The Mega-system: integration of National information systems

Conceptual and Methodological Baselines of the Megasystem

Because a drastic improvement of quality and full interoperability of all National Information Systems are vital for the development of the country, all set of systems is being developed as a logically unified and technologically distributed information processing Mega-system with a common data field as well as unified user’s interface, access principles and authorisation procedures.

All end-systems, irrespective of their ownership (various information systems, their remote data entry and access points, end-users of information) will all be interconnected through a high speed data communications network (see Fig. 1). The unified Mega-system will be spread to all regional and rural administrative centers and to number of cities, border checkpoints, ports, etc. Local authorities will be connected to the Mega-system in order to conduct direct data entry into all components of the Mega-system and to use information from all systems for local needs. Special terminals and access points (information kiosks) are envisaged for public access to information that is specified for general use.

This means that it will be possible to move basic data entry and utilization procedures to places where the information has been originated or exploited as well as to provide direct access to information for everyone who has the proper authorisation (see Fig.2). It will avoid duplication of records and coincidence of records in documents and databases as well will provide united and user-friendly access to information. In addition to various information systems the Mega-system will include register of registers for collection and distribution of information on all components of the Megasytem as well as the communication server -- common central access point to

![Diagram of the Mega-system](image-url)
information resources of the Mega-system. Conceptual and methodological propositions of the Mega-system and corresponding action plan has been accepted by special direction of the Cabinet of Ministers.

In order to realize all plans and to achieve the aforementioned goals on both state and municipal levels information systems for local authorities will be elaborated and implemented on qualitative new advanced level and connected to the Megasystem as soon as possible:

- to conduct direct data entry into all National Information Systems;
- to use information collected in all components of the megasystem for satisfaction of local needs;
- to provide electronic document exchange throughout the country;
- to envisage general access to public information and electronic contacts of population with State and local authorities.

Creation of the Mega-system is not only technological decision, in fact it means solving of number of various informative, legal, organisational, financial and qualification problems first of all. It was necessary among other issues:

- to analyse existing data flows, to formulate the functions of the Mega-system and to distribute them among information systems, to formulate demands on systems and their data structure;
- to define the subjects of various information systems and the amount of stored information, as well as the institutions that are responsible for the collection, processing and distribution of data;
- to formulate the tasks and subjects of information systems for local authorities and to elaborate several intercompatible informative models for implementation by local authorities;
- to define a unified user interface, access principles and authorisation procedures;
- to ensure data quality and security as well as interoperability with EU information systems;
- to elaborate a methodology for data verification;
- to determine the principles of electronic archives.

![Figure 2 The Mega-system: data flows](image-url)
With this conception emphasised was necessity for the country to put in order during the first stage of the Mega-system’s project its main subjects registration which should go ahead of other systems elaboration: private persons (population), legal persons (enterprises, establishments, organisations), real estate (land, buildings, owners) and movable property (transport vehicles, owners), as well as state finances (taxes). In compliance with these principles five relatively primary NIS were proposed for the first stage as to-be-integrated systems:

- Population Register;
- Enterprise Register;
- Real Property Register;
- State Vehicles Register;
- State Revenue Service Information System.

The integration of the primary NIS as well as elaboration and installation of the central body (the register of registers and the communication server) were realised during 1998-1999.

In the same time mentioned primary NIS are not declared as the only state significance information keepers. At present in Latvia operating are over 30 branch information systems by what understood are those NIS settling one branch, ministry, region or one problematic issues. These information systems will be attached to the central core of the Mega-system gradually as far as they will be prepared. It is planned to develop during the second stage connection of the Unified Information System for Local Governments, Education Informatization System and several information systems that deals with real estate.

The Government Data Communications Network for the government’s and local authorities needs is an essential communications element in establishing of the Mega-system. This Network at the moment is the major part of integrated voice/data network, developed by the non-profit organisation state joint stock company State Information Network Agency VITA on a common transport network basis. The Cabinet of Ministers approved a complex contemporary development concept for the network in 1999.

