International Journal of Applied Engineering Research ISSN 0973-4562 Volume 10, Number 17 (2015) pp 38116-38120
© Research India Publications. http://www.ripublication.com

The Development Of Infrastructure Security For Distributed Information Computer Environment Based On Secured Portal Network

Igor S.Konstantinov, Sergej A. Lazarev, Oleg V.Mihalev

Belgorod State National Research University
85, Pobedy St., Belgorod, 308015, Russia

Alexander V.Demidov, Roman V.Shateev

State University– Education-Science-Production Complex
29, Naugorskoeshosse, Orel, 302020, Russia

Abstract

This article discusses the development of security infrastructure for a distributed information-computing environment, which includes the issues of subject horizontal integration solutions in respect of information exchange within the global information space by creating a secure virtual environment (information association), based on a distributed network of portals with a heterogeneous structure, functioning on the basis of open protocols.

Keywords: distributed information-computational resources, virtual protected environment, data access control, user authentication, data exchange, network portals.

Introduction

Information technologies are characterized by a wide development of forms and methods of different information presentation in the Internet. Over the past 20 years, the concept of "corporate portal" expressed by the means of successive software technology has established itself as a universal way of information presentation. A natural development of a corporate portal as the concept is a portal network with a single point of entry which provides a common access control policy for users and administrators. The network portals make an extremely flexible system that provides a universal approach to the management of information exchange. The concept of such a network is described in work [1] and represents a set of access control nodes, united in a single network through open Internet channels with a portal network management center (PNMC). A unified policy of information exchange management is implemented within PNMC, including the ability to secure the authorized access to information and computing resources throughout the network, a single mechanism for a user session control.

The additional complexities are developed by the impossibility to create a uniform policy of access distribution on a set of portals, as well as the implementation on various hardware and software base. The model which allows to solve these difficulties, in particular for gas transporting companies remaining within the concept, is considered in the work [2].

The development and expansion of the information exchange system within the network of portals is the development of technology for the building of closed virtual media in respect of the distributed information resource (DIR) organizations within a global network space based on open protocols, network cooperation and a secure user authentication.

The implementation of this project concept involves the use of standard protocols for secure information exchange (HTTP/HTTPS, OpenSSL), the adaptation of the standard software components based on open-source software provision (OSLinux, OpenLDAP, Nginx, Apache), and also the provision of operation with standard enterprise solutions for authentication (RADIUS [3], LDAP [4], ActiveDirectory [5]).

The central objective of an article is to develop the architecture of DIR security infrastructure as a secured network of portals, including the solution of horizontal integration issues for the subjects of information exchange in the global information space by creating a secure virtual environment (data association) based on a distributed network of portals with a heterogeneous structure.The solution of this problem is necessary to work out on the basis of open application layer protocols, which allows to simplify greatly the use of DIR for end users, as well as infrastructure operation (administration) provided that DIR is secured at a system level or the level above the system one built with the use of public key infrastructure [6].

Methodology.

The structure of DIR reveals custom domains. The user domain is a uniquely named group of users which is associated with one institution and and with one or more portals, which operates on the same hardware and software platform, has its own administrator, may have a privileged access to portal resources associated with an appropriate access server [7].

The control system identifies five key user roles:

1. Unauthorized users who may get the access the open sections of a portal.
2. Authorized users who may gain access to restricted sections of a port depending to which group ofaccess privilege level it is related. Users may belong to only one group of privilege access. The privilege groups have a strict hierarchy of subordination and

attachments, so the users belonging to the group with a highest priority, will have the access to all restricted sections with a lower priority access.

3. Access administrators determine which of the portal sections are open and which are closed and setting the levels of access privileges to the closed sections.
4. Domain admins develop the structure this access server portals. They may create, delete, modify user accounts and move them between the groups of access levels. They also perform the access system operation control and the calls to related portals.
5. Network Administrator creates and deletes domain groups, binds the domain groups with portals, appoints a domain administrator and allows the access to users of one domain group to other portals (it is a necessary but not sufficient access condition). He also performs the operation control of the whole network and data replication.

Architecture of DIRsecurityinfrastructure

The concept of a security infrastructure development for closed virtual organization environments involves the use of a three-tier architecture [1, 7-9] as a basic approach. Its framework offers the division of a software system model into three layers:

- presentation layer;
- application layer (middle layer);
- data layer.

