DATA PROTECTION SYSTEM BASED ON DIGITAL SIGNATURE

Eugen NEACŞU[1]
[1]Advanced Technology Institute, Bucharest, Romania
[1]neacsu.eugen@yahoo.com

Keywords: digital signature, cryptographic systems, networks, encryption

Abstract: *The notion of electronic document is significantly broader than the notion of registration. Any reproduction can be made on computer support, consisting of numerical data, texts, graphics, static or animated images, sound or voice recordings. In order for the reproduction on this mechanism to record legal acts or facts, it is necessary to present it in a form that allows its automatic reading and processing by the interested subjects. This is where the digital signature comes in, which allow us to verify the source (authentication) of information received through telecommunications networks and certify that the data has not been altered along the way (integrity). This can already be achieved by using conventional (symmetric) cryptography or private key cryptography, but digital signatures also guarantee that the signer of a digitally signed message will not subsequently relinquish its "ownership" over the message (non-repudiation of the source). The paper presents a concept of integrated protection of computerized systems using digital signatures.*

1. INTRODUCTION

The electronic document has been defined as any representation in electronic form of facts, things or situations relevant from a legal point of view, which can be reproduced in an intelligible form. The electronic document is an indisputable social reality. In order to become a legal reality, it must have the same properties that are specific to written documents. Thus, the electronic document certifies in its content legally relevant acts and facts, and their rendering is done in an intelligible form. But the most important feature remains the establishment of the electronic document as evidence in court. This feature is more difficult to achieve than in the case of classic documents, due to the specific features of the electronic environment.

In the electronic environment, information is not consumed by use, it can be changed relatively easily, and the transfer of ownership of goods leaves no trace in the sense that we were familiarized to the physical environment. If in the physical environment it is rightly considered that any human activity produces by itself traces in the environment, in the electronic environment there is a need to produce traces, along with the occurrence of events of legal significance. To these is added the problem of interconnection of electronic communications networks that make it possible for a very large number of subjects to access information. For these reasons, greater importance should be given to the security and securitization of documents in electronic form. In ensuring the security of the information contained in a document, it starts from the attestation of the conformity of the information contained in it with the reality producing legal meanings. The conformity of the information is practically achieved through the procedure of signing a document.

2. DATA AND DOCUMENT ENCRYPTION

An important part of software applications refers to the processing and archiving of documents in electronic format. Although these systems help reduce difficulties in processing and archiving a large volume of documents, they do not completely solve the transition from traditional documents to electronic documents. What is missing is the possibility to sign these electronic documents and thus, ensure their non-repudiation.

Data security refers not only to the time when information is used in an information process, but also to its storage. Maintaining their confidentiality and integrity covers many aspects, which relate to both access authentication and encryption so that they cannot be used in case of unauthorized access. [1]

Name and password authentication is the most vulnerable solution and, in addition, forces the user to store such a combination for each application used. The use of the digital certificate stored on the smartcard contributes not only to increase the degree of security but also to an easier use, by using a unique means of authentication for all the applications used.

Encryption, at the data transmission level, can be done by encrypting the link or by encrypting the data. The encryption of the connection is ensured implicitly by the network or Internet communication protocols.

Secure Socket Layer (SSL) is a secure Web protocol developed by Netscape Communications that provides encryption for communications between any two computers on the Internet adopting the universal protocol used - TCP/IP. SSL is based on public key encryption (PKI) and works in two stages: in a first stage a special session key is established (transmitted in an encrypted form using the public key); this key will be used in the second phase for fast data encryption. [1]

SSL provides:

- server authentication based on digital certificates (which discourages impostors);
- confidentiality of transmissions (by encryption);
- integrity of the transmitted data (through verification codes).

The digital signature is an attribute of a user or process, being used for its recognition. Let *B* be a message receiver signed by *A*. *A*'s signature must satisfy the following properties:

- *B* to be able to validate *A*'s signature;
- to be impossible for anyone, including *B*, to falsify *A*'s signature;
- if *A* does not recognize the signing of a message *M*, there must be a "judge" who can resolve the dispute between *A* and *B*.