The Government Data Communications Network must provide close and operative interoperability of all interconnected systems. Various but similar requirements to the network can be separated into several groups:

- reliability; there must be uninterrupted action time, undistorted data transmission, a guarantee of several levels of confidentiality and security of information;
- high speed data transmission; some of real time systems need guaranteed channel capacity (e.g., Vessels Traffic Management Information System);
- presence of a gateway to public data transmission network (the Internet environment) which contains a reliable firewall system.

On-line access is becoming a basic one for data transmission, but on-line connections by means of separate communications channels, however, must not be an end in itself, their usage should be well grounded both technically and economically. Connection of end-users depends on real traffic, e.g., access points of common use for several
branches or dial-up connections would have to be established in cases where the traffic level is low. Connection of rural centers (villages) will have to be done on a selective basis, and in many cases local centers will be able to participate via dial-up connections or by use of diskettes to exchange and update information.

**The Concept of Communications Server**

A communications server is a set of software and computer equipment that allows a wide range of users (both in Latvia and in other countries) to receive information from a variety of sources (government registers, data bases, information systems) through a single contact point. A communications server identifies users, authorizes the use of the respective data, fulfills a request that involves several information sources, and evaluates the cost of the process so that the appropriate financial transaction can be made. A communications server allows users to learn where information is being stored and what kind of information it is, as well as to request and to receive information from various registers without any need for in-depth knowledge about the technical aspects of its storage.

![Diagram of communications between many registers and many users](image)

Figure 3. Communications between many registers and many users

The need to establish a communications server became apparent when the governments of the Baltic States were setting up their joint data transmission network. In order to allow institutions in one country to obtain information about objects registered in another (enterprises, persons, motor vehicles, etc.), it is useful to receive the necessary data from a single information source, without having to study the data base structures of the other country. The use of the communications server, as has been seen through the elaboration of an integrated state significance information systems project, is also of significance within one country, because it provides a universal resource for information exchange among various information systems.
Problem identification

The need to establish a communications server was noted in the national program “Informatics”, as well as during the elaboration of two major projects – the Baltic States Government Data Transmission Network (hereafter in the text – the Network) and the Integrated State Significance Information System (hereafter – the Megasystem). The goal in establishing the network is to provide fundamental improvements in the exchange of telecommunications and data among the administrative institutions of the Baltic States. During the first phase of the project (1998 and 1999), universal solution is being set up to provide for the exchange of data among Latvia’s Company Register, Motor Vehicles Register and Lost Motor Vehicles Register, as well as between these registers and the related international information structures. So far this has involved three concrete activities:

1) Accession of the Latvian Company Register to the European Business Register (EBR);

2) Cooperation between the Motor Vehicles Register and the related European-level structure EuCaris, as well as the establishment of a motor vehicles insurance system in Latvia (the so-called “green cards”);

3) Improvements to the system whereby lost and stolen motor vehicles are registered in Latvia, including a connection to the international data bases of Interpol in this area.

During the second phase of this project, between 2000 and 2002, more work will be done to include Latvian registers into the Network and to integrate them into international information structures. In the second phase, the plan is to place the Population Register, the Lost Persons Register, the Lost Personal Documents Register, the Educational Documents Data Base, the Visas Data Base, the State Statistics Information System, the Consular Information System, the Health Care Information System and the Narcotics Information System on the Network.

In a situation where information from various sources is available on the Network, but users have no knowledge about the technical details of storing that information, there is an obvious need for a universal solution, and that is where the communications
server comes in. The main requirement for a communications server is that it must allow users to formulate their information requests in a simple way and to receive responses to those requests without having to understand the technical aspects of the process. Users are not, after all, informatics specialists; they are employees of other administrative structures of the state, and there is no reason to think that they know anything about the way in which data objects are distributed among the registers of another country. We can expect both standardized and wholly unpredictable requests in this process. In terms of the urgency of requests, we can expect demands for on-line responses that require rapid response, as well as requests for off-line responses that can take hours or even days to fulfill. Needless to say, in setting up the communications system we must provide for all aspects of information confidentiality and user authorization.

The setting up of the communications system is important not only in the context of the Network, but also in the context of the Megasystem, which is a universal resource for the exchange of information among various information systems within a single country.

