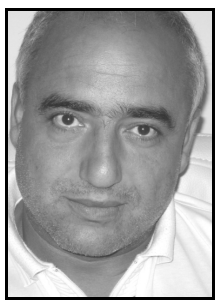
Imed El FRAY, Tomasz HYLA, Witold MAĆKÓW, Jerzy PEJAŚ
WEST POMERANIAN UNIVERSITY OF TECHNOLOGY, FACULTY OF COMPUTER SCIENCE, ul. Żołnierska 49, 71-200 Szczecin

Authentication and authorization in multilevel security systems for public administration

Ph.D. eng. Imed El FRAY



Graduated from the Department of Marine Technology, Szczecin University of Technology in 1993. In 1997 obtained PhD in the field of Marine Technology (specialty: Automatics and machine steering). Main research interests: risk analysis, trusted systems. Employed as Associate Professor at the Faculty of Computer Science and Information Technology, West Pomeranian University of Technology, Szczecin.

e-mail: ielfray@wi.zut.edu.pl

M.Sc. eng. Tomasz HYLA

PhD student of the Software Technology Department of the West Pomeranian University of Technology, Szczecin. He received M.Sc. degree in Computer Science and Engineering from the Szczecin University of Technology in 2007. His research interest includes: IT security applied to electronic health records (EHRs), security of long-term electronic archives and confidentiality in distributed systems.

e-mail: thyla@wi.zut.edu.pl

Ph.D. eng. Witold MAĆKÓW

W.Maćków (1974) received MSc title in 1998 and PhD title in 2007 from Faculty of Computer Science and Information Technology, Technical University of Szczecin (at present West Pomeranian University of Technology, Szczecin). His scientific interests include public key infrastructure application, long term archive systems, authenticated data structures, threshold secret sharing and still image steganography.

e-mail: wmackow@wi.zut.edu.pl

Ph.D. eng. Jerzy PEJAŚ

He received M.Sc. degree in Computer Science and Engineering from the Wrocław University of Technology and PhD degree in Control Systems from Gdansk University of Technology. Main subjects of interest: information and computer network security, methods of secure electronic signatures as well as new trends in applied cryptography. Employed as Associate Professor at the Faculty of Computer Science and Information Technology, West Pomeranian University of Technology, Szczecin.

e-mail: jpejas@wi.zut.edu.pl

Abstract

The article contains a brief survey of the different approaches to authentication and authorization in distributed systems and the new concept of the authentication and authorization based on multilevel security features. Proposed idea should be particularly useful in public administration systems. Such systems can consist of many separated subsystems with completely different authentication mechanisms. The goal of the paper was to develop a prototype of Authentication and Authorization System (AAS in short) to supervise access to the data applications operating in the information systems of public administration.

Keywords: authentication and authorization system, access control system, classified information, IT public administration systems.

Uwierzytelnianie i autoryzacja w wielopoziomowych systemach bezpieczeństwa dla administracji publicznej

Streszczenie

Artykuł zawiera krótki przegląd różnych metod uwierzytelniania i autoryzacji w systemach rozproszonych oraz nową koncepcję uwierzytelniania w oparciu o zabezpieczenia wielopoziomowe. Zaproponowane rozwiązanie powinno być szczególnie użyteczne w systemach informacyjnych administracji publicznej, które zwykle składają się z wielu podsystemów posiadających całkowicie różne mechanizmy uwierzytelniania i autoryzacji. W artykule zaproponowano taki sposób integracji tych mechanizmów, aby w zależności od poziomu uprawnień bezpieczeństwa podmiotu oraz wrażliwości danych możliwe było nie tylko kontrolowanie dostępu do tych danych, ale użycie różnych metod uwierzytelniania (np. uwierzytelniania wieloczynnikowego). Chociaż w systemach rozproszonych poziomy uprawnień bezpieczeństwa podmiotu oraz wrażliwości danych brane są pod uwagę tylko w procesie autoryzacji, realizowanego zwykle w oparciu o modele kontroli dostępu będące kombinacją modeli MAC i RBAC, w naszej propozycji przyjmujemy dodatkowo, że czynniki te powinny być brane po uwagę także w procesie uwierzytelnia i mieć wpływ na stosowane metody uwierzytelniania. Celem artykułu jest przedstawienie koncepcji prototypu systemu uwierzytelniania i autoryzacji (w skrócie SUA) nadzorującego dostęp do aplikacji działających w systemach informacyjnych administracji publicznej. Wymagania bezpieczeństwa dla tej klasy systemów są zapisywane w postaci dobrze sformalizowanej polityki bezpieczeństwa, uwzględniającej poziomy uprawnień bezpieczeństwa podmiotów zaangażowanych w wymianę danych, poziomy wrażliwości wymienianej informacji, a także własności (m.in. poziomy bezpieczeństwa) urządzeń stosowanych podczas przesyłania danych.