The digital signature solves both the issue of transmitter authentication and that of data authentication. Public key authentication systems allow a simple implementation of digital signatures. Because it is owned only by *A*, the *DA* transformation can serve as a digital signature for *A*. The *B* receiver of the signed *M* message (transformed by *DA*) is sure of both the sender's authenticity and that of the data. Because the reverse transformation is public, receiver *B* will be able to validate the signature. [2]

The processes are carried out in the following manner:

- *A* signs *M* calculating $S = DA\ (M)$;
- *B* validates the signature of *A*, checking if $EA\ (S) = M$;
- *A* “judge” resolves any dispute between *A* and *B* by controlling whether *EA* (*S*) leads to *M*, in the same manner as *B*.

To create and use a digital signature, the next steps are followed:

- creating the public key and private key pair for sender *A*;
- sending the public key to the receiver *B*;
- sender *A* creates a message for recipient *B* and uses the document as the input date for the hash function;
- the sender encrypts the result of document processing with the hash function with its own key. The result is the digital signature. The schematic operation is exemplified in the following figure (figure 1).

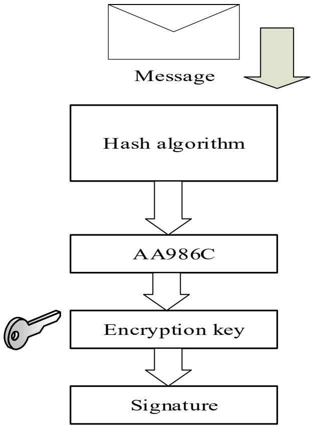


Fig. 1 Digital signature

The message is sent to the destination followed by the digital signature. The digital signature must certify that it is sent by the claimer. [2]

- the recipient will separate the original message from the digital signature;
- the digital signature is decrypted with the help of the sender's public key;
- the same hash function applies to the original document as in the posting.

It is compared if the two results, from the decryption of the digital signature with the public key and from the application of the message hash function, are identical. If it is confirmed, then the message is sent by the claimant. The use of the digital signature is exemplified in the following figure (figure 2).

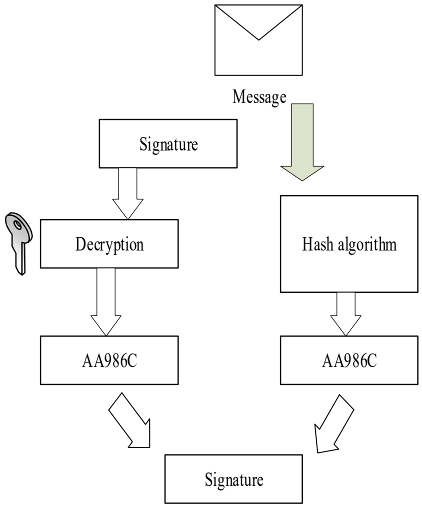


Fig. 2 The use of digital signature

The digital signature does not give confidentiality to the content of the message. It only authenticates that the sender is the one who claims to be. The digital signature is different from the electronic signature. The digital signature is a processing of a message, while the electronic signature is an electronic representation of the classic signature.

3. MATHEMATICAL ALGORITHMS USED FOR DIGITAL SIGNATURE

In practical implementations, public key algorithms are often inefficient in terms of execution time to achieve the digital signature. To save time, a hash function is used in the digital signing process to help create a summary of the document or message to be transmitted. [3]

The main steps to follow for transmitting a file under secure transactions are:

- a summary of the document is created using a hash function;
- the summary is encrypted with the secret key of the sender who also creates the digital signature in this way;
- the document, together with the signature, are sent to the receiver;
- the receiver verifies the signature in three steps (a new summary of the received document is created, the signed summary is decrypted with the public key of the sender, and the two summaries are compared and if the summaries match then *Signature is true*).