**The concept of the solution**

The communications server, which is illustrated in Figure 5, is an Internet resource point. Users of the server can access it via various protocols – HTTP, CORBA, DCOM, SMTP (E-mail) and FTP. The server provides users with an opportunity to find out where information is stored and what kind of information is available, and then to request and receive information from various registers without studying their structure. Because users may have access to sensitive information, users are identified with certificates, and all data transmissions are coded.

Users who wish to have access to sensitive information before work with the system is begun must receive a certificate that corresponds to the X.509 standard. The certificate must issued for a specific period of time (usually one year) by a specialized institution (presumably in Latvia this would occur under the supervision of the Constitutional Defense Bureau). Certificates of this kind contain information that identifies the user, and they are virtually impossible to forge. The certificates are used to code data and to identify the user. Latvia’s communications server will use a standard coding protocol such as SSL.

A user of the communications server sends information requests to it and receives responses from it. This can happen both on-line (HTTP, CORBA, DCOM) and off-line (HTTP, E-mail, FTP).

In the on-line regime, work with the communications server is based on the following structure: At the beginning of the process the user is identified. This means that the user sends his or her certificate to the communications server, which reviews it and specifies the user’s rights. If the user does not have a certificate, then he or she can access the communications server as a guest and receive a limited amount of information from it. Next the user requests information. The communications server once again identifies the user and, on the basis of the level of the user’s authorization, makes the appropriate requests to the data registers, sending the response to the user when it is received. The register receives not only the information request from the communications server, but also the user's certificate, which means that the register itself can identify the user and the user’s level of authorization. The result of this is
that the register provides only that information to the communications server for which the user is cleared.

In an off-line regime, the user requests information via HTTP, E-mail or FTP. During periods of time when it is less busy (usually at night), the communications server processes the request – identifies and verifies the user and then requests the respective information from the information registers. The response is sent to the user via E-mail, or it is stored until the user asks for it on-line.

The main advantage of an on-line regime in this process is that information can be obtained immediately when the need arises. This system can be used in cases when the speed at which a response is received is of importance, either from the point of view of the system (e.g., at border control facilities), or from the point of view of the operation (e.g., an application in which the registration number of an automobile is entered and information is received about the automobile from the Road Traffic Safety Department so that it need not be entered a second time).

The advantage of the off-line regime is that registers can even out the volume of work that is required, given that at night there should be relative few on-line requests for information. Off-line requests can also be sent in by users who have dial-up Internet connections, thus reducing costs. It is advisable to make off-line requests less expensive than on-line ones so that users are motivated to use the off-line system.

**The functions of the communications server**

We can specify five main functions for a communications server:

- User identification
- Authorization with respect to the use of information
- Management of user rights
- Fulfillment of requests that involve several information sources
- Evaluation of the costs of each request for billing purposes
User identification in a communications server

As was noted before, user identification involves X.509-standard certificates. In order to ensure that the certificate mechanism is operational, a communications system needs both a certificate server and a directory server. The former is a server that belongs to the certifying organization, generating and maintaining electronic certificates – both server certificates (issued to the server) and client certificates (issued to the user). The latter is a server in which the public keys of the certificates are stored, along with information about certificates that have been issued – when a certificate has been issued, to whom it was issued, and whether the certificate is valid or has been revoked.

The directory server is available to any interested party. For example, if a WWW server has been issued a certificate, any WWW user can ascertain that the server is secure. If a WWW client has been issued a certificate, in turn, the WWW server can ascertain that the client is authorized to work with the server. Both the client and the server can check the validity of the submitted certificates by looking them up in the directory server.

Work with certificates in WWW applications involves SSL (Secure Socket Layer) technologies, which are supported by most WWW servers, as well as the main WWW browsers – Netscape Navigator and Microsoft Internet Explorer. SSL technologies provide the following components of secure communications:

1) **WWW server approval**: A user can ascertain the fact that the WWW server is secure and that it can be entrusted with confidential information;

2) **The privacy of information**: The entire information flow between the client and the server is coded, using a unique session key. The session key is coded by the server with the client’s public key in order to send the respective information to
the client in a secure way. Each session key is used in only one session, which makes it difficult to decode the information without authorization. The information, in other words, cannot be viewed by unauthorized persons, even if it is intercepted on its way between the server and the client.

