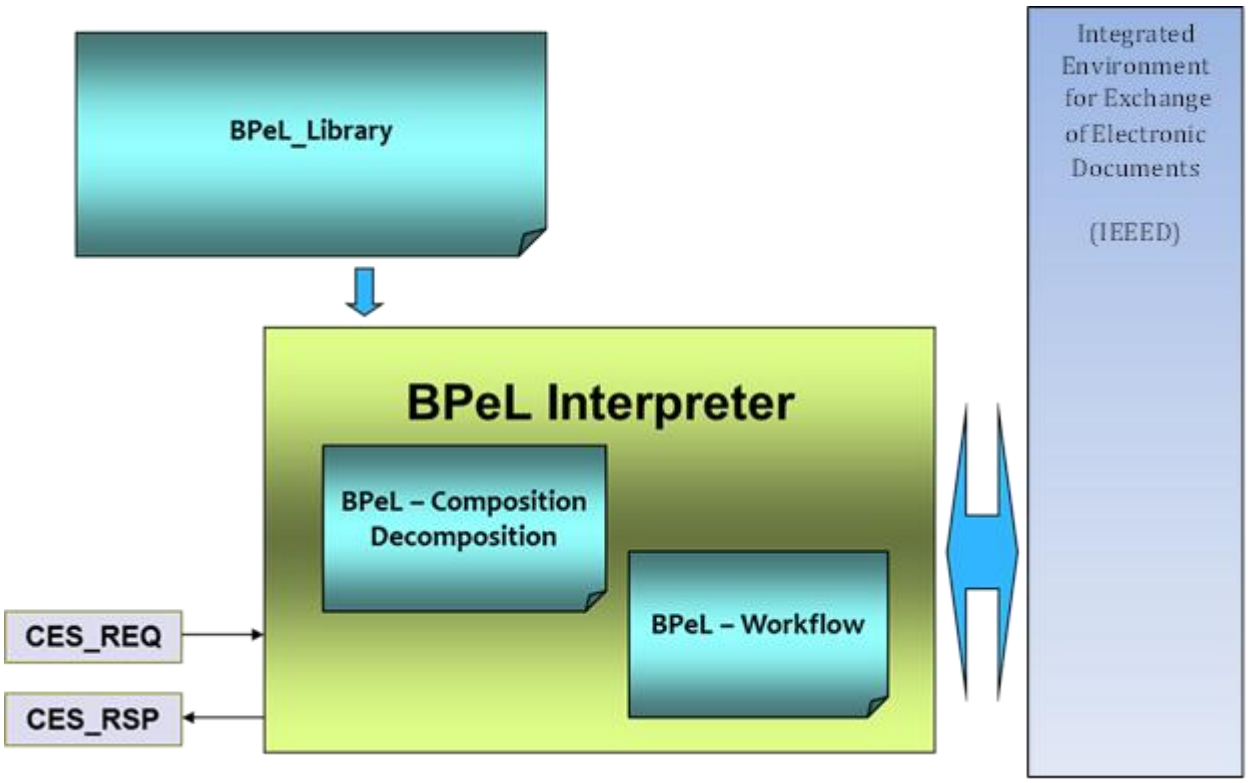


Figure 3-39

3.3.4
THE ADMINISTRATIVE INFORMATION SYSTEM AS A CORE SYSTEM

The nature of AIS

The Law on e-Governance and its regulations (primarily, the Ordinance on the internal flow of electronic documents and paper documents in administrations) define the administrative information system (AIS) as the main system in the administrative unit - a major factor in achieving interoperability and information security of the entire IT infrastructure of the administration.

AIS provides maintenance and processing of data referring to the movement of electronic documents and paper documents in the provision of administrative services and implementation of administrative procedures. Procedures are all working processes in the administration or between different administrations, including internal turnover of documents which do not constitute the provision of administrative services and internal administrative services,

The functional scheme of the functions of the administrative unit, covered by information systems, shows the integrative or central position of Administrative Information System (AIS) and its interfaces with the "external environment" and other systems of the administration. These interfaces are implemented by specialized applications integrated into AIS:

a) liaison with external sources of information:

- integrated Web-application;
- module for integration with Communication Client (CC) of the Unified Environment for Electronic Documents Exchange (UEEDE);
- module for e-mail;
- module for input of information stored on magnetic or other external media.

All these modules interact with integrated AIS application for validation.

b) interface modules for interconnection with other systems of the administrative unit – the e-Governance Act don’t provide for this any specific regulations. In order to ensure unification, it is recommended to organize this exchange through XML-messages without restrictions to their content.