The hash function, used to create and verify the digital signature, is an algorithm that creates a digital representation, a "fingerprint" of the message, in the form of a "hash value" or "hash result" of a standard length, which is usually much smaller than the original message, but nevertheless, to a very large extent, unique to the message. These, unlike encryption and decryption algorithms, perform only the encryption function and the original message will never be recovered. In principle, a message always has the same value after the function is applied and it is impossible for any two messages to generate the same value. [3]

Another comparison of the hash function is similar to a person's DNA code - the sequence of DNA molecules is unique to each person, reflects in the smallest detail the particularities and possible changes in the body, allows the unambiguous establishment of the "owner", but from DNA we can not create, that is, "deduce" the person. When using the same hash function, any change in the original message will invariably produce a different hash result. In the case of a secure hash function, sometimes called a "one-way hash function", it is computationally unfeasible to derive the original message from knowing its hash value.

Therefore, hash functions allow programs, that create digital signatures, to operate with small, predictable volumes of data, while continuing to provide a strong probative correlation with the original content of the message. Therefore, the hash functions effectively provide the certainty that the message has not been changed since the digital signature. In addition, the unilaterality of functions excludes not only the possibility of falsifying the signature, but also the possibility of renouncing or denying its creation - no one but the signatory can calculate the value of the signature of a particular document - being a very useful effect from a legal point of view. [3]

From a cryptographic point of view, the basic properties of a "good" hash function are the dispersion property, the collision resistance quality and the irreversibility property. The collision of a hash function H is the situation when there are two different texts $T1$ and $T2$, but $H (T1) = H (T2)$. The value of the hash function has a fixed length, and the length of the original text is unlimited. Hence, the existence of collisions. The collision resistance requirement means that for a cryptographic "good" hash function, for a given $T1$ text it is computationally impossible to find a $T2$ text that would cause a collision. The quality of the scatter requires that minimal changes in the hash-forgotten text cause maximum changes in the value of the hash function. There is another additional optional requirement, which is related to the resistance of the result of applying the hash function in the transmission process through telecommunication channels - the possibility to check the consistency.

The RSA algorithm (one of the best cryptographic systems with public keys) was created by three researchers, namely Rivest, Shamir and Adleman of the Massachusetts Institute of Technology, and is a de facto standard. It is widely used as a very good cryptographic system with public keys. The algorithm enjoys great appreciation in the governmental and commercial environment, being supported by several researches and studies from the academic community. [4]

RSA is based on the near impossibility of factoring very large numbers. The encryption/decryption functions are exponential, where the exponent is the key, and the calculations are made in the ring of residue classes modulo n.

The parameters of the cryptographic system are: [4]

- p and q are 2 very large prime numbers (secret, possibly known only to the owner).
- the module n, made public, is obtained as a multiplication between p and q, $n = p$ * q.
- Euler indicator $f (n) = (p-1) * (q-1)$, impossible to determine by an attacker, because the prime factors of the numbers n, p and q are unknown.
- the secret key, *PRIV*, chosen as a very large integer relatively prime with $f (n)$, preferably from the interval [max (p, q) +1, n-1].
- the public key, *PUB*, an integer calculated by a version of Euclid's algorithm, as the inverse modulo $f (n)$. $PUB = inv (PR IV, f (n))$.
- M the document in electronic format.
- $H (M)$, summary - digest - document, calculated with a hash scatter function.

To send an encrypted message to a person C, person A encrypts the message (clear text) with C's public key. Person C receives the encrypted message from A and decrypts it with his private key, thus obtaining the original clear text.

Within the group of people, A, B, C, D, E, each holds the public keys of the other and uses them to transmit messages. Also, each person uses their private (personal) key to decrypt incoming messages so that only the recipient of the message can read the message.

This encryption method is used when the sender is interested that no one (not even those in the group) will be able to read the message clearly. The disadvantage of this method is that anyone in the group can send messages, and the recipient cannot be 100% sure of the sender's identity. [4]

The advantage of the RSA is that it can also be used to sign sent messages. The block diagram of the digitally signed message transmission system is shown in the figure bellow (figure 3).