Słowa kluczowe: system uwierzytelniania i autoryzacji, system kontroli dostępu, informacja niejawna, systemów informacyjny administracji publicznej.

1. Introduction

IT systems of the public administration store and process information with various sensitivity levels. This information can be shared by different users or groups (e.g., clients or clerks of various departments) with various levels of security clearance. Therefore, it is obvious that information should be made available separately and access to it should substantially depend on user permissions. Selectivity of the access to information at various levels of information classification can be based on properly chosen methods of authentication and access control mechanisms. This means that access to certain information in the public administration network should be a subject of user identity confirmation, defined applications and rights assigned to him.

In practice, the selectivity of access to various levels of security clearance is often achieved by physically separating some applications/systems from the other in such a way that within one network are processed only the information of predetermined secrecy levels. This approach, although correct in some appropriate cases, is generally denial of the commonly accepted idea of separation of data, application and presentation layers. Applications of public administration (hereinafter referred to as domain applications) should work in a network and share common data and information stored in different databases. Presenting these data and information to users should be governed only by well-defined rules (e.g. access control policies) based on the information confidentiality level.

Obtaining the proper flow of various classification levels information is a difficult task even within a single domain system and usually requires the application of trusted class systems (e.g. Trusted Solaris operating system and Trusted Oracle database) and reliable interfaces (see e.g. [1]). Such systems have three major

disadvantages: they are expensive, applications must be very closely connected with the low level mechanisms of trusted systems and finally - it is difficult to ensure that these mechanisms cannot be circumvented in distributed systems, i.e. those in which applications are located on physically different servers and other networked devices.

2. Related works

Identification, authentication and authorization are key elements of the security subsystem in any computer system. These concepts are defined, for example, in ISO / IEC 9798-1 [2] and specify successive phases of decision-making process of accessing particular system resource by a specified entity. The problem has a number of consistent, safe and efficient solutions at the level of operating systems, database systems and server services.

There is noticeable tendency among the governments of many countries to place the public services on-line and integrate them into one system, avoiding thus the data redundancy and ambiguity. This requires the implementation of a coherent system of identity management and user authentication. The practical usage of multifactor authentication in environment of sensitivity classified information we can trace on the following examples (compare [4]):

- Austria: in use is "citizen card", which can be any device enabling digital signature and secure storage of personal data (cryptographic card, USB token, cell phone, etc.). In addition, as the second factor PIN code is used for the operations classified as potentially more sensitive.
- Denmark: the Danish government issued software tokens password protected. It was considered that this is a sufficient level of security for all citizens shared information and services.
- Estonia: for the identification of the citizens cryptographic identification cards are used. In addition to personal data they contain the appropriate cryptographic keys and certificates. Access to government services and selected e-commerce applications is possible after strong authentication.
- United Kingdom: a centralized system of registration and authentication called "The Government Gateway" supports secure access to government services via the Internet. Authentication is based on a password or a digital signature (four levels of the provided information sensitivity [3]). The digital signature is based on software tokens, but is planned to equip identification e-ID cards with the signing functionality.
- Unification of European identity management infrastructure was a goal of Interoperable Delivery of European eGovernment Services to public Administrations, Businesses and Citizens (abbreviated IDBAC). The program was conducted under the auspices of the European Commission in 2005-2009. The program set out, inter alia, reference model, requirements and ready to use the multi-level authentication mechanism [4]. The document identifies connections between the hazards, potential losses resulting from unauthorized access to resources and required authentication methods, and finally provides security classifications of authentication methods.