The presentation layer (Figure 1) provides an interface with a user and contains the GUI components of a complex. This layer is presented with a simple software logic, responsible for the display of information and network interaction with an application layer.

A middle layer is presented by an application server containing the main program logic. Application servers are designed in such a way that the addition of additional copies to it provided a scaling performance of the software package without the requirement of changes to the application code.

A data layer includes the components of access to the sources encapsulating data storage mechanisms. Usually an application program interface (API) of data management acts as this data layer.

The implementation of this architecture imposes its own features on the selection, construction and interconnection of developed infrastructure components.

Mainpart.

Let's formulate the principles of the software package according to functional requirements. The tool for the set task performance is the architectural modeling language ArchiMate, developed on the basis of IEEE-1471-2000 standard for the architecture description of software systems [10].

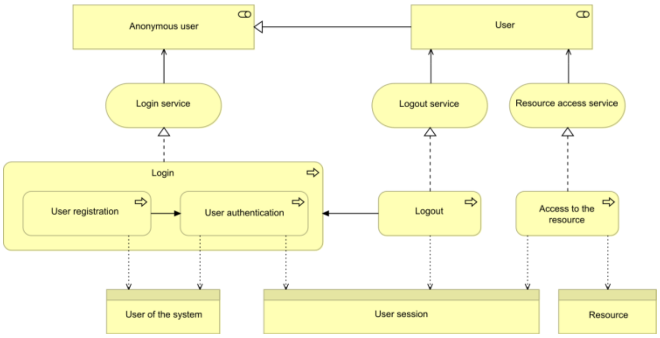


Figure 1 – General scheme of presentation layer

Short sequence of operations:

1 Resourcerequestinput;
2 Resourcerequestdispatch;
3 Resourcerequestacceptance;
4 The analysis of a request belonging to a specific user:

4.1 If a user is authenticated, the following aspects are necessary to check:

– a session key duration period;
– the compliance of user data with a session;
– the correctness of request data signature;

4.2 Otherwise, as in the case of errors during the inspections, it is necessary to perform:

– the development of a response with the authentication requirement;
– authentication form development by a user's name and password, the registration offer provision in a system;
– the analysis of power limitations to a requested resource:

4.3 If the user's access powers to a resource are confirmed, you shall do the following:

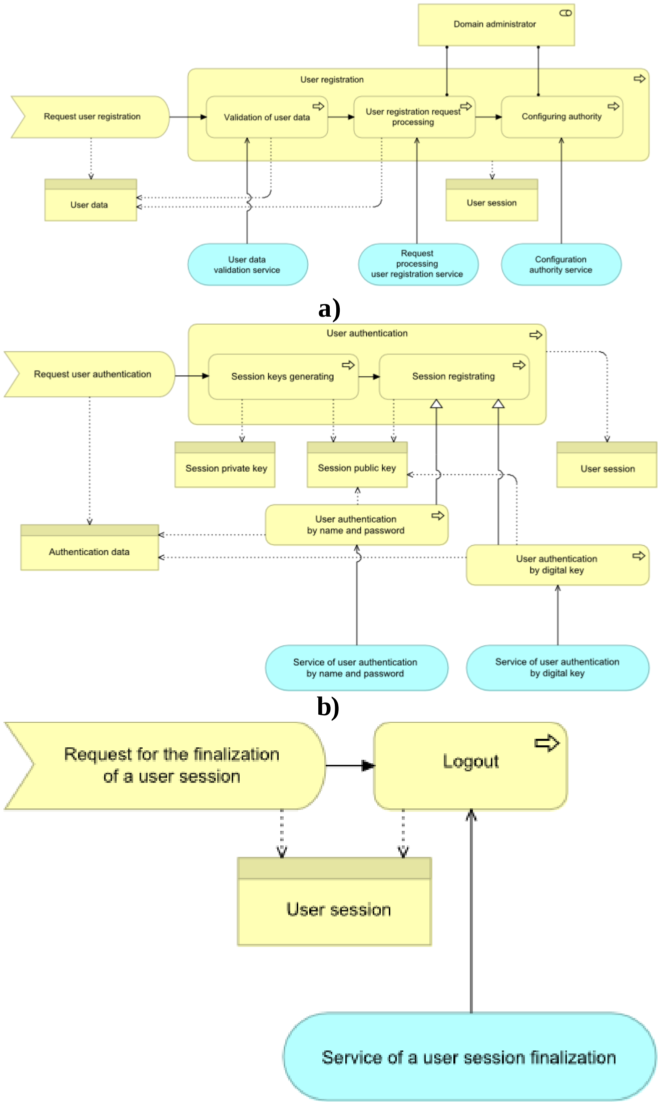
– protectedresourcerequest;
– the development of a response with a protected resource content;

4.4 Otherwise, it is necessary to perform the following:

– the development of a response with an error;
– anerrormessageoutput.

