

E-Government Architecture and the Interoperability of Information Systems – Estonia's Example

Uuno Vallner, director, Development Division, Department of State Information Systems, Ministry of Economic Affairs and Communications, Estonia

The Estonian government's IT architecture and interoperability framework is based on the country's public key infrastructure (PKI) and ID card, the middle-ware X-road for the integration of databases, and the citizen environment that is known as KIT. The framework defines a set of recommendations and guidelines which describe the way in which organisations have agreed (or should agree) to interact with each other. The framework is not a static document, it can be updated every year. Adherence to the architecture and interoperability framework, however, is mandatory in terms of policies and specifications. These set out the underlying infrastructure, thus allowing public sector organisations to concentrate on the building up of E-services.

INTRODUCTION

In June 2004, Estonia's Ministry of Economic Affairs and Communications published the first version of a new document – "The Government IT Architecture and Interoperability Framework". The framework was elaborated through co-operation among state and local government agencies, as well as private sector IT experts. Implementation of the framework is to be co-ordinated by the State IT Interoperability Council. The framework recommends technical policies and specifications for joining up public administration information systems all across Estonia. It's based on open standards and encourages the use of open source software. The three pillars on which the framework is based are the Estonian PKI infrastructure and ID card, the middleware X-road for the integration of databases, as well as the citizens' environment KIT.

Interoperability means the ability of information and communications technology systems and of business processes which they support to exchange data and to enable the sharing of information and knowledge.

The Estonian IT architecture and interoperability framework sets out recommendations on how organisations have agreed or should agree to interact with one another. This is not a static document, it can be updated on a yearly basis. Adherence to the policies and specifications, however, is mandatory. They set out the underlying infrastructure, which means that public sector organisations can concentrate on the building up of E-services.

OBJECTIVES

The objectives of the architecture and interoperability framework are the following:

- To cut down on the expenses of public administration systems through centrally implemented middleware;
- To help in achieving interoperability through the use of open standards, the Estonian PKI infrastructure and ID card, the middleware X-road for the integration of databases, and the citizens' environment KIT;
- To improve coordination of the development processes of information systems for public administration and

to accelerate the development of E-services;

- To achieve the independence of public information systems by following the principles of organisational, semantic and technical interoperability that are described within the framework;

- To create facilities for free competition among IT companies in the area of public procurement.

The joint architecture includes the following elements:

- **Joint co-ordination:** The Ministry of Economic Affairs and Communications will co-ordinate the development of public administration information systems;

- **Agreements:** Common methodologies, concepts and description standards for architecture, common choices regarding standards, infrastructure, common architectural principles;

- **Common tools:** Common software and middleware.

KEY POLICIES

These are the key policy decisions which have been made:

- Public services are provided free of charge throughout the public sector;

- Adoption of common specifications on the Internet and WWW for all public sector information systems, as well as use of standards from the World Wide Web Consortium (W3C), the Internet Engineering Task Force (IETF) and OASIS;

- Adoption of XML as the primary standard for data integration and data management for all public sector systems;

- The use of multilateral solutions at the technical, semantic and organisational level for accessing of services;

- Use of open standards – to reach interoperability, public sector systems need to focus on open standards. The Dutch programme for open standards and open source software defines "open" as follows:

- The costs for using the standard are low and not an obstacle against access;

- The standard has been published;

- The standard has been adopted on the basis of an open decision making procedure;

- The intellectual property rights to

the standard are vested in a non-profit organisation which operates a completely free access policy;

- There are no constraints on the reuse of the standard.

- Adoption of the browser as the key interface – all public sector information systems are to be accessible through browser-based technology; other interfaces are permitted, but only in addition to ones that are browser-based;

- Use of the Estonian PKI infrastructure and ID card in all authentication and authorisation processes, with the use of Internet banking authentication facilities permitted for the authentication of local residents;

- All services use the secure middleware X-road (X-tee in Estonian) for data transport;

- The benefits of open source software are to be considered by all public sector systems, and open source software should be considered favourably alongside proprietary alternatives.

- Single point entry for citizens, entrepreneurs and officials, with additional links to E-services highly recommended.

THE ENVIRONMENT FOR THE SERVICES

All of the public sector information systems are handled as a whole. Citizens, businesspeople, civil servants and programmes are all users of the services. They don't care who provides the services. The framework defines authentication and authorisation rules for all groups of services providers, for information systems and for their customers. The structure of the environment for the services is shown in Figure 1.

