DOI 10.20544/HORIZONS.B.04.1.17.P06
UDC 004.77.056.523

AUTHENTICATION OF USERS IN HETEROGENEOUS INFORMATION ENVIRONMENT[1]

Sašo Nikolovski MSc
University „St. Cyril and Methodius“ – Skopje
Faculty of Economics – Skopje
sasnik@gmail.com

ABSTRACT

The development of organizational information systems over a long period of time, often result in the creation and use of multiple independent information systems within the organization, which are on the other side mostly set in heterogeneous IT structure. By setting up these systems in this information structure, as one of the most important processes in the integration of systems in the foreground is outlined the process for authenticating users who have access to information. Given the complexity of this process in a heterogeneous information environment, within the paper we make a conceptual overview of key aspects for the design and application of the system for authentication.

Keywords: information system, authentication, CAS

INTRODUCTION

Modern living and working of people and business subjects, as a prerequisite for continued development and success have information, knowledge and its management. In this concept, information systems set on information structures are treated as a good basis for achieving a high degree of utilization of accumulated knowledge, both in organizational objectives and in service-service aimed direction for the needs of all users involved in the process of operation. Therefore, in order to obtain accurate information about users, modern trends of

[1] professional paper

using these systems often require the integration of information systems through an array of integration processes among which the most important is imposed the process for authenticating users. This primary position this process receives because of the possibility of selective and targeted distribution of information to targeted groups of users.

AUTHENTICATION IN INTEGRATED ENVIRONMENT

The process of building the security policy on a level of networking, in its coverage of the segments that make security policy reliable and stable for implementation may involve the use of several mechanisms for authentication and authorization of users of network resources. When considering network environment that contains multiple information systems, the expectation is that in it one can meet multiple systems for authentication and authorization of users. Depending on the level of safety that is demanded in each of the systems individually, but according to the rules and standards applicable to the information and data which they distribute to target groups of users, each of the information systems require a login in its authentication system with user name and password contained in its authentication system. The existence of a large number of information systems in a closed network infrastructure (organizational local information network), assume using of many usernames and passwords for user accounts that are authorized to use the information and data contained in each of them. The existence of multiple user names and passwords of users of network resources, entails a series of advantages, but also a number of weaknesses which basically directly affect the security policy with which they are introduced. Contrary to separate information systems with separate authentication systems for verifying the identity of users, the uniting of multiple information systems in an integrated information system, imposes different system of establishing security policy. Therefore, the abandoning of the concept of using multiple information systems as separate entities and the introduction of an integrated information system inevitably requires the introduction of a single sign-on system of users for accessing all information and data resources which it has at disposal and which are allowed for using to the user or user group to which it belongs.

The introduction of such an authentication system further imposes a series of dilemmas about:

- Which approach should one have when considering the options for a single sign-on of users?
- Will this system provide a high enough level of security in terms of selectivity of users in their access to information and data information systems?
- How to implement such a system in an environment that is already in use?
- And finally, how to define the ultimate benefit of designing and implementing such authentication system?

Proper consideration of the above questions and received answers to them give the direction in which one need to think about getting the authentication system that will fully meet the standards for the protection of the informations and data in the cycle of their use, or processing (when we are speaking of data processing, we mean the whole process of using data that is contained in the information systems).

When we say proper consideration of the issues, we mean examining them separately, but also checking their connection and dependence, because the whole process of decision making for using this authentication system contains an array of dependent conditions. For example, there is no doubt that the estimation of the ultimate benefit of introducing such a system for authentication, is directly dependent on the previous questions, but all of them in their basis as a common component have the actual state of the network infrastructure, that is the layout of the information systems in it.

Depending on the actual state of the network infrastructure, in practical implementations of the authentication systems with a single login for using the resources in one network infrastructure, more such systems can be seen (such as solutions that are free to use or commercial) which in its essence possess:

- A single login mediated through central authentication system CAS (*Central Authentication Service* – CAS) and
- A single login in a domain structure.