3) **The integrity of the information**: Both the server and the client calculate the control code on the basis of the content of the information, and if the information has been changed en route, the codes do not match. This means that the receiver of the information sees precisely the same information that was sent by the sender.

Secure data exchange between the WWW server and the client occurs in the following way when SSL technologies are used:

1) The client sends a request for data exchange to the WWW server;
2) The server in response sends its certificate to the client, asking for the client’s certificate if appropriate;
3) The client checks the validity of the server certificate through the digital signature of the certificate server, sending the client’s own certificate to the server if necessary;
4) When the authorization process is complete, the client sends the session key to the server, coding it with the public key of the server;
5) Both the server and the client know the session key, and further data flow between the server and the client during the respective session is coded with the session key.

The certificates of the server and the client are exchanged quickly and without any involvement by the user. The same is true with respect to an exchange of certificates among other applications.

When information is requested from the communications server (through the WWW or otherwise), the process occurs in the following way:

1) The user is identified through the aforementioned protocol, and the communications server checks the user in the directory server.
2) The communications server has a data base which records user rights, and the server uses this data base to specify the authorization level of the specific user. In carrying out the user’s request, the communications server checks the user’s rights in its own data base and, if the necessary level of authorization is there, then the request is sent along to the concrete register.
3) The register is also sent identification data about the user who has requested the information.
4) The software in the register checks the information in the directory server and authorizes the user.
5) According to the level of the user’s authorization, either the request is carried out and the result is returned to the communications, server, or the communications server is told that the user does not have the right to carry out the request.
6) The communications server returns the result to the user.

A user can also request information from the register directly, without passing
through the communications server. In that case the operational mechanism is similar:

1) When the information is requested from the register, the user must supply identifying information (a certificate).

2) The software in the register checks the information in the directory server and authorizes the user.

3) On the basis of the user’s authorization and the level of his or her access rights, either the request is fulfilled and the result is sent back to the user, or the user is sent information saying that he or she does not have the right to receive the data.

This mechanism ensures that there is no need for the user to reintroduce identification each time a new request is made. In each session, the user is identified on the first occasion that a request is made with respect to a confidential data source, and in later requests the information is sent on to all of the respective information sources. Another advantage of the mechanism is that there is a centralized method for distributing user rights, as well as a unified policy with respect to this. It’s also true that the user’s rights do not change depending on the way in which he or she accesses the information – via the WWW, via a different application, or through some other method.

Management of user rights

The rights of users can be divided into several categories:

- The right to obtain information about what is stored in a concrete register – provided that the information is publicly available;
- The right to obtain information about one entry in one table in one register, based on the unique identifier of that particular entry;
- The right to obtain a list of data from one table in one register, selected on the basis of specific criteria;
- The right to obtain a list of data from several tables in a single register (whether the link exists or not);
- The right to obtain information from several tables in one register that are linked through a specific relation, the data being chosen on the basis of specific criteria;
- The right to obtain information about one object from several registers on the basis of the primary key of the object;
- The right to obtain information about the existence of a link among specific objects from various registers;
- The right to obtain a list of data that are selected on the basis of criteria entered by the user, the data coming from several tables in several registers that are mutually linked.

The obtaining of information can be differentiated at four levels:

- A response as to whether the requested information has been found or has not been found;
• A response as to how many entries have been found;
• The primary keys of objects;
• The data that is being requested.

Each of these levels provides a different volume of information, and there are instances when the jump between proximate levels is quantitative, while in other instances it is qualitative. We could consider four different requests here:

“Does individual X own an automobile?”
“How many automobiles does individual X own?”
“What automobiles does individual X own?”
“Does individual X own automobile Y?”

The management of user rights is intentionally divided up so that it occurs in several places. The communications server has its own user management module, in which it stores information about the right of users to make various kinds of complex requests. Information about the right of a user to receive data from a specific register is stored either in the communications server or in a concrete register. The place where information about user rights is stored is harmonized between the communications server and the register. Because it is expected that before a register issues information, it will want to check the user’s rights to use the information, then information about the user’s rights with respect to a specific register will usually be stored in that register. From the perspective of centralized management, it would be better if information about user rights with respect to all registers were stored in the communications server. For various organizational reasons, unfortunately, this is either impossible on only partly possible. Information about user rights is stored both in the communications server and in the registers themselves.

