Interoperability and Security Standards and Rules in the Polish Law on Informatization

G. BLIŹNIUK
grzegorz.blizniuk@wat.edu.pl

Institute of Computer Sciences
Cybernetics Faculty, Military University of Technology
Kaliskiego Str. 2, 00-908 Warsaw

Observing time-period from 2003 till 2008, polish governmental efforts in informatization was focused on e-government legal foundations and IT standards too. Main purpose of this article is to achieve short discussion of crucial associations between IT practice (especially software engineering rules) and legal limitations of IT plans and strategies in Poland. Main issues of author considerations are rules of interoperability and security of IT systems in polish public administration.

Keywords: interoperability, IT systems, software engineering

1. Introduction

The primary objective of informatization of public administration is to increase effectiveness of the operations of traditional administration and to raise the quality of electronic public administration (e-government) services provided for citizens and business entities. One of the key preconditions necessary to achieve the above objectives is to ensure interoperability of the information and communications systems, i.e. to enable effective exchange of information in electronic form and to ensure interoperation between the information and communications (data communications) systems and public registers. Exchange of information in electronic form takes place between:
- government (public administration) and citizens,
- government (public administration) and business entities and organizations,
- various units of Polish public administration,
- Polish public administration and administrations of other countries.

The objective of the law was to enable achieving accessibility, interoperability and technological neutrality of the interfaces of information and communications systems used to carry out public tasks. The law should enable an appropriate Minister responsible for informatization (IT systems implementation) to perform the role that involves coordinating, stimulating and supporting the development of IT systems in Poland while maintaining the principle of technological neutrality of IT solutions used.

The e-government implementation (public administration informatization) process affects a number of various entities and constitutes the horizontal base. They are:
- citizens and companies (more generally: non-public entities) – government (public administration) services are provided for them,
- Polish central government, local self-government and European administrations – Polish public administration should be able to communicate within Poland, as well as with other EU administrations (e.g. Schengen administration, customs administrations, court administrations, digital tachograph systems etc.),
- ICT industry and business associations – interested in working for the public sector and this is a reason why they need defined informatization standards and plans,
- universities, institutes, research and development units– the academia is interested in providing know-how for the public administration (government).

2. Interoperability

The need to guarantee interoperability of IT systems within the Polish public administration required preparing and implementing a law on informatization. Before the law came into force the Polish legislature did not guarantee the way to methodically ensure the required interoperability.

Interoperability in the law on informatization is understood in three mutually affecting one another areas, namely:

* Act of February 17, 2005 on information technology implementation in the operations of entities that carry out public tasks (Journal of Laws no. 64, item 565 and of 2006 no. 12, item 65 and no. 73, item 501) [1]
organizational interoperability, understood as achieving effective collaboration between public entities, a citizen and business – in the law particular emphasis is placed upon ability to interoperate during administrative activities performed with the support of the ICT systems,

informational interoperability, i.e. ability to effectively exchange information between public entities, a citizen and business – understood both in the syntactic data compliance dimension, as well as in the semantic information integrity dimension,

technical interoperability, understood in the dimension of technology used to exchange data between the public administration (government) information and communications systems, and a citizen and business.

3. Organizational interoperability

In order to ensure that the Minister responsible for informatization could have influence upon increasing organizational interoperability within the entire public administration it was necessary to enforce the Minister with the appropriate law in compliance with the legal rules in force under the Polish legal system. This enables, based on legal authorizations, effective coordinating of the so-called domain based laws and the appropriate executive acts related to specific information and communications systems of which there are almost 900.

In most cases these laws specify general functional scope of the information and communications systems, and sometimes also describe the technological requirements for such systems. It is unfortunate to repeat in the successive laws basically identical technical and organizational requirements for the information and communications systems. Such a bargain arose first of all as a result of an earlier lack of a law on informatization. It is exactly in this law where the information and communications systems interoperability framework was defined, common for all the other domain based laws.