2.1. Authentication and authorization in heterogeneous systems

In the case of distributed systems, especially the heterogeneous systems, authentication solutions (having crucial importance for the whole process of resource sharing) are usually very complex. Most common solution is usage of authentication servers that mediate between the subject and the elements of a protected computer system. Such a server must be able to map the result of authentication on all constituent subsystems. Two AAA technologies (called Authentication, Authorization and Accounting) are worth discussing:

- RADIUS (Remote Authentication called Dial-In User Service [5]) and his successor Diameter [6].
- TACACS (Terminal Access Controller Access Control System [7]), modified by CISCO XTACACS (Extended TACACS) or its latest version TACACS + [8, 9].

Both technologies enable usage of different authentication methods but greater flexibility in this issue presents a TACACS +, where additionally authentication and authorization processes are strictly separated.

2.2. Various sensitivity data classification systems

Collecting and processing sensitive data imposes additional requirements on the functioning of the security subsystem. Most important requirements are: full mediation and full control over the information flow according to a predetermined policy. These requirements may be fulfilled by mandatory access control (MAC), mechanism based on the labeling of entities and objects and on protection model most adequate to the reported needs (for example Bell-La Padula privacy model [10]). Alternatively the role-based access control (RBAC [11]) could be use, which can model typical mandatory access control behavior, while giving much more flexibility during configuration and possibility of functionality extension thanks to public key certificates and attribute certificates usage. RBAC control, attribute certificates and X.509 certificates are effectively combined in the system PERMIS (Privilege and Role Management Infrastructure Standards [12]), which is dedicated to the management of user privileges in decentralized distributed systems.

2.3. Multi-factor authentication in single sign-on systems

Single sign-on is gaining increasing popularity in distributed systems. Such a mechanism allows for login to a single network service and maintenance of this authentication information within the whole complex system of loosely connected services and resources. If another service is consistent (mainly due to safety requirements) to the service, which was first seen, another login will be omitted. This approach call for clear definition of the required security levels for different services and resources and login methods differentiation. An example may be Oracle Single Sign-On server [13]. In such a system so called authentication level is defined for each service or application. The specified level is the numerical value, such as LowSecurity = 20, LowMediumSecurity = 30, ..., HighSecurity = 60. In addition to predefined values, we can operate on own values, what enable to diversify security levels more fluently. Specific authentication type or mechanism may be defined for each security level separately. At the time of the authentication attempt a plug-in is called (e.g. strong authentication with public key certificate or Microsoft Active Directory authentication services). Authentication at some level allows access to all services registered in a Single Sign-On server at levels equal to or lower.

2.4. Systems based on privilege management infrastructure

High expectations are associated with access control systems in which user authentication is based on public key and attribute certificates. Public Key Infrastructure (PKI) provides strong authentication mechanisms [12], while Privilege Management Infrastructure (PMI) complements the functionality of PKI by secure link between the user and authorization data (e.g., position, privileges). The combination of PKI and PMI allows to create secure access control system in which users are authenticated and authorized according to their certificates. The PKI certificates are used to bind the identity and the public key belonging to the owner of this identity. Attribute certificates, which are the main element of PMI, links the entity name and one or more privileges belonging to that entity (as attributes). There are several important reasons why attribute certificates and PKI certificates are issued separately:

- attribute certificates and PKI certificates can be issued by different certificate authorities;
- certificates validity periods may differ; PKI certificates are usually issued for one or two years; attribute certificates may

expire much faster, and in special cases may be drawn up to a very short period of time (e.g. one day);
- in case of attribute cancellation attributes certificates should be revoked only (e.g. due to privileges change), PKI certificate stays unchanged (there is no need to repeat whole complex process of user certification).