The communications server is designed to work with both of these options, as well as with a combination of them, and the following scheme emerges:

• The communications server checks the right of the user to make a request in the first place, as well as the right of the user to seek out a link between objects in various registers;
• The communications server checks whether the user rights with respect to the concrete register are stored in the communications server or the register;
• If the rights are stored in the communications server, then it checks the rights before it sends the request to the register;
• If the information is stored in the register, then the register checks the user rights before it fulfills the request;
• If the rights are not stored in the register, then the register can, if necessary, receive information about the rights from the communications server in order to be able to check the rights of the respective individual to make the request.

Because it is possible for users to connect to the registers not only via the communications server, but also directly from an application, and because it should be true that in both instances the user has the same authorization to obtain information, then the check of whether a user has the right to obtain information from a specific register should occur not in the communications server, but in the register itself.
Information requests and the obtaining and depiction of information

The basic mission of the communications server is to provide users with access to various information sources so that they can obtain data from them. Let us take a look at the problems that arise in this process, devoting particular attention to the submission of requests and the obtaining of responses, and leaving aside the issue of user authorization, control over data access, registration of who has asked for information and what information has been requested, billing issues and such matters.

Information sources

An information source or resource facility can be any information system or data base from any organization. There are administrative regulations concerning the organizations, information systems and data bases that are included in the communications server’s network of services.

Over the course of time, the number of information sources can reach into the tens or even hundreds of sources. In Latvia alone there are already several dozen government registers, and their number may increase. Communications servers should also provide access to certain foreign information sources, as well as to the data bases of various other organizations in Latvia; these, too, could be included in the range of services provided by the communications server.

The communications server itself does not have an information sources. Each information source is primarily meant to carry out concrete and specific functions inside the respective organization. Information systems and data bases that are used in an organization are chosen, designed and optimized specifically for the needs of the respective organization. They may not be aimed at providing information to other entities, but if such an opportunity is intended, then it can be very specific, and many limitations can be applied to it. This means that the communications server must adapt to the information sources, and not vice-versa. Of course some information sources can upgrade their information systems and optimize their data exchange procedures in order to meet the communications server’s requirements.

Information sources that are part of the communications server’s network can differ in terms of significance and volume. The more significant a data base, the better must be cooperation with it. The size of data bases must also be taken into account, because it has much to do with the respective data processing mechanisms.

Another key issue is the quality and stability of information sources. Information systems can involve a wide variety of technologies, and they are of varying ages. Depending on the resources that have been invested, some are of a higher quality and some – of a lower quality. Of course, it is easier to make contact with a high-quality information system and data base that have been designed with modern technologies than with systems that are old and of a lower quality level. A communications server must certainly be ready to deal with information sources that are unstable, that make errors and that in some instances are not even accessible.

Information systems can be designed with various systems, they may have various data bases, and their use may involve various operating systems and computer technologies. A communications server must be prepared to handle these problems,
although this is no longer the worst possible difficulty, given that many different solutions are in existence.

Information can be stored in a wide variety of formats – that is the next issue. The most popular method for data storage is still relation databases. Object-oriented databases, static WEB pages and dynamic WEB pages that are generated from an internal format are becoming rapidly more influential. We must not, however, forget other information storage methods such as files of many different structures.

A concrete information unit and a logical group of information units can be doubled, stored in various formats, coded in various ways and stored in such a way that some of the information is kept secret. Information can be contradictory either within a single information system or among various information sources. This means that in the future the field of communications servers will have to involve various laws and data processing algorithms that are based on the technologies or artificial intelligence.

All of these aspects serve to demonstrate how serious is the issue of various information sources being highly varied. It should also be added that this heterogeneity exists among more than just information sources. The same situation can exist within a single register or a single organization.