The law plays a role of the so-called horizontal regulation which constitutes the essential reference point for other laws related to the informatization of specific domains of the public administration’s activities. The law shall be applicable to:

- central government agencies, state control (audit) and law enforcement agencies, courts, public prosecutor’s office organizational units, and also units of the local territorial self-government and the agencies thereof,
- state budget units, state budget enterprises and the state budget units’ auxiliary farms,
- target funds,
- autonomous public health care units,
- Social Security Organization (ZUS), Farmers’ Social Security Organization (KRUS),
- National Health Fund,
- central government or local self-government legal entities set up under separate laws in order to carry out public tasks.

All of these organizations and units are defined as “public entities” in the law.

So what are the foundations of organizational interoperability under the current law on informatization? The answer to this question requires studying several important issues covered by the law under discussion.

First of all authors of the draft law made an assumption that it was applicable to the information and communications systems operating at the interfaces between central government, local self-government, a citizen and business. The law introduces the need to define a rolling, maximum five year e-government implementation (state informatization) plan which will be of particular importance for IT companies. It is clear that the worst thing that might happen is a lack of clear rules of how the public procurement market in IT area is to function, and in particular a lack of information, available appropriately ahead of time, on the information and communications systems planned to be implemented. The informatization plans may play a role of mandatory tools for the Polish government to provide information for the Polish data communications industry on possible public orders in the ICT area.

In art. 5, item 2 of the law the objective of the E-government Implementation Plan [6] (State Informatization Plan) is defined as:

- defining organizational and technological instruments for the development of information society,
- coordinating public use IT projects implemented by more than one public entity,
- modernizing and merging information and communications systems used to carry out public tasks,
- ensuring secure conditions and operational compatibility of the IT systems used to carry out public tasks,
creating conditions for the growth of international cooperation in the informatization area.

Objectives defined in the law focus on ensuring organizational interoperability.

In art. 5, item 3 of the law the content of the E-government Implementation Plan is defined:

- definition of priorities for the development of information and communications systems used to carry out public tasks,
- list and description of multi-sector and sector specific IT projects used to implement the above mentioned priorities, estimated costs of implementing such projects and indication of possible sources of financing thereof,
- information society development action program,
- definition of public tasks that will be carried out electronically and dates of commencing the implementation thereof.

Multi-sector IT projects shall be established by way of an ordinance (in accordance with art. 8, item 1 of the law) of the Council of Ministers, at the request of the appropriate Minister responsible for informatization. Sector specific IT projects shall be established by way of ordinances (in accordance with art. 9, item 1 of the law) of the appropriate Ministers responsible for the affairs of the given area of central government, following the receipt of an opinion of the appropriate Minister responsible for informatization.

Another important assumption of the law, is an obligation imposed on the Minister responsible for informatization to certify all information and communications systems used to carry out public tasks with respect to the compliance thereof with the so-called „minimum requirements”. This supervision is more to stimulate development of the government (public administration) information and communications systems, than to ensure a standard checking of the compliance thereof with the minimum requirements.

A delegation to establish, by way of ordinance, minimum requirements for the information and communications systems [2], Journal of Laws no. 212 of 28.10.2005 item 1766,


The regulations of these ordinances will be reviewed in reference to the informational interoperability and the technical interoperability.

An important point, brought to the law [1] (art. 21 of the law), is openness of the acceptance test sets for the interface software that enables data exchange with IT systems to be used to carry out public tasks. Guidelines with respect to the procedure to be followed to document and conduct acceptance tests are provided in:

- Ordinance of the Council of Ministers of October 11, 2005 on acceptance tests and testing the interface software and verifying such tests [4], Journal of Laws no. 217 of 31.10.2005 item 1836.