AUTHENTICATION RULES

The framework involves two-level authentication – that of information systems and that of users. Every information system is authenticated through a certificate that is issued by the X-road certification authority. Individuals, for their part, can be authenticated via their ID card, through Internet banking (only citizens) or through certificates (only officials). Programmes are authenticated by the certificate of the individuals who launch them.

AUTHORISATION RULES

The framework involves two levels of authorisation – that of information systems and that of users. Each information system is authorised by the service provider – each service contains a list of institutions and groups of institutions for which access is permitted. Each institution is responsible for authorising its own users. This rule is very important, because now we can get rid of bilateral agreements between service providers and customer organisations. When we started the X-road project, the Estonian Databases Act stipulated that the service provider was responsible for the authorisation of all users. That was similar to a situation in which alcohol producers would be made responsible for the results of misuse of alcohol.

OWNERSHIP OF PUBLIC SECTOR DATABASES

Service providers must provide a new service each time a public institution needs one. This is another very important rule. The owner of the public sector databases is the government, and that means that government insti-

tutions, not service providers, determine the services that have to be provided. The old law said that the right to provide or not to provide services rested with the service providers.

The framework sets out rules for connecting information systems to the environment of services. Each organisation must use a security server for interaction with state information systems.

THE CITIZENS' ENVIRONMENT

Estonia's citizens' portal (KIT) provides holders of ID cards and Internet banking clients with additional access to restricted or confidential information – that which requires user authentication. In addition, the citizen portal allows people to access their personal information system, in which there is direct access to the following basic components of KIT: The citizens' document management system, an electronic mailbox that can be redirected, and a secure environment for accessing services and for providing digital signatures.

The citizens' information system is equal to that of a ministry, a city government or a bank. The citizen com-

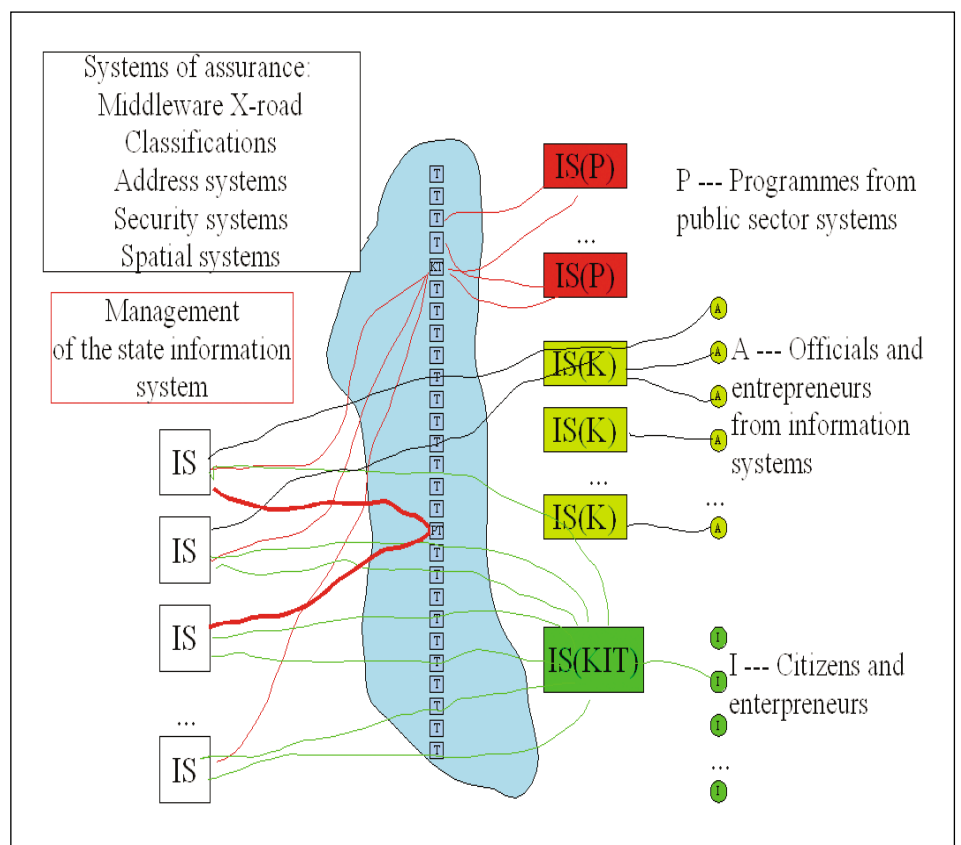


Figure 1. The environment for the services

municates with all other information systems in the state via his or her personal information system (office). All information systems can and must communicate with the citizen's office and reflect the state of processing his or her affairs. The citizen no longer needs to search for services. Instead, he or she has the right to order up services and to monitor their processing without leaving the "office".

