Journal of Danubian Studies and Research

The Role of Digital Certificates in EGoverning. The Case of the Romanian Regulation and Surveillance Authority

Senior Lecturer Andra Marin, PhD Candidate
"Mihail Kogălniceanu" University Iași,
University of Bucharest, The Doctoral School of the Faculty of Law
andra_ma@yahoo.com

Abstract: The implementation of electronic governance related projects implies user authentication, accounts activation and personal data verification. Certain public services, particularly those involving financial transactions or statements, require a high security level. The use of the PKI technology and, consequently, of digital signatures, constitutes the most viable solution, meeting the required security standards, protecting, on the one hand, the signatory's identity, and, on the other hand, the integrity of the transmitted message. Due to the use of the digital certificate, the development of online public services is now possible, especially since it meets the requirements of security standards, but also because it is highly trusted by users. This article intends to analyze the impact of the digital certificate on the improvement of *communication* between state authorities, including specific transactional relations, and also to consider its influence on security improvement of *dataflow*. The study demonstrates that the digital certificate is closely connected to the information society, directly determining the dynamics of the development of new applications that provide a better interface between the state and its citizens.

Keywords: electronic governance; public services; *communication* between state authorities

1. Introduction

The information and communication technology has demonstrated its capacity to transform the way business relations function, the manner in which the public administration operates and it has a significant impact on scientific research, being an extremely promising business of the foreseeable future. (Vulkan, 2003, p. 20) In a constantly changing society, the ability to adapt to the opportunities provided by the Internet and to the new technologies, but also to new challenges, is crucial. (Greenstein & Vasarhelyi, 2002, p. 102) The rapid development of the information society entails the adoption of rigorous strategies, designed to revolutionize the interaction between the state and the citizen, to transform the manner in which public services are provided and in which the state institutions function.

Virtual space, banking and all other electronic services have become a common space that provides the convenience and the flexibility of non-stop availability, 24 hours a day, from the comfort of our own homes. However, a certain degree of mistrust still exists, both from private users, as well as from economic agents and organizations of any type, regarding the security of information and of transactions. (Germain, 2003) Encryption of information is insufficient, since it does not offer data that could ensure the identity of the sender or the integrity of the message (of the encrypted information). Digital certificates have managed to overcome these shortcomings of previously used technologies, being able to ensure higher security levels, guaranteeing the electronic identity and the integrity of the transmitted message.

This article brings into question the possibility of introducing digital certificates in the G2G functional relations. Three scenarios are suggested for approaching the problems that arise in case the Regulation and Surveillance Authority should become the guarantor of electronic identities of state institutions.

We intend to bring to your attention a review of the digital certificate characteristics, to briefly analyze the Romanian legal framework and to finally address the three scenarios suggested for the implementation of the concept of electronic identity in the context of G2G relations.

2. Digital Certificates

A digital certificate contains information about its holder (name, email address, date of issue and expiry), a public key of PKI architecture (public key infrastructure) of the document holder, as well as the electronic signature of the Certification Authority.

Digital certificates link the holder's identity to the public key-private key pair. The ensemble consisting of standards, procedures, protocols and software that supports the digital certificate constitutes the public key infrastructure (PKI). The public and the private keys are connected through complex mathematical algorithms that ensure the security of the private key, given that the public key is available to anyone, and together they are engaged in the encryption - decryption and message integrity verification processes. The pair of keys can be inscribed on any type of special device, from hard disks to smart cards and even floppy disks.

Digital certificates can be separated into two main categories:

- *Simple certificates* are used when wishing to guaranty the integrity of signatory's data, to encrypt the transmitted information, the authentication of the signatory not being of a major importance as long as the data integrity is not corrupted.

- *Qualified certificates* meet the three qualified electronic signature requirements: the proof of signatory's identity (non-repudiation), data integrity and data transmission security. Besides the voluntary use of these certificates, in the business environment, qualified digital certificates are necessary for lodging tax returns to NAFA, for participating in auctions through the e-procurement system, for accessing online services offered by public institutions and for time stamping documents.