Another important assumption mentioned in the law on informatization (art. 15 of the law) is the principle that if non-public entities, e.g. a citizen and business, have a state imposed need to communicate therewith via IT systems then the applicable software shall be provided free of charge. The method of providing such software is defined in:

- Ordinance of the Council of Ministers of September 27, 2005 on the method, scope and manner of accessing the public register data [5], Journal of Laws no. 205 item 1692.

In summary, the main assumptions of the organizational interoperability are based on the following guidelines:

- horizontal approach plus technological and political neutrality of the law,
- informatization plans,
- establishing multi-sector and sector specific IT projects,
- establishing the Informatization Council – an advisory body providing assistance for the Minister of Informatization,
- establishing the National Register of Information and Communications Systems and Public Registers,
- checking the systems’ compliance with the minimum requirements,
- openness of the acceptance test sets for the interface software,
free of charge providing of the required interface software to non-public entities and local self-government units.

The above quoted provisions of the agreement create a good framework for ensuring organizational interoperability in the performance of public tasks.

4. Informational interoperability

Informational interoperability is related to two essential issues, i.e.:

- syntactic compliance of data sent between systems (it is applicable to the method of describing the data transfer structure), also called syntactic interoperability,
- semantic compliance of information, frequently called semantic interoperability.

Exchange of information between public and non-public entities should be analyzed taking into account two most important tools thereof. They are: an electronic document and exchange of reference register attributes.

With respect to the syntactic interoperability the law on informatization is to bring about full compliance and manageability of the description formats of the logical structure of an electronic document in the Polish public administration, and also a common description of the format of key reference attributes of public registers. As an example of a lack of syntactic compliance given frequently is a different way to write names of localities or streets. It is certainly possible to introduce additional mechanisms that link different ways of writing names, but this is always a potential place where ambiguous interpretations are possible, and what follows – potential threats for the integrity of information sent between systems.

The syntactic compliance of the data description is a basis for achieving semantic compliance of information which is undoubtedly a much more complex task. The point is to achieve full informational integrity of the data communications systems which will make it possible, for example, to avoid ambiguous interpretations of information sent.

The basic regulations aimed at ensuring informational interoperability are provided in three executive acts issued on the basis of art. 18 of the law are:

- Ordinance of the Council of Ministers of October 11, 2005 on the minimum requirements for the information and communications systems [2], Journal of Laws no. 212 of 28.10.2005 item 1766,
- Ordinance of the Council of Ministers of October 11, 2005 on the minimum requirements for the public registers and exchange of information in an electronic form [3], Journal of Laws no. 214 of 28.10.2005 item 1781,
- Ordinance of the Minister of Science and Informatization of October 19, 2005 on acceptance tests and testing the interface software and verifying such tests [4], Journal of Laws no. 217 of 31.10.2005 item 1836.

The first of the above mentioned ordinances includes a number of important requirements which are to raise the level of informational interoperability:

In § 2 section 1 of the ordinance a general requirement is stated that „information and communications systems used by public entities to carry out public tasks should comply, with respect to properties and features in the area of functionality, reliability, usability, performance, portability and maintainability, with such properties and features defined in the ISO standards approved by the national standardization unit, at the stage of designing, implementing and modifying such systems”.

Appendix no. 1 specifies requirements that enable data exchange with other information and communications systems used to carry out public tasks using the communications and encryption protocols:

- to exchange data with the information and communications systems,
- to exchange data with the information and communications systems in a form of communications between a client and a server of an electronic mail system,
- to encrypt data exchange with the information and communications systems,
- to exchange data with the information and communications systems with respect to other network services.

Appendix no. 2 specifies requirements that ensure access to information resources made available by the information and communications systems used to carry out public tasks using data formats:

- to encode and encrypt information,
- to data that includes text or text and graphics documents,
- to data that includes graphical information,
- to compress large size electronic documents,
- to create and modify WWW sites,
- to define the information layout,
- to process documents saved in the XML format.
It should be emphasized that it is the first legal act in Poland in which the XML standard is indicated as the basis of the description of the logical structure of an electronic document, i.e. the manner of laying out information in a document defined by specifying information elements and the relationships between them.