The introduction of a system for single login of users into the network infrastructure, regardless of the authentication system in question carries with it a range of benefits, but also some risks.

Consideration of the benefits from the introduction of such systems for authentication, usually are perceived by the user side through:

- Freeing users from remembering multiple user names and passwords for each system separately,

- By establishing a security framework that is implemented both on existing and new application solutions,
- Simplified management of user profiles and privileges that belong to their generic forming and joining the group of users for which they are formed.

Contrary to benefits and their belonging to the user side, the risks or anomalies (difficulties) of the introduction of these authentication systems are perceived primarily at networking system level, in the segment of safety and security at:

- Access of an unauthorized user to all network resources through a logged user in the system
- Possibility of abusing accidentally discovered user account and its password as the single point of attack to all network resources, and certainly
- The implementation of these systems imposes itself as a costly process, right because a number of changes that should be made to existing systems and application solutions for their full cooperation with this system.

But certainly, with proper and accurate configuration of the security policies within the organizations and institutions on the procedures for the use of network resources, from the perspective of users, administrators and developers of new application solutions, the benefits give primacy exactly to this system for authentication.

CENTRAL AUTHENTICATION SYSTEM – CAS

The process of verification of the authenticity of network users imposes itself as a complex problem. Information systems or information portals are bringing the need for identifying users in cases when they have a need of accessing background data sources through application solutions or through appropriate communication services. In such cases, each of the application solutions with appropriate structural arrangement, can be considered as an information system with its basic security infrastructure. In a presentation of one modern institution or working organization, at least two information systems can be seen (system for electronic mail and system for distribution and management of documents) where each of them has its own authentication system. During the introduction of information integration and at information level, it is realistic to expect that the new integrated IT structure, as the most efficient solution for authenticating

users imposes single login (*Single sign-on*) in order to obtain access to both systems.

Performing of an authentication process in a network environment with heterogeneous operating platforms in which there is no premium network authority (domain controller), as the most appropriate solution to meet the need for single sign-in using network resources raises the Central Authentication Service – CAS.

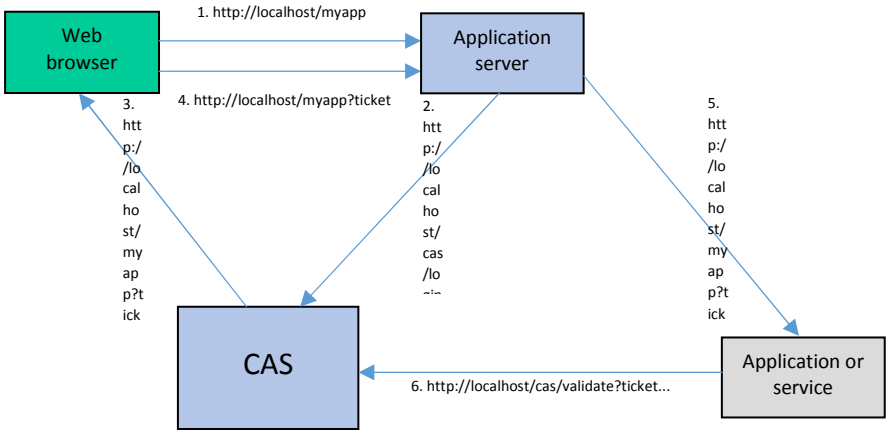

Figure 1. Concept of Central Authentication Service – CAS

CAS (Figure 1) in the process of authenticating users is treated as a tripartite system, involving at the same time in the process a web browser by the user, a web application that has a system for authenticating users and the CAS. It should be noted that the process of authentication with CAS takes place with so-called tickets which are generated by the CAS system, and the application or application service confirms them.

SINGLE LOGGING INTO THE DOMAIN STRUCTURE

When we talk about an integrated environment it should be noted that the existence of a hierarchical network infrastructure and the involvement of the central location for authenticating users, lays the foundation for building an

integrated information system with information infrastructure. The very existence of the highest hierarchical network authority in the network infrastructure, as well as the existence of a sub-system for e-mail, has already outlined a concept that should be followed when building a system for authentication in an integrated environment.