The registration of a user implies the establishment of a new record at an AAA server. A typical AAA server, being a heavily used component within the framework of the proposed concept raises a number of problems (performance, mobility, etc..) solved by researchers [11-13]. When the data are entered into a system an administrator shall activate an account - for these purposes an administration interface is defined at an application level, which allows to change configurations, user access rights and the access of protected resources.

Authentication and authorization is performed directly on the nodes that control the access for all network users. A session key is used as a public key certificate. Then it shall contain the necessary data of a user for each session, its public key, involved in the verification of resource request integrity, and the signature of the network node which generated authentication. Besides, a public key infrastructure, the services which are offered to take as a basic set of technical means, presupposes the existence of restrictions during the certificate validity period, after which it becomes an invalid one, and the ability to revoke a valid certificate.


Domain administrator
User registration
Request user registration
Validation of user data
User registration request processing
Configuring authority
User data
User session
User data validation service
Request processing user registration service
Configuration authority service
User authentication
Request user authentication
Session keys generating
Session registrating
Session private key
Session public key
User session
Authentication data
User authentication by name and password
User authentication by digital key
Service of user authentication by name and password
Service of user authentication by digital key
Request for the finalization of a user session
Logout
User session
Service of a user session finalization

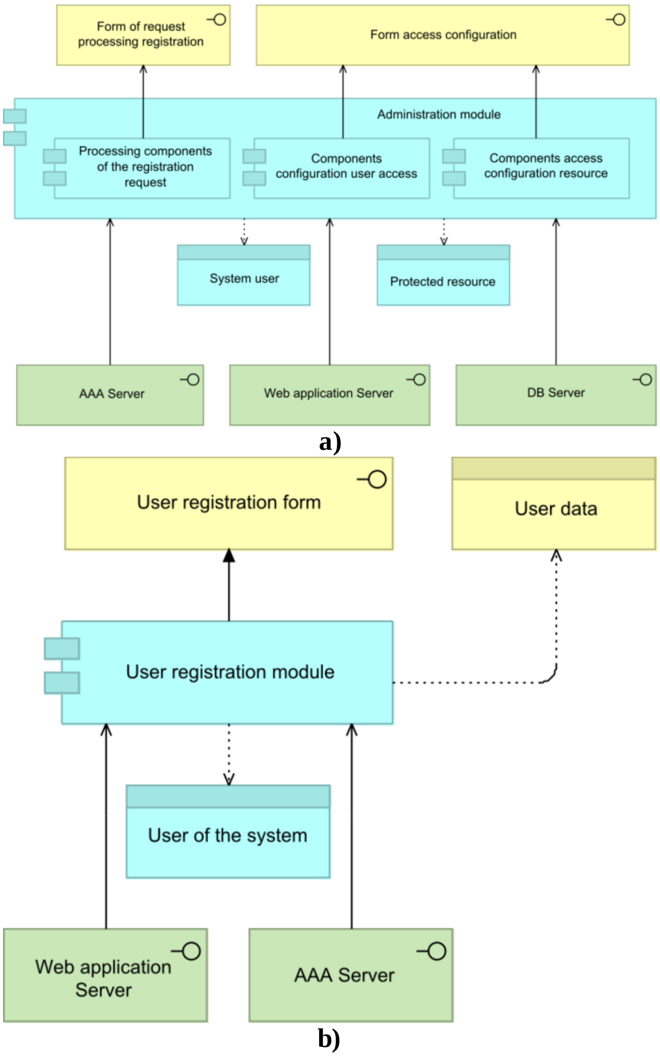
a)

b)

c)

Figure2 – Presentationlayerschemeofevents: a – new user registration, b – session initialization, c – session completion