A CITIZEN GUIDE AND RELATED SERVICES

The information portal is a freely accessed Web site which informs people about their rights and obligations in terms of communications with state and local governments. The portal also contains tips for conducting administrative operations with state agencies, as well as forms, links to legislative acts and useful homepages, relevant phone numbers, as well as WWW services. The portal has often been called the citizen's handbook.

The information portal can be found at <http://www.eesti.ee>, but it is available only in Estonian at this time. Russian and English versions have been produced, but they lack the thoroughness of information that is a part of the Estonian language portal (the other portals can be found at <http://www.eesti.es/rus> and <http://www.eesti.ee/eng> respectively).

The main page of the information portal serves as a gateway to the entire portal, which is hierarchically structured. The page also provides a link to the citizen portal, and authentication through an ID card or an Internet bank is needed to access it. In some cases, certain topics that are covered by the information portal also require user authentication. When the information portal refers to a service that requires authentication, the user must provide identification through the aforementioned means.

Responsibility for preparing and updating information on the portal and for the validity of that information rests with various institutions. The information portal, in other words, is a common database of information services that provided by the state and the local governments, business and third sector of Estonia.

FORENAME.SURNAME_NNN@EESTI.EE

A citizens' E-mail system is needed for communications with server providers. Each citizen has an E-mail address – Forename.Surname_NNN@eesti.ee, which is assigned via the ID card. Citizens can choose a different user name, their personal ID code is the default user name. In order to avoid junk mail, only authorised information systems are allowed to send mail to this address. It is assumed that citizens use the address and redirect it to their customary mailbox.

THE VIRTUAL OFFICE

Each user has his or her own private space, in which data can only be processed by the relevant individual. The document management system can only be used through an authentication system. The user can archive initiated processes. All of the information systems of state and local government agencies and enterprises send notices of E-services to the user's archive. Processes can be initiated by the user and the information system of an agency. All subsequent activities related to the specific process are linked to the initiation document in the citizen portal.

THE DIGITAL SIGNING ENVIRONMENT

The citizen portal also includes a space for digitally signing documents and for the exchange of signed documents with partners. The information system allows people to submit documents (applications, proposals, complaints, etc.) to any agency that has joined the KIT and then to monitor the processing of those documents in the state's apparatus in terms of the status of documents (e.g., "approved", "being processed", "on hold", "waiting for approval", "under review", "completed").

DIRECT SERVICES

This part of the system was developed in the course of the X-road programme. Citizens can make queries to state databases about their own data. Results are seen on the inquirer's monitor. These services are not complicated in terms of business logic, and decisions can be taken without the intervention

of a civil servant. Citizens cannot, however, read the data of other people.

THE ENVIRONMENT OF OFFICIALS

The primary users of government services are officials. They need to authenticate and authorise themselves by logging in once, and then they see the entire list of services that are authorised for them. Unlike local residents, they can find and review more detailed data, they can use their own environment to change and to add data during the decision making process (insofar as their authority so permits). The government system ensures adequate security for the treatment of inquiries that are made to databases and the responses that are received.

The databases function in a standard way – they are connected to the X-road system through a special user interface. Because of this, queries to all databases are made in a similar way. The system was designed and installed in a secure environment. The security servers of the databases and information systems which are connected to the X-road system communicate through encrypted channels. It is impossible for a civil servant to read or to process data that are not related to his or her duties.

The topology rules of consumer information systems are as follows:

- Every information system is connected to the X-road via a security server;
- The certification authority provides certification to the security servers;
- Service providers use a special adapter server for SOAP queries;
- Small institutions can use the special MISP portal;
- Larger institutions integrate the MISP portal into their own information systems. □

REFERENCES

1. Vallner, U. "An E-community, E-citizens and E-services – a New Infrastructure and Reengineering of Institutions", *Baltic IT Review*, No. 4(27), 2002.
2. Vallner, U. and T. Tammet. "Single Point Entry to the Estonian Government's WWW System", *Baltic IT Review*, No. 1(12), 1999.