The e-Governance Act requires that AIS has to be certified, i.e. it must pass specific procedure for assessment of conformity with the requirements for interoperability and information security.

Furthermore, AIS must meet the following requirements that are not included in the formal conformity assessment:

1. AIS shall maintain one or more official documentary registers that are entered in the Register of registers and data;

2. AIS shall maintain the following types of information objects:

• user;• task; • document; • individual; • entity , etc.

3. AIS should support the following departmental nomenclature :

• of the types of documents;

• of services and procedures;

• of unified stages of services or procedures

4 . AIS shall maintain the status of implementation of each service or procedure, enabling applicants to check the status of the services they have ordered.

5 . AIS should provide connectivity to the average for the Unified Environment for Electronic Documents Exchange (UEEDE);

6 . AIS should provide an integrated application for validation of signed electronic documents in accordance with the protocol XAdES (XML Advanced Electronic Signature), outlined in the recommendation of ETSI (European Telecommunication Standardization Institute) TS 101 903

The Refference Model of AIS

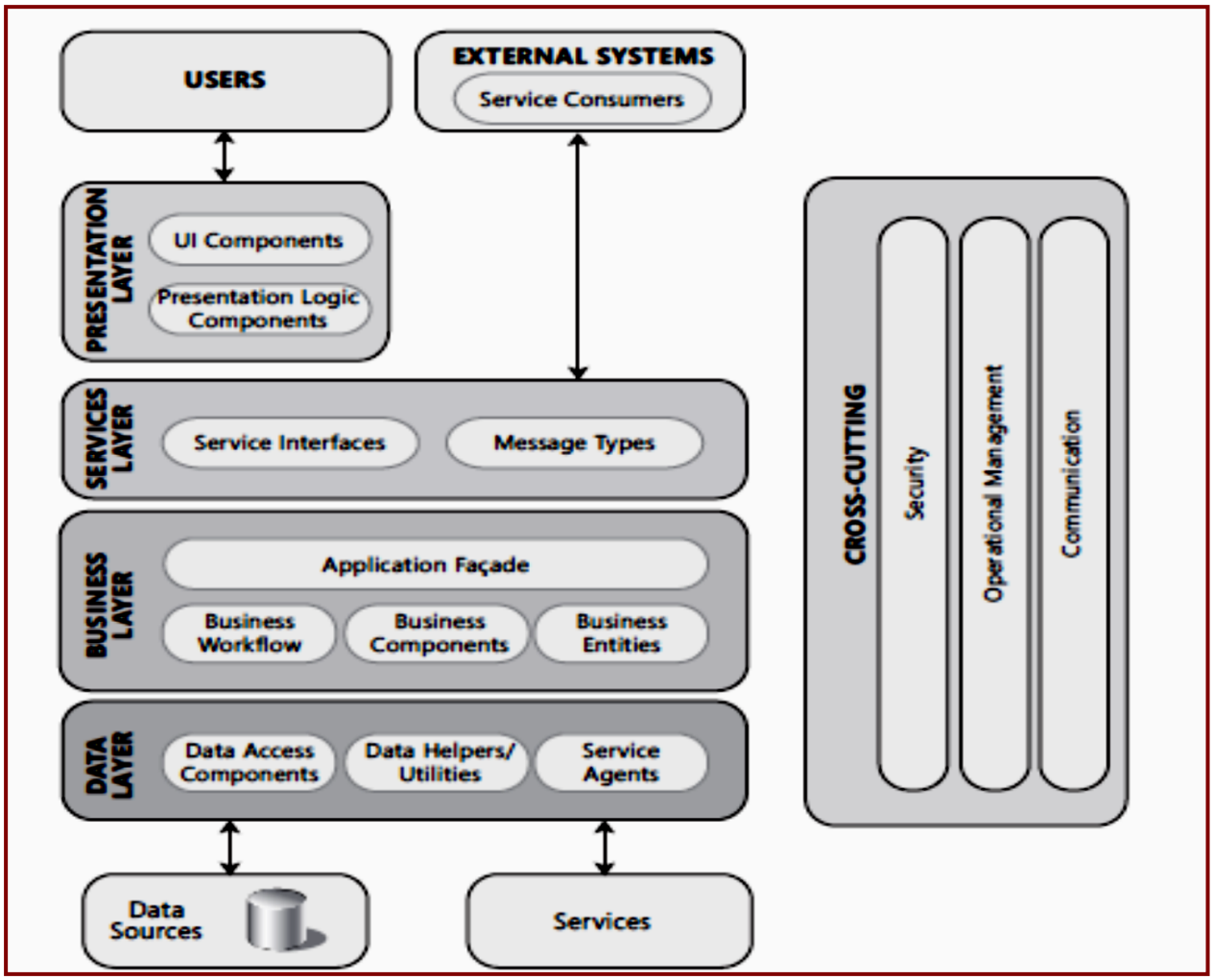


Figure 3-40

The core position of AIS