3. Goal

Our main idea was to design authentication and authorization system (AAS), which should meet at least the following requirements:
- authenticates users (entities) and the various active hardware and software elements involved in carrying out the functions of a specific application; used authentication methods should depend on the information sensitivity level made available to the user, or accessed through the active element;
- restricts and separates access for operators and other active elements (pre-defined secrecy levels); access granularity should depends on the actual needs and capabilities of AAS managed active elements (e.g. in extreme cases the level of granularity may be set on the level of entire database);
- prevents bypassing or substituting authentication and authorization mechanisms;
- enables effective evaluation of mechanisms and functions correctness provided by AAS.

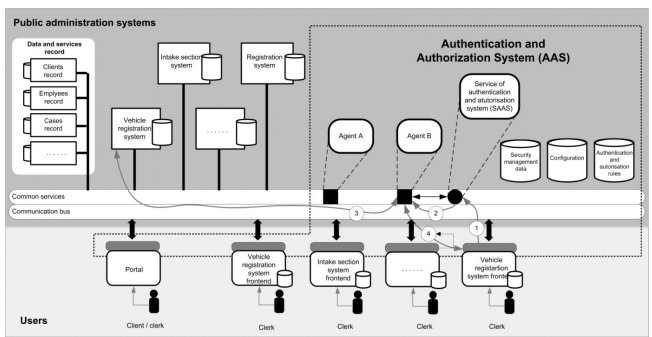


Fig. 1. AAS location in public administration system
Rys. 1. Położenie AAS w systemie administracji publicznej

AAS should be integrated with public administration network systems (see Fig.1) and should serve as a single point of access to public administration network resources. Such a solution should enhance security of existing network subsystems, which produce, process, store, access and transmit data of different sensitivity levels.

4. Main concept

4.1. Data classification

From the viewpoint of confidentiality two general information types may be distinguished - classified information and public information (e.g. classified information labeled "Top Secret", "Secret", "Confidential" and public information labeled "Sensitive" or "Public"). Usually, the classification label of information is expanded by adding a set of categories to each security level. The division of information into categories as well as the number of categories depends on many factors. Simple set of information categories may look like this [14]: a personal information category, a cryptographic information category, a nuclear information category, a logistics information category, a financial information category, other information category. A pair {security classification, information category} defines information secrecy level (also in AAS system).

4.2. Basic assumptions

It is essential that every AAS user, active device component or group of devices on the network (generally, an entity) has assigned the following certificates:
- a public key certificate necessary to verify signatures submitted by the entity in the authentication process;
- a public key certificate for encrypting data exchanged in the public administration system;
- a security certificate, issued in the form of an attribute certificate, specifying the maximum permitted levels of classified access to information stored on the network.

It is also assumed that access to specific network elements, especially network resources is possible through a properly defined and implemented network services. Services interfaces are divided into two groups:
- interfaces developed in accordance with the AAS specifications (AAS interface);
- interfaces that do not meet the AAS requirements, i.e. existing interfaces of applications found in the public administration network at the time of integration with AAS.

AAS interface requires installing appropriate software modules (access modules, see Fig. 1) on the user workstation and in an application domain. In the case of the existing interface access module is installed only on client workstation.

Set of different authentication and encryption methods is prepared for different types of entities (individuals, processes, equipment, etc.). The use of a particular method or methods depends on a security policy and an information security classification. Authentication and encryption methods are highly integrated with public key infrastructure services. As an alternative the certificateless authentication and encryption model is proposed.