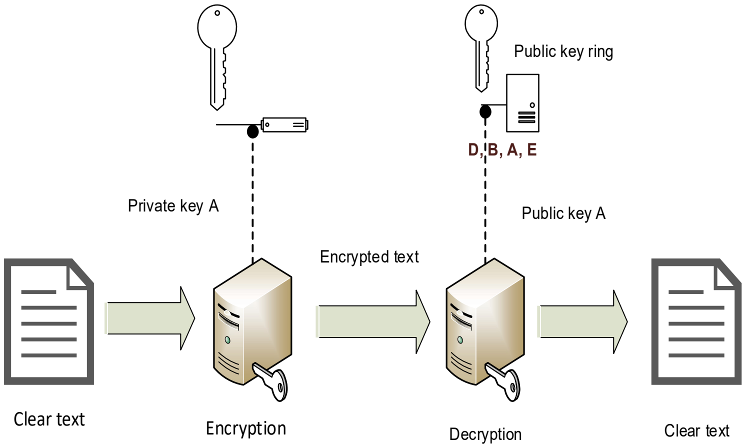


Fig. 3 Digitally signed message transmission system

As it is known, each member of a group holds the public key of the other members of the group and its private key. To send an encrypted and signed message to person *C*, person *A* encrypts the message (clear text) with his private (personal) key. Person *C* receives the encrypted message from *A* and decrypts it with its public key (*A*'s public key), thus obtaining the clear original text.

Unlike the first encryption scheme, in this case, everyone in the group can decode the message, but there is no doubt about the sender's identity.

A, *B*, *C* and *D* can be both individuals and programs, which means that this encryption system can be used by both: people, for the transmission of massages (for example: the transmission of e-mails, files in any format), as well as programs (client/server software packages), in order to transmit information from the server application to the client application and/or vice-versa, within LAN (Local Area Network) or WAN (World Area Network) networks.

Unlike the DSA and El Gamal algorithms, which can only be used for digital signature, the RSA algorithm can also be used for encryption/decryption. The strength of the algorithm lies in the difficulty of factorizing *n* into *p* and *q*. RSA labs suggest using very large 128-bit or 1024-bit prime numbers, which are factorized over several years. [5]

Under various forms of implementation, the RSA algorithm is known as the most secure encryption and authentication method available. A practical example of using and implementing an RSA cryptographic system is the SFTP (Secure File Transfer Protocol) application which uses its own protocol in the secure transmission of files, ensuring the authentication of parts and the secrecy of messages through cryptographic algorithms with public keys: RSA, ElGammal. [5]

The steps to transport a file securely (specific to the SFTP application and not the RSA algorithm) are as follows: [6]

1. a document is summarized using a hash scatter function;
2. the summary is encrypted with the private key of the sender;
3. the result from step 2 is encrypted with the public key of the receiver;
4. the encryption of the document is performed with the public key of the receiver;
5. the encrypted document together with the signature are sent to the receiver;
6. the receiver gets the signature and the encrypted document and decrypts it with his private key;
7. the function from step 1 applies to the result from step 6;
8. the receiver decrypts the signature with his private key;
9. the result from step 8 is decrypted with the public key of the sender;
10. the result in step 9 is compared to the one in step 7. If the results match, then the digital signature will be validated.

4. CASE STUDY

Users' private keys are generated either using smart-card cryptographic devices or in software format.

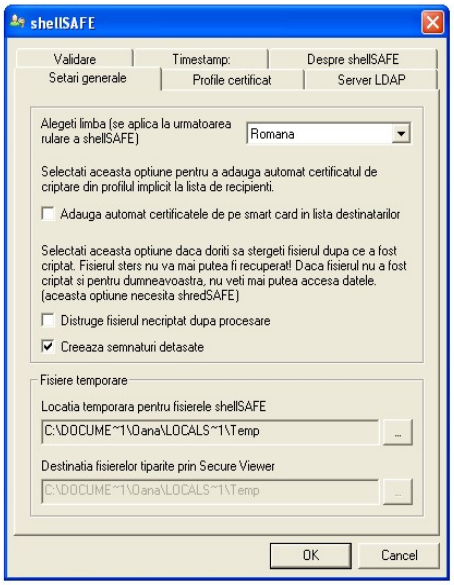
The clickSIGN application offers solutions for digital signing of individual documents and document encryption, adding timestamps, checking digital signatures and the integrity of received documents. clickSIGN is a program marketed by the software company Isigma, and is a component of the shellSAFE suite of security applications integrated into Windows Explorer and Microsoft Office that enables encryption and digital signing of files and directories to provide maximum security, no matter where the documents are stored. An alternative for clickSIGN is DocuSign (Document Signature) application. [7]