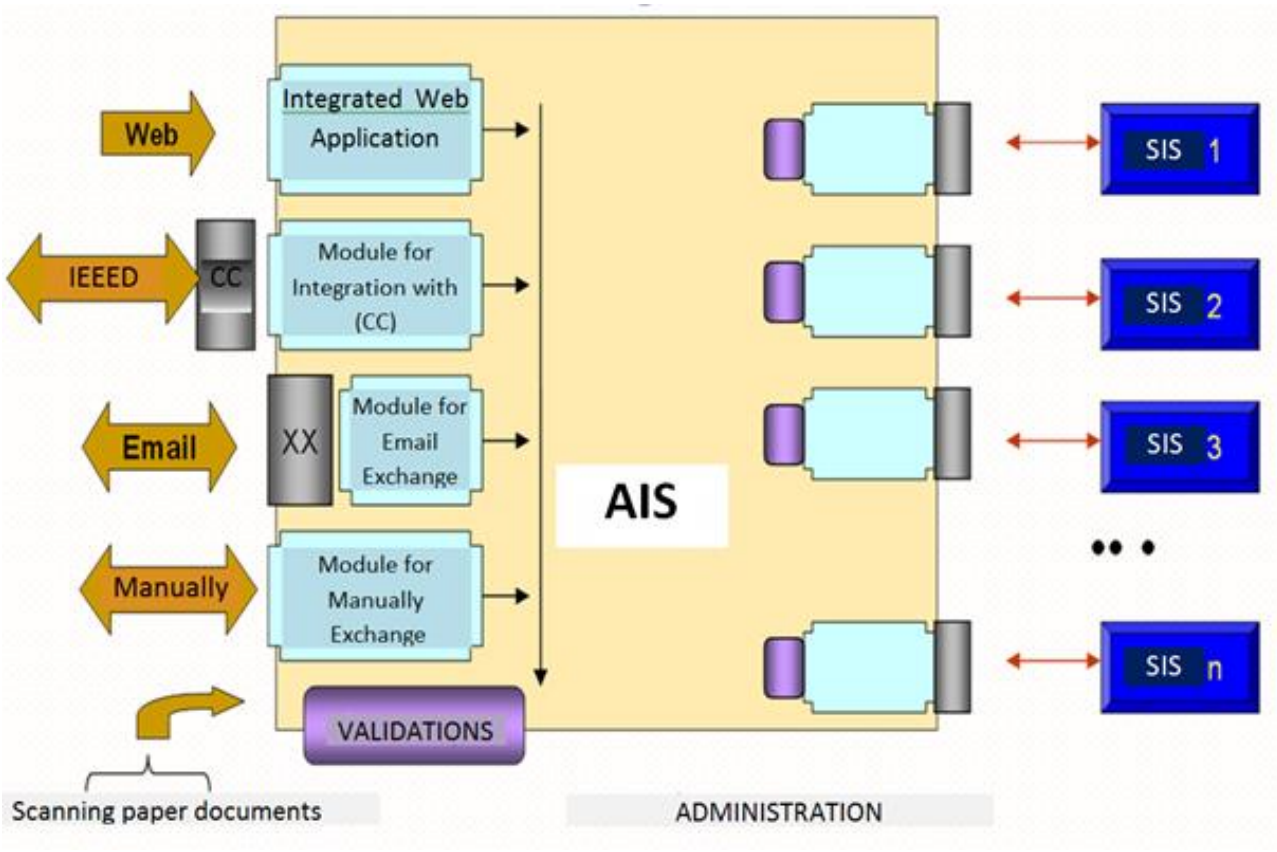


Figure 3-41

The documents induce starting of determinate procedures

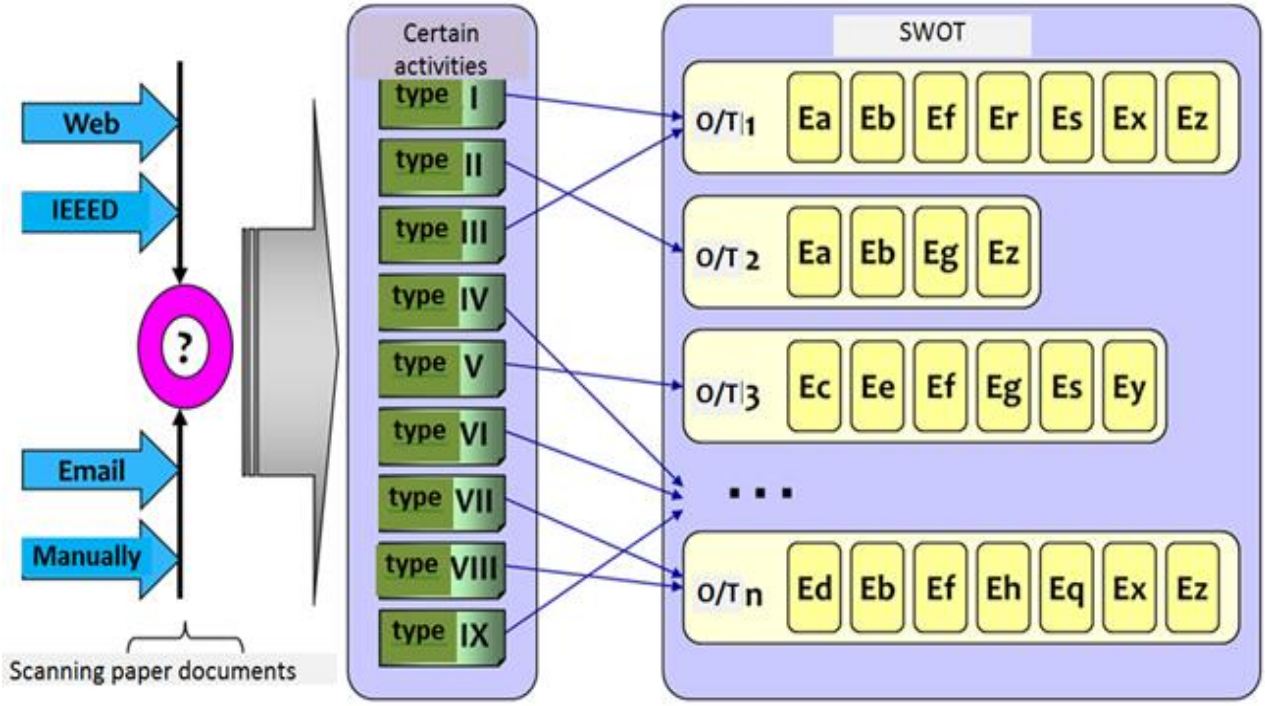


Figure 3-42

Web application for documents receipt

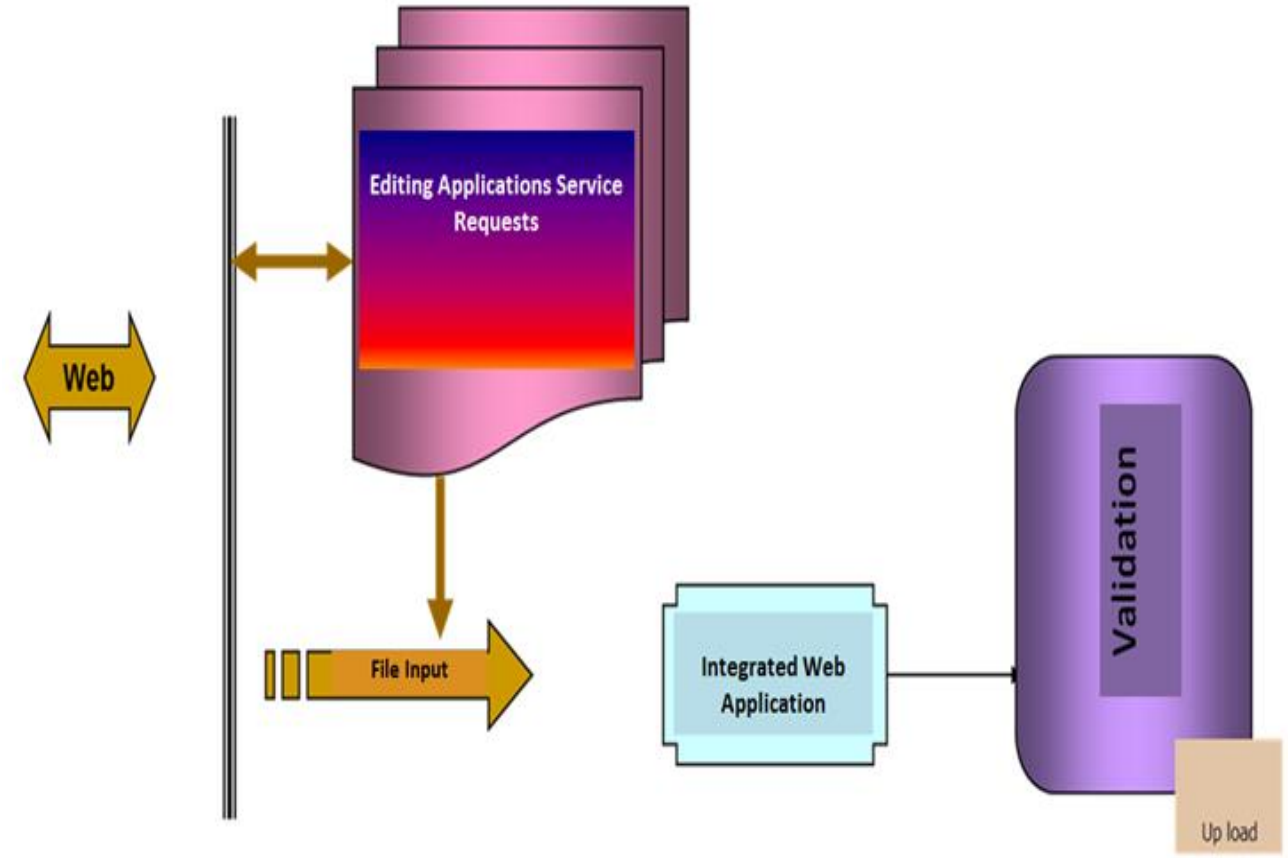


Figure 3-43

Model of the status of procedure

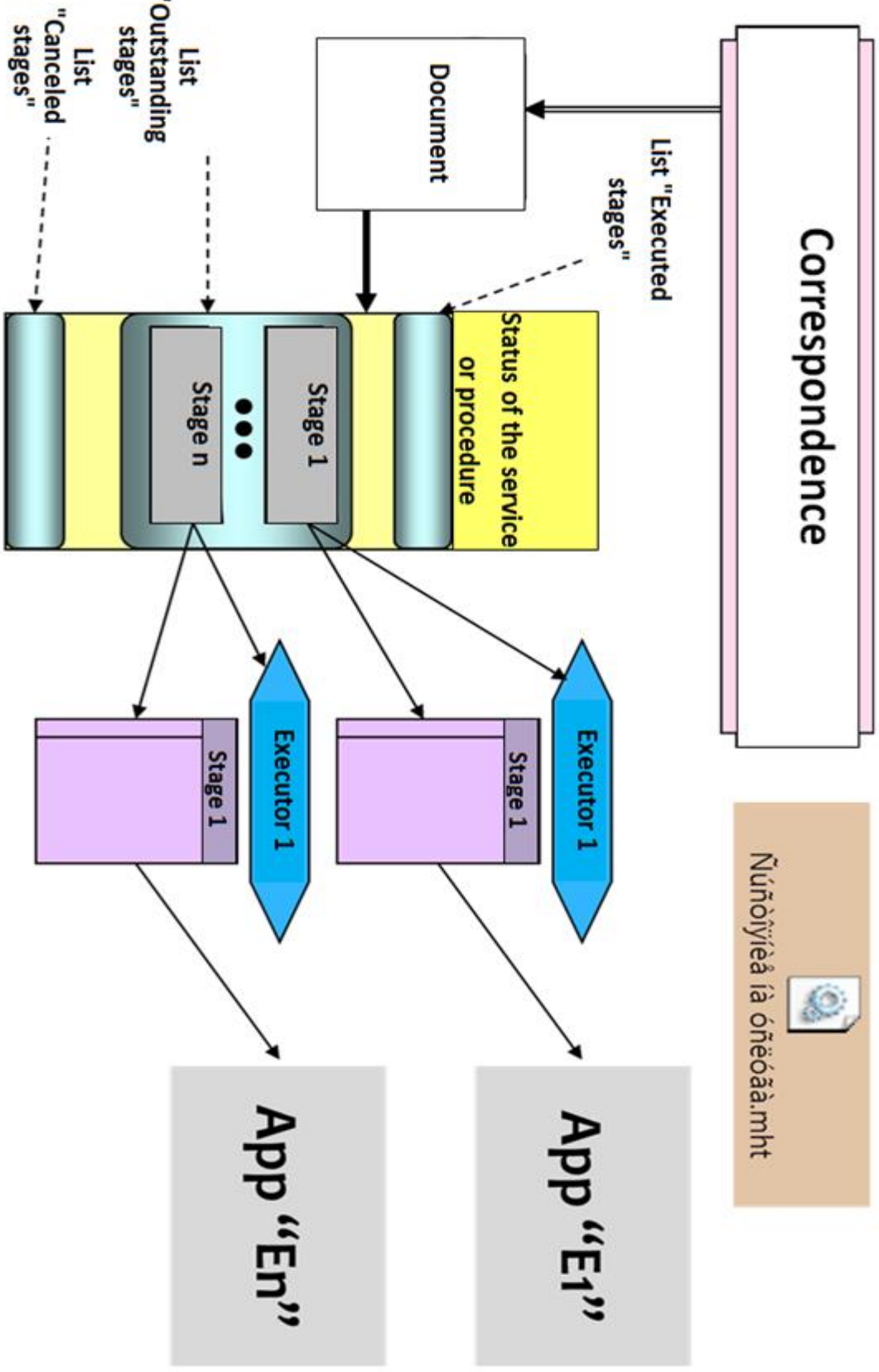


Figure 3-44[3]

[3] STATE AGENCY FOR INFORMATION TECHNOLOGY AND COMMUNICATIONS

State agency for information technology and communication. **Figure 3-45**

The technological process of the re-engineering of the AIS consists of the following sequence of actions:

1. analysis of the type and quantity of indispensable Document Registers; registration of these registers in the Register of registers and data; adjustment of AIS for processing these registers;

2. establishment and maintenance into AIS of Classification schemes for following types of information objects:

a) users; b) documents; c) tasks; d) personal data; e) nomenclatures.

3. establishment of Departmental nomenclature of types of documents for concrete administration; adjustment of AIS for processing this nomenclature;

4. establishment of Departmental nomenclature of stages of services and procedures for concrete administration; adjustment of AIS for processing this nomenclature;

5. establishment of Departmental Nomenclature of Services and Procedures for concrete administration; adjustment of AIS for processing this nomenclature;