Some example of the communication scenario might look as follows:
- *The user connects to AAS providing his ID and declared confidentiality level, which should be achieved after the authentication procedure (connection 1 in Fig. 1);*
- *In accordance to a declared confidentiality level and security policies AAS selects and executes a proper authentication protocol (based on* the *certificate attributes);*
- *After a successful user authentication, AAS system: (a) issues a user authentication token, which contains the authenticated user ID and confirmed user secrecy level and the token validity period, (b) creates an agent (connection 2 in Fig. 1), which will mediate any data exchange between user and domain applications working for him or her (user workstation is logically plugged into an agent, connection 3 in Fig. 1);*
- *The user runs the desired service; agent (who periodically checks the validity of the user token), issues and sends a confirmation of the token validity to the domain application (connection 4 in Fig. 1);*
- *Starting from this moment agent acts as an intermediary authorizing system for each user request (connections of 3 and 4 in Fig. 1).*

In the case when a domain application fails to meet the AAS, the agent forces an additional procedure of user authentication, implemented in a domain application. A user authentication always takes place only after the previous workstation authentication. Local stations and mobile devices should be equipped with authentication and authorization modules working in conjunction with AAS.

4.3. Proposed architecture

A generic AAS architecture is shown in the Fig. 2. Proposed architecture consists of following main components: the authentication and authorization services module, the mediator module, the access module, PKI and AA modules, the certificateless service module, keys, certificates and storage media management module.

Authentication and Authorization Service Module (module AASM) is a core of AAS. Any attempt to register within any administration domain systems (and use of a domain application) must go through it. AASM has complete information on registered users and applications used by them and is able to monitor the information flow between users and domain applications. The most important features of AASM module include:

- users identity management - entities registration (e.g. users, workstations) and information identity monitoring (e.g., unique IDs generating).
- users authentication - feature responsible for confirming the identity of the user; used authentication method depends on the declared secrecy level of accessed information and confidence to the user workstation; session token is generated as a result of proper authentication to the selected domain application;
- users and the information flow authorization – function responsible for permissions, roles, users and groups and for managing relations between them all; authentication of users and information flow in accordance to the defined access control policy and chosen access control models.
- data encryption/decryption management - function does not perform the encryption or decryption operations directly, but decide on the appropriate methods selection and allows to order their execution to relevant components of AAS.
- digital signatures management - a function responsible for signing and signature verification during entities and/or information authentication or during documents signing and non-repudiation verification.
- safe logging and events monitoring in AAS - AAS records in the event log all required and executed operations, administration events and security-related events;
- auxiliary support functions - database and cryptographic hardware modules management.

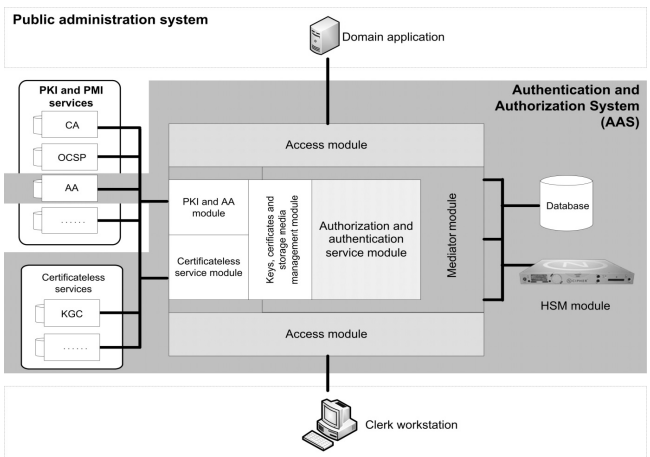


Fig. 2. Basic components of the Authentication and Authorization System (AAS)
Rys. 2. Podstawowe komponenty Systemu Uwierzytelniania i Autoryzacji (SUA)

Mediator Module is a service created and provided by AASM for handling transactions between the successfully authenticated user and the domain application of public administration system. This module, in cooperation with the access module and AASM, forces an additional authentication to the domain application (only if the domain application does not support AAS interfaces), permits the exchange of information between the entities of the same or different secrecy levels and forces the use of different encryption methods tailored to the secrecy level.

Access Module is the interface between the domain system and AAS and it is necessary for these systems integration. The main task of this module is to convert information between formats comprehensible for AAS and domain systems. Access Module can support one of two interfaces defined in AAS: existing interface of domain application and the AAS compatible interface.