Increasingly more state institutions provide improved electronic public services that require authentication on the basis of digital certificates: the National Agency for Fiscal Administration, the Romanian National Health Insurance House, the National Trade Register Office, the Territorial Labor Inspectorate, the National Securities Commission, the Official Gazette, the Private Pension System Supervisory Commission, the Electronic Procurement System Authorities etc. We specify that all these relations fall within the functional G2C (Government to Citizen) or G2B patterns (Government to Business).

Furthermore, the digital certificate can be used in official correspondence with business partners or even within the same company. The digital certificate has a personal character, and the accredited Romanian certification authorities offer one year validity, with the possibility of renewal.

3 Types of Authentication

Digital certificates help verify the identity of a sender, i.e. they certify that the sender has received, in an authorized manner, a key that cannot be falsified within the context of identity theft, for example. Used in conjunction with encryption, the digital certificate provides a viable security solution, protecting the identity of all parties involved in an electronic transaction.

The digital certificates are issued by certification authorities (CertSign, DigiSign, TransSped, AlphaTrust, CertDigital, Isign[1]) and are signed with a private key. The

[1] The Registry of Certification Service Providers, available online on the Ministry of Communication and Information Society site, http://www.mcsi.ro/Minister/Domenii-de-activitate-ale-MCSI/Tehnologia-Informatiei/Servicii-electronice/Semnatura-electronica/12-Registrul-FSC---V-15

most commonly accepted format of digital certificates is defined by the X.509 standard.[1]

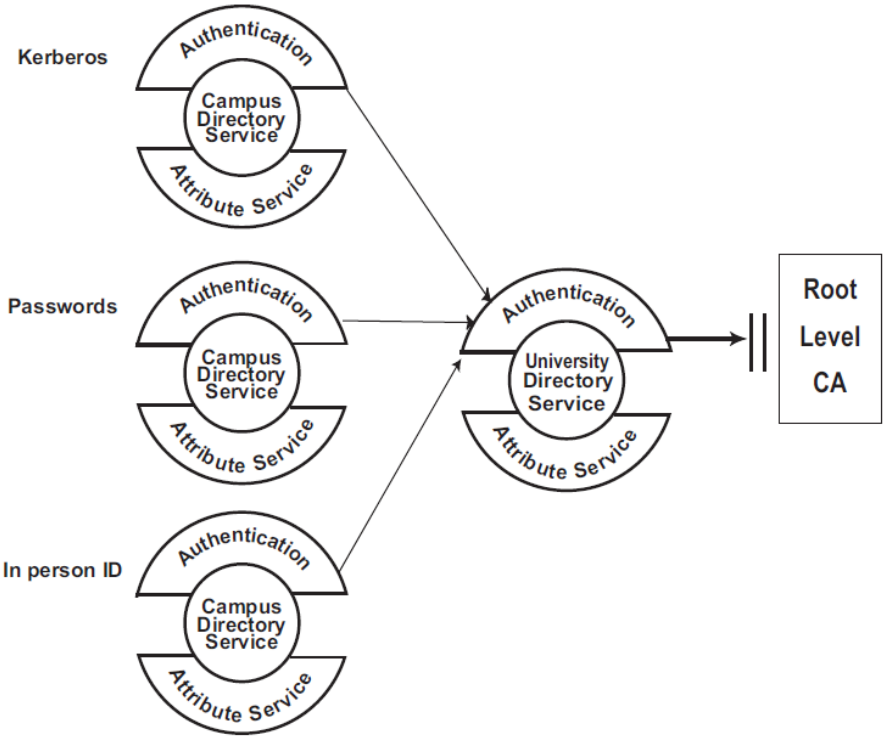

Figure 1 shows various ways to control access to services offered by a university server: Kerberos[2], passwords and authentication with identity cards.

Figure 2 illustrates the authentication process based on the digital certificate. Access is generally done through the server's web interface. The server requires

[1] According to technical and methodological norms of December 13, 2001, for the implementation of Law no. 455/2001 regarding the electronic signature, Art. 46, with subsequent amendments; The first version of X.509 standard was created in 1993 and has subsequent versions. In normative acts, the X.509 standard refers to the latest version at a given time.