The second of the above mentioned ordinances (on the minimum requirements for the public registers and exchange of information in an electronic form) is a legislative act which provides in a systematic manner the scope and definition of data types for 16 key reference attributes of public registers in Poland. This is very important for maintaining the interoperability of public registers and to indicate those register attributes which play an essential role in the data exchange between the key information resources in Poland. The ordinance covers the following register attributes: Personal ID number (PESEL), surname-section, first name, company ID number (REGON), territorial unit symbol, territorial unit name, locality identifier, locality name, street symbol, street name, premises number, building number, National Court Register number, Tax Identification Number (NIP), registered parcel identifier, building identifier.

It is assumed that the scope of the register reference attributes will be modified in accordance with the upgrades of the information and communications systems used to carry out public tasks.

The third of the above mentioned ordinances (on acceptance tests and testing the interface software and verifying such tests) defines:

- methodology, conditions and procedure to be followed to prepare the interface software acceptance tests,
- procedure to be followed to conduct the interface software testing,
- types of interface software subject to testing,
- detailed scope of information related to the interface software and the method and procedure to be followed to provide such information,
- sample statement on the result of testing and verification of the interface software testing.

The interface software was rightly treated in the regulations in a unique manner because it plays a special role in ensuring the informational interoperability.

5. Technical interoperability

The lowest interoperability level is the technical dimension thereof. This level is well understood by programmers who deal with the software of protocols used to exchange data between information and communications systems, electronic documents formats and other file formats. In that manner TCP/IP or the UNICODE character encoding standard are applicable to the technical dimension of interoperability.

The detailed scope of technical requirements is provided in the Ordinance of the Council of Ministers of October 11, 2005 on the minimum requirements for the information and communications systems [2], Journal of Laws no. 212 of 28.10.2005 item 1766. They regulate the scope of standards for:

- character encoding format,
- communications protocols,
- encryption protocols,
- format of files used to store electronic documents,
- format of files used to store graphics, audio, compressed files.

Ensuring the technical interoperability is also the objective of Ordinance of the Minister of Science and Informatization of October 19, 2005 on acceptance tests and testing the interface software and verifying such tests [4], Journal of Laws no. 217 of 31.10.2005 item 1836. It specifies the technical side of ensuring interoperability of information and communications systems used to carry out public tasks.

6. Security

Another objective of the law on informatization was also to achieve a higher level of information security, including the data communications security for the IT systems used to carry out public tasks. The law introduced an obligation to define a security policy for all IT systems used to carry out public tasks.

The guidelines related to the scope of preparing the state informatization plans among others impose the need „to ensure secure conditions and operational compatibility of the IT systems used to carry out public tasks”. Art. 18 of the law provides guidelines to prepare the minimum requirements for the information and communications systems in such a way so as to take into account in particular the need to maintain „efficient and secure exchange of
information in electronic form between public entities and between public entities and official agencies of other countries or international organizations”.

This is why the ordinance of the Council of Ministers of October 11, 2005 on the minimum requirements for the information and communications systems [2], Journal of Laws no. 212 of 28.10.2005 item 1766 describes the security policy in the following manner:

1. § 3.1: A public entity shall define, modify as required and implement a security policy for the information and communications systems used by such entity to carry out public tasks.

2. § 3.2: When defining the security policy mentioned in item 1, a public entity should take into account the provisions of the Polish Standards with respect to information security.

It seems to be right to apply here the following national standards related to information security:

- PN ISO/IEC 17799:2003 Practical information security management principles – guidelines on how to define security policies of organizations from various sectors, including also central government and local self-government,
- PN-I-07799-2:2005 Information security management systems. Specification and guidelines to be applied – requirements related to the information security management systems – how to manage security taking into account risk management.