Attribute Authority is a system whose primary function is issuing entities attribute certificates (not only for users) and their distribution and revocation. These features are available as a request/response service.

PKI and AA Module mediates the exchange of information between certification authorities and privileges management infrastructure. The service of attribute certificates issuing and revoking is an internal part of AAS. The other PKI and PMI services are provided by external actors and made available through this module.

Certificateless Services provide certificateless authentication and encryption mechanisms, as an alternative to PKI based mechanisms. The main component of this subsystem is Key Generation Center (KGC), which role may be compared to the role of a certification authority in PKI-type systems.

Certificateless Service Module enables cooperation of Authentication and Authorization Service Module with Certificateless Services.

Keys, Certificates and Storage Media Management Module is responsible for controlling of configuration changes in passive and active resources (keys, certificates, algorithms.

5. Summary

Consistent authentication and authorization access strategies to information in the public administration systems with different levels of secrecy should be implemented due to the existing threats. In this paper is proposed AAS system designed to fulfill such requirement and which is composed of three mechanisms: a mechanism of multi-factor and multi-level authentication, a mechanism of multi-level authorization and a mechanism of multi-level encryption/decryption. These mechanisms are applied to individuals, processes and to equipment and are intended to protect the access to information and equipment with different secrecy levels. Also, they are intended to control the information flows in public administration systems.

The most important part of the ASS is a usage of many authentication levels, many authorization levels and first of all, the supervision of information flows with different levels of secrecy between different network elements and public administration' applications. Such approach should allow to realize different strategies of entities authentication and access authorization to information in public administration systems. In particular the advanced method and cryptographic mechanisms would be used (e.g. hierarchical ID-based encryption [15]).

6. References

[1] Stallings W.: Data Protection network and internet work. WNT, 1997.
[2] ISO/IEC 9798-1:2010. Information technology - Security techniques - Entity authentication - Part 1: General, 2010.
[3] Registration and Authentication, e-Government Strategy Framework Policy and Guidelines. Office of the e-Envoy. Version 3, 2002.
[4] IDABC European eGovernment Services eID Interoperability for PEGS, for a multi-level authentication mechanism and a map-ping of existing authentication mechanisms, 2007.
[5] Rigney C.: Remote Authentication Dial In User Service (RADIUS), RFC 2865, 2000.
[6] Nelson D.: Common Remote Authentication Dial In User Service (RADIUS). Implementation Issues and Suggested Fixes, RFC 5080, 2007.
[7] Calhoun P.: Diameter Base Protocol, RFC 3588, 2003.
[8] Finseth C: An Access Control Protocol, Sometimes Called TACACS. RFC 1492, 1993.
[9] Carrel D.: The TACACS+ Protocol, Version 1.78, RFC Draft, 1997.
[10] David Elliott and La Padula, Leonard J.: Secure Computer Systems: Mathematical Foundations, Bell, 1973, MITRE Corporation.
[11] Ravi Sandhu, Ferraiolo David, Kuhn Rick. ANSI INCITS 359-2004. American National Standard for Information Technology – Role Based Access Control, 2004.
[12] Chadwick David W., Alexander Otenko: The PERMIS X.509 role based privilege management infrastructure. Future Generation Computer Systems, Vol. 19, Issue 2, February 2003, pp. 277-289.
[13] Vinaye Misra: Oracle Application Server Single Sign-On Administrator's Guide. 10g Release 2 (10.1.2), Oracle, 2005.
[14] Polkowski K.: Information Security in Poland, Part I (in polish), Ochrona Mienia i Informacji, No 6, pp. 17-19, 2009.
[15] Hengartner, P.: Steenkiste Exploiting Hierarchical Identity-Based Encryption for Access Control to Pervasive Computing Information, Proc. of the First Int. Conf. on Security and Privacy for Emerging Areas in Communications Networks, SECURE-COMM, pp. 384 – 396, IEEE Computer Society, 2005.

otrzymano / received: 14.05.2010
przyjęto do druku / accepted: 02.07.2010 *artykuł recenzowany*