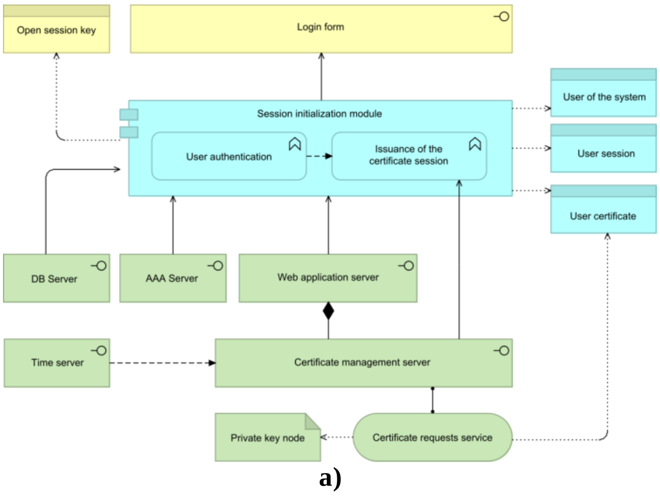
Separate access servers keep a user information of its domain group. A user domain implies a uniquely named user group that is associated with one corporate institution and one or more portals, it operates on the same hardware and software platform and may have a privileged access to the portal resources associated with an appropriate node. In the case of a user appeal of another domain group a network node may take a solution on the basis of trust policies between nodes [1, 9].



a)

b)

Figure 3 – Applicationlayerschemes: a – administration components, b – registration components



a)

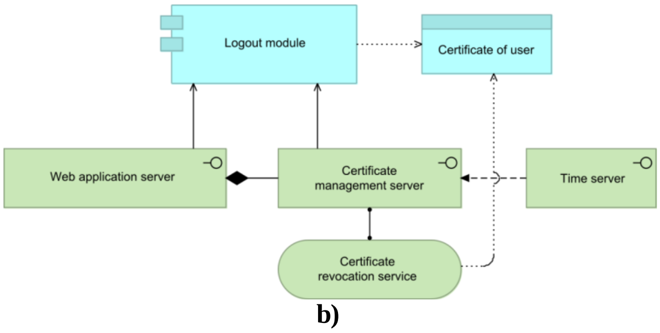


Figure 4 – Scheme of certificates and PKI application layer: a - session initialization, b - logout

Based on the concept of a developed infrastructure building in the course of the performed tasks and functional requirements analysis the main components were defined.

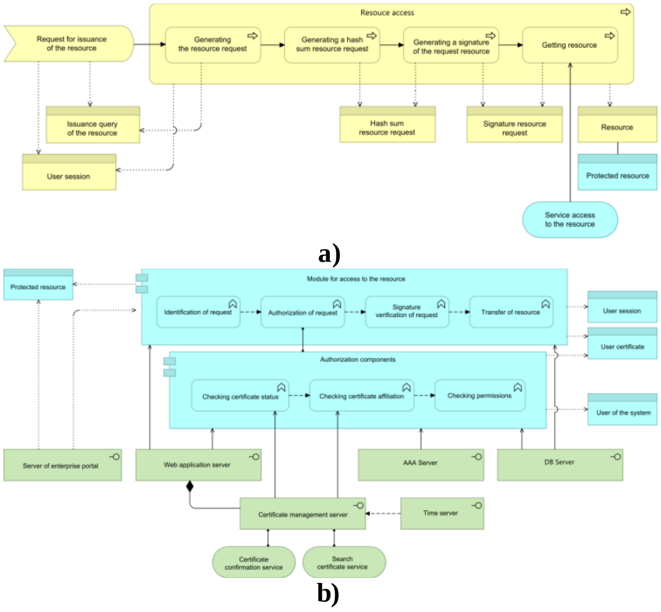

Resouce access
Request for issuance of the resource
Generating the resource request
Generating a hash sum resource request
Generating a signature of the request resource
Getting resource
Issuance query of the resource
User session
Hash sum resource request
Signature resource request
Resource
Protected resource
Service access to the resource
a)
Protected resource
Module for access to the resource
Identification of request
Authorization of request
Signature verification of request
Transfer of resource
User session
User certificate
Authorization components
Checking certificate status
Checking certificate affiliation
Checking permissions
User of the system
Server of enterprise portal
Web application server
AAA Server
DB Server
Certificate management server
Time server
Certificate confirmation service
Search certificate service
b)

Figure 5 – Resourcerequestauthorizationscheme: a – representation layer, b – application layer

The infrastructure components and their relations were identified during the development. It allowed to form a clear architecture of software and a design framework.