Minimum requirements: operating system: Windows 2000 SP2, SP3, SP4 or Windows XP, RAM: 128 MB, free hard disk space: 50 MB.

When using certificates stored on a smartcard device, it is mandatory to install the necessary drivers for the smart card device.

Certificate profiles are defined to allow the user to perform operations with multiple digital certificates. The user can use certificates stored on the smart card device, or certificates in PKCS # 12 format (files with * .p12 or * .pfx extensions) stored on the hard disk. It is a single default profile (the one that is most often used), but the user can choose the profiles he needs to perform cryptographic operations.

When no profile is defined, the clickSIGN application will use digital certificates stored on smart card devices.



Alegeti limba (se aplica la urmatoarea rulare a shellSAFE) Romana

Selectati aceasta optiune pentru a adauga automat certificatul de criptare din profilul implicit la lista de recipienti.

☐ Adauga automat certificatele de pe smart card in lista destinatarilor

Selectati aceasta optiune daca doriti sa stergeti fisierul dupa ce a fost criptat. Fisierul sters nu va mai putea fi recuperat! Daca fisierul nu a fost criptat si pentru dumneavoastra, nu veti mai putea accesa datele. (aceasta optiune necesita shredSAFE)

☐ Distruge fisierul necriptat dupa procesare

☑ Creeaza semnaturi detasate

Fisiere temporare

Locatia temporara pentru fisierele shellSAFE

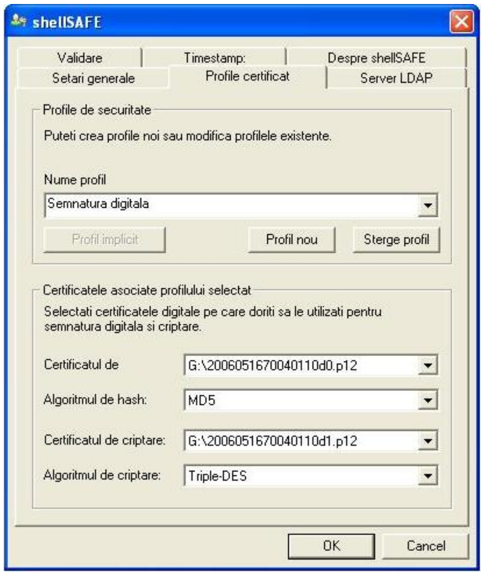
C:\DOCUME~1\Oana\LOCALS~1\Temp

Destinatia fisierelor tiparite prin Secure Viewer

C:\DOCUME~1\Oana\LOCALS~1\Temp

Fig. 4 Certified profile

Profiles are created from "Control Panel> shellSAFE Configuration> Certified Profiles". To create a profile, press the "New profile" button and enter the name of the desired profile in the specified field. When using the default clickSIGN, the certificates on the smart device will be used, in order to use a certificate from a PKCS # 12 file, this option is chosen and the location of the file containing the certificate is opened.



Profile de securitate

Puteti crea profile noi sau modifica profilele existente.

Nume profil

Semnatura digitala

Certificatele asociate profilului selectat

Selectati certificatele digitale pe care doriti sa le utilizati pentru semnatura digitala si criptare.