6. establishment of Departmental nomenclature of schemes for storage of documents for concrete administration; adjustment of AIS for processing this nomenclature;

7. creation of Interfaces between AIS and "external environment" by specialized applications, integrated into the AIS, such as:

a) module for Web-application; b) module for integration with the Communication Client of the UEEDE; c) module for e-Mail exchange; d) module for reception of documents stored on magnetic of other external media

8. interface modules for connection with other specific system of this administration – the regulations of the e-Governance Law do not prescribe any special requirements for these connections. The administration has an alternative between direct communication (i.e. the method of components call) and communication based on messages. The advantages of the second one are related to the ability to separate components from one another;

9. establishment of internal rules for working with the AIS adapted to the specifics of the particular administration. Creation of profiles for access of various groups of employees to the resources of the AIS. The profiles correspond to the duties of employees included in their job description.

3.3.5
COMPLIANCE VERIFICATION

According to the e-Governance Law, the administrative bodies shall use information systems, which have been certified for compliance with the requirements of the Law for interoperability. When organizing public procurement for introduction of information systems, the administrative bodies shall include mandatory requirement that these systems must be certified for interoperability.

The compliance of the information systems implemented by the administrations with the requirements for interoperability is certified by persons who are accredited by respective accreditation authority. The accreditation is done while observing the principles of rule of law, independence, impartiality, publicity and equality. The persons accredited along this procedure are enlisted in a public list of the accredited persons. The period of validity of the accreditation is 3 years.

The certification shall be made while observing the principles of lawfulness, independence, impartiality, publicity and equality. The information systems and the program applications certified using the procedure of the Ordinance shall be entered into a public list of the certified information systems and products.

Subject to certification for compliance with the interoperability requirements shall be:

1. Specifications for:

- development or acquisition of an administrative information system;

- building of direct connectivity between the information systems;

2. Information system which:

- has a functionality to ensure the maintenance and data processing concerning the circulation of electronic documents and documents in hard-copy form when delivering administrative services and performing administrative procedures;

- is a new version of an information system which has been already certified;

3. Program applications that:

- perform functions for visualization and/or editing of electronic documents;

- in composition of other applications or systems perform functions for verification of electronic documents for conformity with their registration in the Register of the information objects.

In the lists of the accredited persons and of the certified systems and products, circumstances about the persons accredited for certification of information systems, respectively about the certified information systems and products shall be entered.

The lists are data bases managed by an information system containing the descriptions of the composition and the organization of the data.

History of the entries shall be kept in the lists.

The following types of objects shall be entered into the list of the certified information systems:

1. objects of the type “certified system”;

2. objects of the type “certified application”;

3. objects of the type “certified specification”;

4. objects of the type “test set of documents”.