It must also be remembered that each information source exists fairly independently. It can be updated, changed or liquidated, it can be created anew, its operations can be suspended for a while, or it can be withdrawn from cooperation with a communications server. This means that a communications server must exist in an environment that is not only highly varied, but also is extremely changeable.

**Users**

For our purposes, we will say that a communications server user is any subject that wishes to obtain a service from the server.

Users are usually differentiated on the basis of their level of authorization to obtain specific information from specific information sources. These rights are regulated by law and by other normative acts, and they are managed by a specific user management bloc within the communications server.

From the perspective of the communications server, another very important user classification is based on a different aspect – the way in which the user requests information and the way in which the user receives a response. A communications server should be operated on the basis of the principle that it is there for the convenience of users, not vice-versa. This principle means that the server must be ready to receive information requests of a great many varieties and forms, and it must be ready, every time, to provide a response that is convenient for the user in terms of its type and form.

**Requests and responses**

A communications server must be ready to accept information requests that are stated in various ways and forms. The main operational regime for communications servers is an on-line connection, but this can involve a dedicated line to the communications server, dial-up access to the server, or a connection through informational networks (the Internet, the Latvian State Significance Data Transmission Network (VNDPT), or
the networks of other national, global or organizational networks). We must also remember other ways to submit a request – E-mail, a request submitted on an electronic information carrier such as a diskette, a written request submitted on paper, or even an oral request.

Responses to various requests can be prepared in the same format as the original request. It should be added, however, that the user must have the right to select the method of response, irrespective of the way in which the request was submitted. Limitations on the ways in which requests and responses are formatted can be specified by administrative regulations, but in terms of technologies, a communications server must be prepared for all kinds of cooperation methods.

The forms of requests and responses can be highly varied. The most popular cooperation form is probably a WEB page, both for requests and for responses. This form of cooperation can be highly varied, and this is underpinned by existing WEB-type applications. The use of special procedures and functions may also be important when the procedure itself has parameters that specify the request and its result (i.e., the response to the desired request as specified by the parameters). Cooperation can also occur in the following forms:

1) Special applications that can work with the communications server;

2) Active objects that can work with the communications server and can be used in the client’s applications;

3) Files with requests that are recorded in a specific format or response files in a specific format;

4) A group of files (including even databases) for the requests and the responses;

5) Paper documents in an agreed format for requests and responses;

6) E-mail, which can be seen as a modification of items 3, 4 and 5 on this list.

It is commonly held that requests from a user can come in a dialogue regime from a human user and in an automated regime where the user is an application on the user’s computer.

There must also be plans to work in a synchronous regime (request-wait-response) and in an asynchronous regime (request-processing over a specific period of time-report to the user about the availability of a result-response), because this ensures more efficient work for the user and the communications server alike, especially when it comes to processing large and complex requests.

In work with the user thought must also be given to such aspects as the various levels of preparedness among users, the language of communication, the respective text coding formats, the abilities of the user’s computer equipment, operating systems and applications, and limitations in all of these things.

In other words, the main mission and, at the same time, the main problem that a communications server must handle is the way in which many different kinds of requests can be handled, submitting processed information from various information sources that sometimes are not compatible, and submitting a result to the user in the desired type and form.
Information about information

As the number of information sources available through the communications server increases, an overabundance of information can quickly occur – one in which even the administrators of the communications server can get lost. It is necessary to classify all of the information sources and the information that is contained therein, keeping firmly in mind that information sources can change.

Communications servers must have data source repositories that contain formal descriptions of the sources, their properties, the data that are contained within them and the properties of the data. These repositories must be very flexible, it must be able to change them easily and quickly so that changes in the surrounding environment can be monitored. If there is to be a proper reaction to user requests, other parts of the communications system must be able to adapt to changes in the repository in a dynamic way.

The repository is not, however, meant only for internal use in the communications server. The user, too, must know where and what he can receive (of course, within the limitations of the user’s authorization). This means that the communications server must also, so to speak, provide information about information. Using forms and terms that the user can understand, the server must describe the information that can be obtained and the ways in which it can be requested. There must also be efforts to link the various request formulation mechanisms as closely as possible to the repository, thus making easier the work of a user who takes advantage of the communications server’s services only seldom.