Certificatul de: G:\2006051670040110d0.p12

Algoritmul de hash: MD5

Certificatul de criptare: G:\2006051670040110d1.p12

Algoritmul de criptare: Triple-DES

Fig. 5 Digital signature

The Certified Profiles tab has the following fields:

- "Profile name" - field in which the profile name can be entered. To add, delete or set a default profile that is used most often, use the "New profile", "Delete profile" and "Default profile" buttons.
- "Signing certificate" - select the location of the certificate: smart card device (which is the default option), or using a PKCS certificate # 12.
- "Hash algorithm" - choose the algorithm for digital signing.
- "Encryption certificate" - select the location of the certificate: smart card device (which is the default option), or using a PKCS certificate # 12.
- "Encryption Algorithm" - the field in which the encryption algorithm can be chosen.

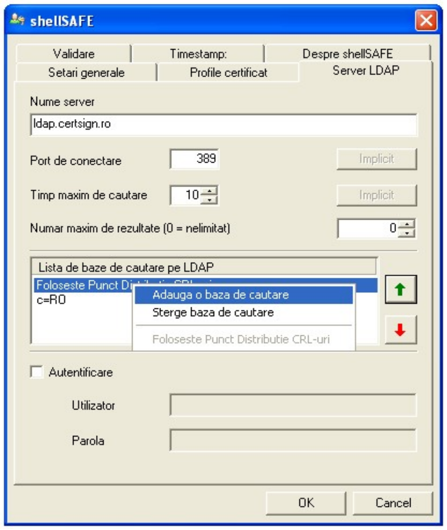
An encrypted file can only be accessed if it matches the profile of the chosen digital certificate.

The LDAP Server tab configures the parameters for connecting to the directory server (such as Active Directory).

To configure a connection to the LDAP server, open the "Control Panel> shellSAFE Configuration> LDAP Server" location, enter the IP or hostname of the LDAP server, the port (if different from the default port) and the search base.

The LDAP Server tab contains the following fields:

- "Server name" - LDAP server address (IP address or hostname);
- "Connection port" - the port used for the connection to the LDAP server, if the automatic Default button is pressed, it will be completed with port 389 which is also the default port of the LDAP server;
- "Maximum search time" - the period after which the search for the LDAP server stops, if the search returned no results;
- "Maximum number of results" - is the maximum number of results that can be displayed. If the user wants all results to be displayed, fill in the field with the value "0";
- "Basic LDAP search list" - configures the search base for digital certificates on the LDAP server. To change the search base using the "Up" and "Down" buttons. To add or delete a search base, right-click on the "LDAP search base" field and choose the appropriate option;
- "Authentication" - this option is selected when the connection to the LDAP server requires authentication: the fields "User" and "Password" are filled in with the username and password required to access the LDAP server.



Nume server: ldap.certsign.ro

Port de conectare: 389

Timp maxim de cautare: 10

Numar maxim de rezultate (0 = nelimitat): 0

Lista de baze de cautare pe LDAP:
Foloseste Punct Di
c=RO

□ Autentificare

Utilizator:

Parola:

Fig. 6 LDAP Server

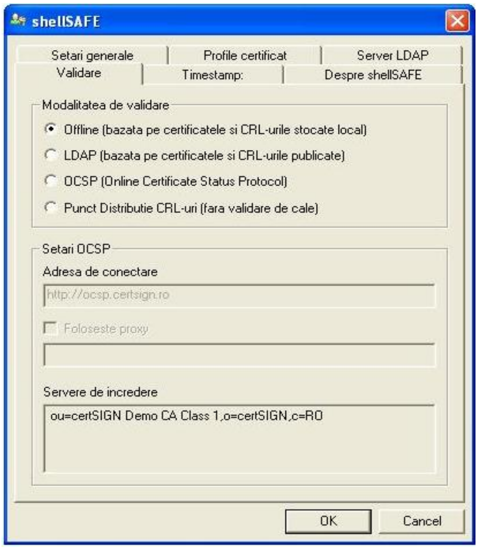
A signed document can be a trusted document when a digital signature is not destroyed (the information was not changed after it was signed) and when a signing certificate is valid, if a certificate is not revoked or expired, and the trusted chain from the Root Certification Authority in the public key infrastructure hierarchy is not destroyed.