[2] Kerberos is a secure method for authenticating a request for a service in a computer network. Kerberos was developed in the Athena Project at the Massachusetts Institute of Technology (MIT). The name is taken from Greek mythology; Kerberos was a three-headed dog who guarded the gates of Hades. Kerberos lets a user request an encrypted "ticket" from an authentication process that can then be used to request a particular service from a server. The user's password does not have to pass through the network. A version of Kerberos (client and server) can be downloaded from MIT or you can buy a commercial version.

the certificate. The client presents the certificate and the server checks the client's identity and the authenticity of the certificate, thus authorizing access to content[1].

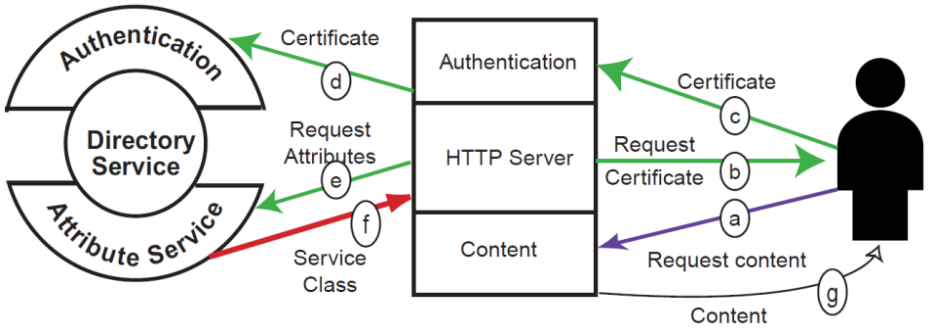

Figure 2. The authentication process based on the digital certificate

This type of authentication is widely used, fact which justifies the interest of state authorities to facilitate the functioning of large-scale secure online public services.

Another well-known application of the public key encryption technology is **Secure Socket Layer (SSL)**, which protects the communication channel. In everyday life people access commercial sites in order to buy goods, and want to benefit from secure data communication sessions during which financial transactions take place, so that the credit card codes, for example, could not be intercepted. A typical SSL session is presented in Figure 3. and consists of:

[1] DLF & CREN (2000) *Digital Certificate Infrastructure: FAQ*, Digital Library Federation & Corporation for Research and Educational Networking, available online at http://www.diglib.org/architectures/cren-dlf.pdf, last accessed in February 2012.