Summary

The main results of a study are new principles and approaches to the construction of a security system on the basis of a session key use with a period of action limited by this session to improve the system reliability from an unauthorized access, the use of signed hashes in order to avoid the substitution of DIR requests RIVS and transferred information content.

Conclusions.

According to the obtained results, it is suggested:

- to perform an analysis and an algebraic modeling [14, 15] of Web-service combination proposed in operation;
- to carry out the development of new scientific and technical solution complex in the field of software infrastructure provision for DIR security based on an application layer open protocols, which allow to simplify greatly the use of DIR for end users, as well as the operation (administration) of an infrastructures with the provision of DIR security at a system level or at the level exceeding the system one built using a public key infrastructure;
- the performance of research and development work for DIR security software prototyping.

Acknowledgements.
The research on this topic was sponsored by the RF Ministry of Education and Science, the project ID is RFMEFI57514X0099.

References

1 Lazarev, S.A., A.V. Demidov, 2010. The Concept of Construction of a Control System of an Information Exchange in TheNetwork of Corporate Portals. Information Systems and Technologies, #4(60): 123–129. (in Russian).

2 Demidov, A.V., 2013. Modeling of Access Control System of Gas Transportation Enterprise Portals. Proceedings of the International Conference on Intelligent Information Systems (IIS2013), pp: 210-214.

3 Remote Authentication Dial In User Service (RADIUS). Date Views 04.08.2015 www.rfc-editor.org/rfc/rfc2865.txt.

4 LDAP: Technical Specification Road Map. Date Views 04.08.2015 http: //www.rfc-editor.org/rfc/rfc4510.txt.

5 ActiveDirectory. Date Views 04.08.2015 technet.microsoft.com/en-us/library/bb727030.aspx.

6 Karamanian, A., Tenneti, S. and Dessart, F., 2011. PKI Uncovered: Certificate-Based Security Solutions for Next-Generation Networks. Cisco Press Networking Technology, pp: 272.

7 Lazarev S.A., O.A. Ivashchuk, I.S. Konstantinov, K.A. Rubcov, 2014. Mechanism of Information Exchange Management within Portal Network of Environmental Monitoring Subjects, International Journal of Applied Engineering Research, 9 (22), pp. 16789-16794.

8 Eckerson, W.W., 1995. Three Tier Client/Server Architecture: Achieving Scalability, Performance, and Efficiency in Client Server Applications. Open Information Systems 3(20).

9 Lazarev, S.A, I.S. Konstantinov, O.V. Mihalev, V.L. Kurbatov, 2014, Analysis of the single session access model in the distributed portal network of the interacting parties of the informational space,

Research Journal of Applied Sciences, 9 (11), pp. 771-773

10 ArchiMateCertification. Date Views 04.08.2015, URL: www.opengroup.org/certifications/archimate/.

11 Kim, M., Kim S. and Kong A.J., 2007. High performance AAA architecture for massive IPv4 networks. Future Generation Computer Systems, 23(2): 275-279.

12 Georgiades, M., Akhtar, N., Politis, C. and Tafazolli, R., 2007. Enhancing mobility management protocols to minimize AAA impact on handoff performance. Computer Communications. Special Issue: Emerging Middleware for Next Generation Networks, 30(3): 608–618.

13 Moon, J.S. and Lee, I.-Y., 2011. An AAA scheme using ID-based ticket with anonymity in future mobile communication. Computer Communications. Special Issue of Computer Communications on Information and Future Communication Security, 34(3): 295-304.

14 Rai, G.N., Gangadharan, G.R. and Padmanabhan, V. Algebraic Modeling and Verification of Web Service Composition. The 6th International Conference on Ambient Systems, Networks and Technologies (ANT-2015), the 5th International Conference on Sustainable Energy Information Technology (SEIT-2015), pp: 675-679.

15 Chashin, J.G., I.S.Konstantinov, S.A. Lazarev, 2014.Simulation of the software-defined network for a high-performance computing cluster, Research Journal of Applied Sciences, 9 (10), pp. 704-706.