The following circumstances for objects of the type “certified systems” shall be entered into the section “Certified systems” from the list of the certified systems:

1. data identifying the certified system such as model, version, configuration, etc;

2. data identifying the interested person;

3. data for the accredited person who has made the certification;

4. scope of certification including the types of electronic documents which are maintained by the system;

5. number and date of the issued certificate.

List of accredited persons and a list of certified systems and products. **Figure 3-46**

REFERENCES

1. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions “Towards interoperability for European public services”, COM(2010) 744 final, 16.12.2010, Brussels, Belgium Annex 1 “European Interoperability Strategy for European public services”

2. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions “Towards interoperability for European public services”, COM(2010) 744 final, 16.12.2010, Brussels, Belgium Annex 2 ”European Interoperability Framework for European Public Services”

3. Directive 2003/98/EC on the re-use of public sector information, 17.11.2003

4. “The Role of e-Government for Europe's Future”, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions, COM(2003) 567

5. ISO/IEC 2382-01, Information Technology, Vocabulary, Fundamental Terms

6. IEEE Standard Computer Dictionary: A Compilation of IEEE Standard Computer Glossaries. New York, NY, 1990

7. Report on "Key Principles of an Interoperability Architecture", 24.06.2004, Irish Presidency of the European Public Administration Network e-Government Working Group

8. Decision 2004/387/EC on interoperable delivery of pan-European eGovernment services to public administrations, businesses and citizens (IDABC), 21.04.2004

9. The European e-Government Action Plan 2011-2015 "Harnessing ICT to promote smart, sustainable & innovative Government", COM(2010) 743, 15.12.2010, Brussels, Belgium

10. MODINIS Programme: follow-up of e-Europe 2005 action plan”, available at http://ec.europa.eu/information_society/eeurope/i2010/ archive/modinis/index_en.htm “D2.7 Study on Interoperability at Local and Regional Level. Final Version”, 20.04.2007

11. “European Interoperability Framework for Pan-European eGovernment Services”, IDA working document, Version 4.2, 01.2004

12. “Proposal for a Decision of the European Parliament and of the Council on interoperability solutions for European public administrations (ISA)”, COM(2008) 583, 29.09.2008, Brussels, Belgium

13. “Final evaluation of the implementation of the IDABC programme”, Communication from the Commission to the European Parliament and the Council, COM(2009) 247, 29.05.2009, Brussels, Belgium

14. „ISA: Community Programme on interoperability solutions for European public administrations”, available at http://ec.europa.eu/idabc/servlets/Doc6ffa.pdf?id=31770

15. “ISA Work Programme - First revision”, 2011

16. “eTEN: Trans-European e-Services”, available at http://ec.europa.eu/information_society/activities/egovernment/implementation/eten/index_en.htm

17. “ICT Policy Support Programme”, available at http://ec.europa.eu/information_society/activities/egovernment/implementation/ict_psp/index_en.htm

18. e-CODEX project, available at www.e-codex.eu

19. epSOS project, available at www.epsos.eu

20. PEPPOL project, available at www.peppol.eu

21. SPOCS project, available at www.eu-spocs.eu

22. STORK project, available at https://www.eid-stork.eu/

23. Ralf Klischewski Contextual Strategies towards Interoperability in e-Government Journal of Theoretical and Applied Electronic Commerce Research, ISSN 0718–1876 Electronic Version, VOL 6 / ISSUE 1 / APRIL 2011 / 26-42 © 2011 Universidad de Talca - Chile

24. W.E. Moen, Interim Report for the Z-Interop Project The Z39.50 Interoperability Testbed, School of Library and Information Sciences Texas Center for Digital Knowledge University of North Texas Denton, TX 76203

25. “European Interoperability Framework (EIF) – Towards Interoperability for European Public Services“, Brochure accompanying the European Interoperability Framework communication, 2011

26. "European Interoperability Architecture: Phase 2 – Final Report: Common Vision for an EIA", v.2.0, 11.2011

27. “Architecture Guidelines for Trans-European Telematics Networks for Administrations”, Version 7.1, IDA programme, 09.2004

28. Report "European Interoperable Infrastructure Services: Study on potential reuse of system components", v.1.1, 2009

29. Bollinger T., A Guide to Understanding Emerging Interoperability Technologies, MITRE, Washington 2000

30. Kantor, M.; Burrows J. H.,. "Electronic Data Interchange (EDI)". National Institute of Standards and Technology. Retrieved 2012-08-13

31. EICTA white paper on Interoperability, http://www.eicta.org/files/WhitePaper-103753A.pdf. Recommendations to governments and industry on ensuring interoperability by EICTA, the voice of the ICT and consumer electronics industry in Europe, 2004.