Namely, if it is known that the active directory of the highest network authority, the domain controller, store all user names and passwords for all users in the domain network infrastructure, then there is no doubt that building of the system for single sign-in in the computer network for using its network resources (including services of information systems) will be conducted with reference of this very network authority.

During the integration of information systems based on the platform or platforms from one vendor (eg. integration of *Microsoft* platforms), the process of performing the authentication of users for eachof the application solutions is carried out in a way that directly involves in communication exactly the domain controller. This statement is due primarily to application readiness of the platforms to perform authentication of users through the domain controller.[2]

But, in cases when we need to integrate information systems that are placed on different platforms from different manufacturers, single sign-on of users and their authentication in the integration of information systems opens up a range of issues, that further complicate the process of authentication. Namely, the use of the domain controller in such a heterogeneous environment in terms of platforms, requires complex customizations and changes of the existing application solutions. They include the development of special authentication modules for communication with the domain controller, resulting in obtaining a complex and expensive system for authentication in an environment that is already functional. In such cases, as a recommendation usually can be found the idea of implementation of CAS,[3] contrary to the idea of complex reworking and further complication of the process of authentication with the involvement of the domain controller in an environment that is not natural for its undisturbed

[2] J. Policelli, *Active Directory Domain Services 2008 How-To*, Sams Publishing, Indianopolis, 2009, p. 394.
[3] http://www.huque.com/~shuque/doc/2007-10-LDAP-Authn.html

operation.[4] Exception are the application solutions which include authentication modules implemented in the structure at its very design.

CONCLUSION

In attempts to introduce a level of cooperation between separate autonomous information systems, a key role have the degree of interoperability between systems and service orientation of the database for each of the systems separately.

The introduction of integration processes in systems which are heterogeneous at all levels due to the gradual introduction of information technologies in the process of using information systems (different operating systems, different development platforms of application solutions, different data platforms on which databases are placed), impose integration that provides a certain level of homogeneity, both at the level of data structures and systems for authenticating users. In such cases, the central database is established as a foundation for integrative connection of systems in the segment of getting integrated information from multiple data sources, through its service-oriented design, which on the user side results in a fast, stable and secure integrated information system. Regarding the security of the new information infrastructure, the authentication takes its primacy through authentication at the central level of all user groups. This involves the introduction of a single sign-on of users in the system and access to all services which are assigned to it by user group to which it belongs. This demand imposes using the system for central authentication of users or system for authentication through the domain authorites of information structure at which the information system is placed.

LITERATURE

1. H. C. Lucas, *Information Systems Concepts for Management*, McGraw-Hill, New York, 1978.
2. D. S. Linthicum, *Enterprise Application Integration*, Addison Wesley, 1999.
3. Joseph M. Firestone, *Enterprise Information Portals and Knowledge Management*, Elsevier Science, Burlington, 2003.

[4] As a natural environment of the domain controller is considered domain structure with network clients who are members of the domain and as such they accept the domain controller as a top (*Master*) supervisor in network infrastructure.

4. Madjid Nakhjiri, Mahsa Nakhjiri, *AAA and Network Security for Mobile Access*, John Wiley&Sons Ltd, West Sussex, 2005.
5. C. O□Dell, C. J. Grayson, *The Transfer of Internal Knowledge and Best Practice*, The Free Press, New York, 2008.
6. J.Policelli, *Active Directory Domain Services 2008 How-To*, Sams Publishing, Indianopolis, 2009.
7. W. Xiaoli, Y. Yuan, *XML-based Heterogeneous database integration system design and implementation*, Department of Computer Science and Engineering, Henan University of Urban construction, 2010.
8. J. R. Vacca, *Network and system security*, Elsevier Ltd, Burlington, 2010.