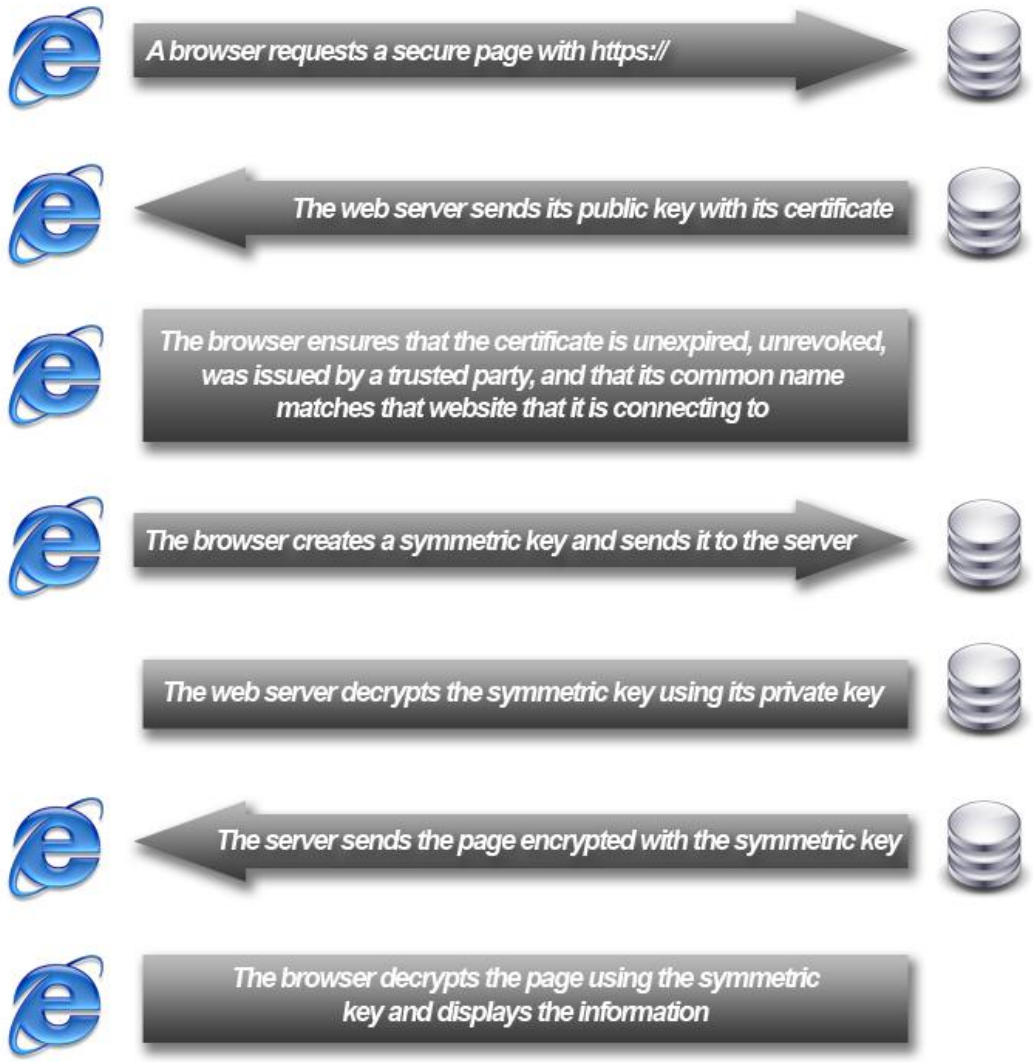

Figure 3. A typical SSL session

- a browser requests the connection to a server that uses a technical digital certificate. The link of the site indicates this by the "https" address type;
- the server responds by providing the certificate;
- the browser verifies the digital signature using the server's public key; the website's address is also verified using the certificate. This process is called the server authentication;

- optionally, the server may require the client's certificate, in order to verify access rights;
- the verification of this certificate is based on the client's public key;
- the browser generates a symmetrical key, in order to encrypt communication between the two;
- communication is then encrypted ("locked") using the server's public key, so that only the server can decrypt the message, using the corresponding private key.

Secure Shell (SSH) allows access to a computer terminal located in the network using a tunneling mechanism, which aims to transmit private data via public networks, protected by encapsulation.

IPSec is a protocol that uses symmetric key encryption between authenticated partners, providing the advantage of higher speed.

Secure MIME is a standard used for digitally signing electronic messages that contain attached files. The electronically signed messages present all the known advantages (user hash algorithms confidentiality, confidentiality through the use of encryption, non-repudiation and authentication by using the X.509 infrastructure of the PKI).

4. A Brief Survey of Legal Framework with Respect to Electronic Signature and Digital Certificate

Law no. 455 of July 18, 2001[1] regarding the electronic signature and Law no. 451/2004[2] regarding temporal marking establish the necessary legal framework. In December 2001[3] the technical and methodological norms for the implementation of Law no. 455/2001 had been approved, regulations that were subsequently modified by Government Decision no. 2303 of December 14, 2004 (the tendency of explaining the technical standards within the text of the normative act entails the necessity of constantly elaborating legislative amendments and modifications, dictated by the dynamics of information technology).

[1] The Law regarding electronic signature - 455 / 2001, Published in the Official Monitor no. 429/2001.
[2] The Law regarding temporal marking no. 451/2004, Published in the Official Monitor, Part I no. 1021.
[3] The technical and methodological norms for the implementation of Law no. 455/2001 on the electronic signature – Government Decision 1259/2001, modified by Government Decision 2303/2004.

In addition, we briefly mention other laws that complete the picture of authorized electronic relations in Romania: the Law regarding the legal status of the electronic notary activity[1], the Law regarding the archiving of electronic documents 135/2007[2], the Law regarding the electronic recording of commercial transactions 260/2007[3].

According to the technical norms for the implementation of Law 455/2001, any person, natural or legal, while on Romanian territory can benefit of certification services in order to use the electronic signature.

However, in 2001, the activity of issuing digital certificates, already having a clear legal framework, could still not begin because of the lack of the specifications regarding the Romanian Regulation and Surveillance Authority, the entity that practically authorizes and audits, on periodical bases, the certification authorities that, in their turn, issue the certificates.