The international standardization system currently being developed is based on the 27000 series standards – in particular standard 27001 – the successor of PN-I-07799-2. It is worth noting that the Polish standard PN-I-07799-2 is ahead of the international standard. It provides guidelines for developing clear and unambiguous criteria for the security of information and systems that process it. This is of particular importance for central government and local self-government and thus it may constitute an appropriate way to implement guidelines that result from the ordinance on the minimum requirements for the systems and related to the need to define the information and communications security policies. Based on this approach it will be possible to derive the following benefits:

- objective evaluation of the information security status in an organizational unit,
- compliance of the central government and local self-government information and communications systems with the legal regulations,
- setting measurable objectives for the information security management based on the prior definition of the required security level which is accompanied by the identification of responsibility for the individual information security elements at each stage of its development and storing,
- reducing the risk of losing, corrupting, gaining unauthorized access to the internal information of an organization,
- reducing material losses resulting, for example, from disclosing information, losing data and undesired modification of the data stored in IT systems and from a number of other threats to which an organization was up to now especially vulnerable,
- increasing an organization’s operations security and credibility on a competitive data communications market,
- ability to precisely define origins and real causes of the highest business risks which will make it possible to counteract the arising thereof,
- improving the flow of information and access thereto while at the same time increasing the information utilization security,
- ongoing removing of vulnerabilities and risk of losing information,
- raising the flexibility of an organization’s operations by better aligning the organizational structure to the internal and external requirements of its functioning,
- clear, coherent and coordinated program of investment expenditures for information security and information technology,
- change of the personnel’s mentality, increase of motivation and effectiveness of the work processes,
- ability to subject the information security management system set up to independent evaluation (certification) with respect to compliance with the Polish standard PN-I-07799-2 or international standard ISO/IEC 27001.

7. Summary

When analyzing solutions considering interoperability, information and communications security included in the law on informatization emphasized should be that the described model followed bases on
accomplishments of the EU program IDABC [7]. This program defines ICT aspects of interoperability in horizontal dimension which is being used by more than 40 domain based programs also developed within IDA. The IDA2 program did not solve all the problems, especially the ones related to the possibility of utilizing the interoperability of public registers. Important strategic solutions and appropriate instruments are proposed in the law on informatization of the operations of entities that carry out public tasks. These solutions shall lead to the point where users of administration services will, for identification purposes, be using one of the two register numbers, i.e.:
- **PESEL number** (personal ID number) – for private individuals,
- **Tax Identification Number** (NIP) – for business entities that are not private individuals.

The above identifiers should constitute the primary reference attributes of public registers in Poland, meaning that other IT systems should refer to these attributes always when identifying a private individual or business entity. Thanks to this approach a large number of currently used identifiers can be treated as internal identifiers used in the public administration systems. The following citizens will use a unique ID number when contacting public administration.

Close analogy may be found between the IDA program development concept and the earlier mentioned horizontal positioning of the law on informatization in relation to the domain based laws that introduce the need to set up further information and communications systems.

Further suggestions derived from the accomplishments of IDA also led to the recognition of the XML standard, including the derivatives thereof, as the basis for the description of an electronic document’s logical structure.

In summary it should be clearly emphasized that the essence of the e-government implementation involves a skillful application of the contemporary IT methods and tools in order to obtain appropriate instrumentation for the public administration services, ergonomic for the beneficiaries of such services. The above principle is applicable to both the traditional public offices which without the appropriate IT support will not be able to work effectively - as well as to a virtual public office which constitutes an alternative for the traditional public offices but does not oust them in any way. It can be stated that the law on informatization, including the executive acts thereof provides the necessary legislative tools that enable materializing this idea in reality.

8. Bibliography


[4] Polish Minister of Scientific Research and the IT, *Directive of Minister of Scientific Research and the IT from day 19 of October 2005 r. in the cause of acceptances test and studying the interface software and the verification of this examination*, Polish Diary of Acts No. 217 from the 31 Oct 2005, pos. 1836 – in polish;