Users often don’t care where and how the desired information is stored. This means that the communications server must satisfy requests that concern information from many different sources. The repository, therefore, must also describe the links between the sources, as well as the ways in which various contradictions among the sources can be resolved, data be converted, etc. The repository must be an entity that makes it possible to consider all of the sources in a communications server to be one, big database.

The abilities of the communications server

A communications server is a dynamic system which must work in a highly changeable external environment. A communications server must be much more flexible and dynamic than a day-to-day system, because it must work with highly heterogeneous external information systems that keep up with rapid technological changes. When it comes to technologies, communications servers must be a step ahead of other systems, because otherwise it may turn out that the communications server ends up unable to perform its functions.

The goal of this paper is not to describe the internal architecture and ideology of communications servers precisely. The establishment of such systems is a very serious process throughout the world these days, and various solutions are being sought out that are linked to the following technologies:

- Distributed Dynamic Systems
- Distributed and Dynamic Objects
- Dynamic Object-Oriented Programming
Many of these technologies are still quite new, and they are still being developed. This means that not all of them have ready-made tools that support various properties or functions of the technologies. Some tools exist, some are at the prototype stage, while some have already become popular among professionals (this is particularly true of prototype tools that are designed at universities and research laboratories in order to test the latest technologies). In the design of a communications server it is worthwhile to such modern technologies and research results as the Multilanguage Interpreter and the Database Browser Generator.

**Evaluation of requests for billing purposes**

A billing system is part and parcel of the mechanism whereby a communications server fulfills requests. When a specific request is fulfilled, the system not only does what has been requested, but it also automatically calculates the resources that are used in the process. Within the communications server, a price has been attached to every resource, and it can change on the basis of the volume of information that has been requested, the time of day when the request is filed, etc. The price of each request is calculated automatically and stored in a journal that then is used for billing purposes.

A resource is an information request to a register. The price of resources changes on the basis of the type of the request, the complexity of the request, the register that is involved, etc.

**Uses of a communications server**

There are three major ways to use a communications server:

- As an international resource facility that can be used to access information from Latvian registers;
- As an internal resource facility that can be used to search for information in registers;
- As a way of setting up cooperation among various registers.

The need to access information from Latvian registers via a single contact facility is the main reason for elaborating the communications server. Of course, this is more than just a trivial solution in which a single Internet application is designed for connection to other registers via their Internet addresses. This simplified design does not deal with the main issue – the ability to collect information from various sources (i.e., various registers) without the user having to hook up to each register separately. The information that a user needs is collected from the various registers by the communications server, and the user himself may be completely unaware of the technical details of this process. Thus the communications server is needed by employees of foreign institutions in order to obtain information that is stored in Latvia’s registered.
A second use for the communications server is the fulfillment of domestic information requests in Latvia. The previously described situation in which users do not want to or are unable to understand the technical details of information storage is typical among the personnel of Latvia’s administrative structures. Of course, given the fact that access rights to authorization may vary for foreign users and Latvian users, the communications server sets out a unified set of requirements in this area, and solutions are the same for both groups of users.

The third way of using a communications server is to use it in order to exchange information among various registers. It is obviously irrational to maintain communications channels and to conduct information exchange individually with each of many registers that are mutually linked. It is much more rational to set up a centralized contact facility – the communications server – which is linked to all of the registers and through which information is exchanged among them.

Register can be connected to a communications server via different ways. Every register that participates in the data exchange procedure can have its own database in which those data that are intended for transfer to other registers and for publication can be separated out. The database can be maintained by a separate computer or server so that approaches to the public database do not hamper work with the basic database of the register. Data from the basic database are regularly copied to the public database (an automatic replication mechanism). This solution is rational not only from the perspective of using communications channels; it also ensures:

- That the fulfillment of external requests does not hamper the work of the register;
- That there is higher security, i.e., that in the case of unauthorized access, the basic database is not damaged.

The link between the communications server and the public database can be implemented on the basis of various technologies, such as DCOM object calls, MS Transaction servers and Oracle SQL*NET. User authorization is provided via a certificate server, a directory server and the Lightweight Directory Access Protocol (LDAP).