In July 2008, according to the declaration of the DigiSign Director, Daniel Pestina, there were approximately 50.000 owners of authentication electronic signatures.

It was only in June 2009, when, through Ministerial Order no. 473, the procedure for granting, suspending and withdrawing accreditation decision of certification service providers is set. It should be noted that this normative act undergone subsequent amendments and completions in 2010 and 2011[4].

Article 1 already establishes that the regulatory and supervisory authority specialized in this field is the Ministry of Communication and Information Society that establishes the procedure for granting, suspending and withdrawing accreditation decision of certification service providers. One of its attributions is to establish and update the Registry of Certification Service Providers and to protect, by making records under the Law. 455/2001 on electronic signature, the

[1] The Law regarding the legal status of the electronic notary activity - 589/2004 Published in the Official Monitor no. 1227/December 20, 2004.
[2] The Law regarding archiving of electronic documents 135/2007 - Published in the Official Monitor no. 345 of May 22, 2007
[3] The Law regarding the electronic recording of commercial transactions 260/2007 - Published in the Official Monitor, Part I no. 506 of July 27, 2007 – Abrogated by Government Ordinance 190/2009.
[4] Ministerial Order no. 1000 of October 26, 2010 for the amendment and supplementing the Order of the Minister of Communication and Information Society no. 473 of 2009 regarding the procedure for granting, suspending and withdrawing accreditation decision of certification service providers
Ministerial Order no. 888 of September 5, 2011 for the amendment and supplementing the Order of the Minister of Communication and Information Society no. 473/2009 regarding the procedure for granting, suspending and withdrawing accreditation decision of certification service providers

identification data and information regarding the certification service providers storage, as well as to inform the public on the stored data and information.

4.1. The Authentication through Digital Certificates in the Case of G2G Relations

The purpose of this discussion is the need of state institutions' authentication through digital certificate infrastructure, with regard to G2G relations and transactions.

The questions that arise are:

- Who will be recognized certification authority for this type of identity?
- Will the public institutions' certification authority coincide with the authority certifying the identity within the private sector?
- Will the regulation and surveillance authority redundantly be authenticated by the use of a digital certificate by the certification authorities that it supervises?

3.1 Scenario no. 1 – the same certification authorities recognized in Romania provide digital certificates to the private, as well as to the public sector.

Since certification authorities operating in the private sector have already invested in necessary infrastructure and have complied with the requirements imposed by law and are monitored by the Ministry of Communication and Information Society, in its capacity of supervisory and regulatory authority, the easiest conclusion would be that state institutions should not be concerned with this matter and submit to the already existing mechanism in the private sector. This scenario, however, does not sufficiently reflect the national interest and does not ensure the security of information, altering the institutional hierarchy established by law.

3.2. Scenario no. 2 – the existence of distinct certificate authorities for the public and private sectors

These two types of certification authorities could function independently and simultaneously, having an equal level of authority, in terms of certificates' qualification. The obvious disadvantage – as shown above – is the need to invest in PKI infrastructure, so that it could ensure the recognition of the certificates issued by authorities that are not part of the national system of identity management. Furthermore, the necessity of national legislation updating becomes a sine qua non condition, in order to implement such a strategy.

3.3 Scenario no. 3 – hybrid systems of certification authorities

The third scenario implies the state's ability to provide limited PKI services, concerning the **issuance** of identity digital certificates and of e-government certificates, without giving private certification authorities the responsibility of integrating them in the already existent general infrastructure. The technical details related to the implementation of such system are not the object of this study; however, we express our opinion that this mechanism could provide the best solution for the time being.

4.2. The Government Public Key Infrastructure

By definition, the certifying authority is the institution that should cumulatively fulfill the characteristics resulting from Art. 20 of Law 455/2001 regarding the electronic signature and the issuance of digital certificates. Regarding certification, there are two types of certificates – personal and technical. The personal certificates are issued in order to certify the identity of a natural or legal person, while the technical certificates authenticate different components of the PKI infrastructure: web servers, administration tools, network applications etc. There are several other items that complete the picture of society informatization: the temporary stamp, the servers of certification authorities, the infrastructure administration applications.