32. Teixeira de Sousa P., Stuckmann P., telecommunication network interoperability, TELECOMMUNICATION SYSTEMS AND TECHNOLOGIES - Vol. II

33. Dzida, W. International User-Interface Standardization. In J. Allen B. Tucker (Ed.), The Computer Science Engineering Handbook (pp. 1474 - 1493), Boca Raton, Florida: CRC Press, 1996

34. ATHENA Contribution to Interoperability Policy Action Plan Version 2 February, 2006

35. INTEROP Interoperability Research for Networked Enterprises Applications and Software Network of Excellence - Contract no.: IST-508 011 www.interop-noe.org

36. Blagoev L., Manolov S. Model Requirements for the Interoperable Content Management in e-Government, Proceedings of the International Conference on Information Technologies (InfoTech-2010)

37. Choy D., Brown A., Gur-Esh E., McVeigh R., Müller F., Content Management Interoperability Services (CMIS) Version 1.0, OASIS 2009

38. Manolov S., Trifonov R., Electronic Data Interchange Between Parties Involved In Incident Handling Process, Proceedings of the International Conference on Information Technologies (InfoTech-2012)

39. T. Vitvar, V. Peristeras, K. Tarabanis Semantic Technologies for E-Government Springer-Verlag Berlin Heidelberg 2010

40. S. Manolov Fully controled environment for interoperability between administrative information systems Proceedings of the International Conference on Information Technologies (InfoTech-2008)

41. Breaking Barriers to e-Government, Overcoming obstacles to improving European public services MODINIS study, Contract no. 29172, A Legal and Institutional Analysis of Barriers to e-Government Draft Deliverable 1b, 16/08/2006

42. "EUROPE 2020 - A strategy for smart, sustainable and inclusive growth", Communication form the Commission, COM(2010) 2020, 03.03.2010, Brussels, Belgium

43. "A Digital Agenda for Europe", Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions, COM(2010) 245, 26.08.2010, Brussels, Belgium

44. "European Interoperability Architecture: Phase 2 – Final Report: Common Vision for an EIA", v.2.0, 11.2011

45. “Supporting the European Interoperability Strategy Elaboration”, Final Report Phase 1, 02.07.2009, Deloitte

46. “Achieving Technical Interoperability – the ETSI Approach”, European Telecommunications Standards Institute, White Paper No. 3., October 2006

47. Sylvia Archmann, Just Castillo Iglesias, Interoperability and community building for transformational e-Government, www.epracticejournal.eu

48. Jylhänkangas R. "European Interoperability Strategy, Framework and the Levels of Interoperability", Presentation at the Digital Agenda for Europe Going Local, 2011

49. European countries aligning their interoperability policies, http://joinup.ec.europa.eu/news/european-countries-aligning-their-interoperability-policies, March 13, 2012

50. Law on e-Governance In force as of 13 june 2008 Promulgated in SG no 46 of 12 june 2007

51. Ordinance on the electronic administrative services In force as of 13 June 2008 Adopted by Council of Ministers decree no. 107 of 19 May 2008 Published in State Gazette no. 48 of 23 May 2008

52. Ordinance on the requirements to the uniform environment for exchange of electronic documents Adopted by Decree of the Council of Ministers no 158 of 2 July 2008 Promulgated in SG no 62 of 11 July 2008

53. Ordinance on the general requirements for interoperability and information security In force as of 25 November 2008 Adopted by CoM Decree nr.279 of 17 November 2008 Promulgated in State Gazette, no. 101 of 25 November 2008

54. Ordinance on the registers of the information objects and the electronic services Effective as of 13 June 2008 Adopted by Decree of the Council of Ministers no.98 of 16 May 2008 Promulgated in SG, no 48 of 23 May 2008

55. Ordinance on the electronic signature certificates in the administrations Effective as of 13 June 2008 Adopted by Decree of the Council of Ministers no 97 of 16 May 2008 Promulgated in SG, no. 48 of 23 May 2008

56. Ordinance on the internal circulation of electronic documents and documents in hard-copy form in the administrations In force as of 13 June 2008 Adopted by CoM Decree no. 101 of 17 May 2008
Promulgated in State Gazette no. 48 of 23 May 2008

57. S. Manolov The right way to the real achievement of interoperability between the governmental information systems International workshop: "e-Government and data protection" (Varna, September 2006)

58. S. Manolov The interoperability requirements for pan-European electronic services Proceedings of the international conference on information technologies (InfoTech-2007), vol. 1

59. L. Blagoev, K. Spassov NMDPA – a part of the semantic network of the administration Proceedings of the international conference on information technologies (InfoTech-2013)