For issuing digital certificates for state institutions, a new certification authority, directly subordinated to the Regulation and Surveillance Authority, could administrate the newly created identities. Subsequently, however, it may recourse to an existing certification authority, in order to integrate these identities in the PKI infrastructure. Practically, the application for a personal or technical certificate is addressed to this specially created certification authority, subordinated to the Ministry of Communication and Information Society that afterwards issues the certificate through a commercial certification authority. The entire authentication process is thus doubled, the mutual authentication being performed through the set of encryption protocols invoked (for example SSL, SSH, etc.) to a higher level of guaranteeing transaction security.

The number of certificates issued in this manner will be much smaller than the traditionally issued certificates, designed for the private sector.

The digital certificate validation is an important element associated with the confidence enjoyed by PKI infrastructure[1]. The Regulation and Surveillance Authority will be self-reliant, not having to comply with the classical trust route used for certification in the private sector[2]. The certificate issued by this authority will be installed simultaneously with the associated commercial certificate. In the case of state institutions that will be using such a digital certificate, the public key of the Regulation Authority will function as a root key and will be made public so that anyone could have direct or on demand access to it.

5. Conclusions

This article presented several scenarios for the use of digital certificates in G2G relations. In the short term, The Ministry of Communication an Information Society, in its capacity of regulation and surveillance authority, could partially extend its activity by becoming a certification authority that would partially function according to the general requirements of certification authorities, performing only that part of the services relating to the client identity verification and to certificate issuance. For any other associated services, it may appeal to the commercial certification authorities under its supervision.

6. References

Germain, J.M. (2003). Beyond Biometrics: *New strategies for security, E-Commerce Times,* available online at http://www.ecommercetimes.com/perl/story/31547.html, date: February 10, 2012.

Greenstein, M. & Vasarhelyi, M. (2002). *Electronic Commerce: Security, Risk Management and Control*. New York: McGraw-Hill, p 102.

Vulkan, N. (2003). *The Economics of E-Commerce: A Strategic Guide to Understanding and Designing the Online Marketplace.* Princeton University Press, p. 5-25.

DLF & CREN (2000). *Digital Certificate Infrastructure: FAQ*, Digital Library Federation & Corporation for Research and Educational Networking, available online at http://www.diglib.org/architectures/cren-dlf.pdf, date: February 2012.

The Registry of Certification Service Providers, available online on the Ministry of Communication and Information Society site, http://www.mcsi.ro/Minister/Domenii-de-activitate-ale-

[1]Mohapatra, P.K. *Public Key Cryptography*, ACM Crossroads Student Magazine, 2001, available online at http://www.acm.org/crossroads/xrds7-1/crypto.html, last accessed in February 2012.

[2] Riedl, R. *Rethinking Trust and Confidence in European E-Government. Linking The Public Sector with Post-Modern Society*, IFIP International Federation for Information Processing, 2004, Volume 146/2004, 89-108

MCSI/Tehnologia-Informatiei/Servicii-electronice/Semnatura-electronica/12-Registrul-FSC---V-15, date: February 2012.

The Law regarding electronic signature - 455 / 2001 – Published in the Official Monitor no. 429/2001.

The Law regarding temporal marking no. 451/2004 Published in the Official Monitor, Part I no. 1021.

The technical and methodological norms for the implementation of Law no. 455/2001 on the electronic signature – Government Decision 1259/2001, modified by Government Decision 2303/2004.

The Law regarding the legal status of the electronic notary activity - 589/2004 Published in the Official Monitor no. 1227/December 20, 2004.

The Law regarding archiving of electronic documents 135/2007 - Published in the Official Monitor no. 345 of May 22, 2007.

The Law regarding the electronic recording of commercial transactions 260/2007 - Published in the Official Monitor, Part I no. 506 of July 27, 2007 – Abrogated by Government Ordinance 190/2009.

Ministerial Order no. 1000 of October 26, 2010 for the amendment and supplementing the Order of the Minister of Communication and Information Society no. 473 of 2009 regarding the procedure for granting, suspending and withdrawing accreditation decision of certification service providers.

Ministerial Order no. 888 of September 5, 2011 for the amendment and supplementing the Order of the Minister of Communication and Information Society no. 473/2009 regarding the procedure for granting, suspending and withdrawing accreditation decision of certification service providers.