To verify the validity of a certificate, clickSIGN also verifies the validity of all certification authorities in the trusted chain. This can be done using online mechanisms (LDAP servers or On Line Certificate Status Protocol Responders), or offline, using information stored on the user's site. [8]

The Validation tab contains the following fields:

- "Offline (based on local certificates and locally stored CRLs)" - this option is recommended to be introduced only if there is no online connection or if the Certification Authority does not provide additional information for certificate validation. When this option is chosen, the certificates from the trusted authorities in the trusted chain and the corresponding CRL must be installed locally;

- "LDAP (based on publishing certificates and CRLs)" - this option validates the certificate by connecting to an LDAP server and downloading the necessary information from there (certificates from trusted certification authorities, and CRLs). This option uses the configuration from the "LDAP Server" tab and is a convenient option for the user, as the user does not need to be aware of installing certificates and reinstalling CRLs when they have expired;
- "Online Certificate Status Protocol (OCSP)" - this option provides additional mechanisms for certificate validation and can also be used to validate the status of the certificate at a given time. To configure OSCP options, the user must create a list of trusted servers;
- "Login address" is the URL address of the recipient's OCSP server;
- "Trusted servers" is a list of certificates used by the OCSP server to sign its response. To add or delete a certificate, right-click in the "Trusted Servers" field and choose the appropriate option.



Modalitatea de validare

● Offline (bazata pe certificatele si CRL-urile stocate local)
○ LDAP (bazata pe certificatele si CRL-urile publicate)
○ OCSP (Online Certificate Status Protocol)
○ Punct Distributie CRL-uri (fara validare de cale)

Setari OCSP

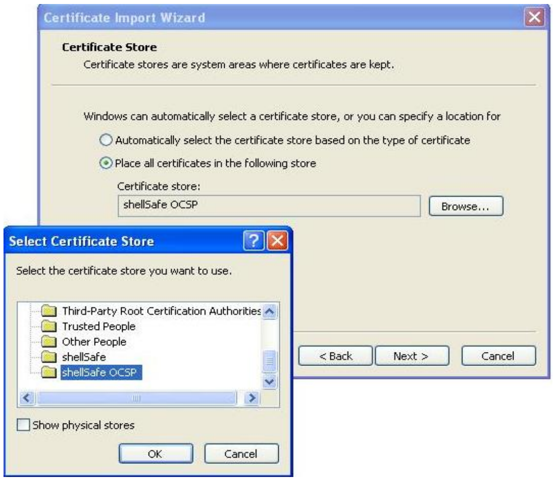
Adresa de conectare: http://ocsp.certsign.ro

□ Foloseste proxy

Servere de incredere: ou=certSIGN Demo CA Class 1,o=certSIGN,c=RO

Fig. 7 Validation

To install the certificates required for offline validation, double-click on each certificate in the certificate chain (a file with the .cer extension) and the "Welcome to the Certificate Import Wizard" window will appear. Click the "Next" button to continue. From the window that opens, select the option "Place all certificates in the following store" and then click on the "Browse ..." button.



Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for

○ Automatically select the certificate store based on the type of certificate
● Place all certificates in the following store

Certificate store: shellSafe OCSP

Select the certificate store you want to use.

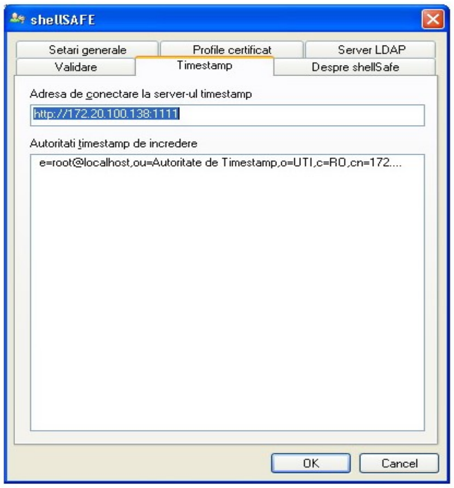
Third-Party Root Certification Authorities
Trusted People
Other People
shellSafe
shellSafe OCSP

□ Show physical stores

Fig. 8 Installing the certificates

Timestamp is the configuration needed to add a timestamp to signed documents. The Timestamp tab contains the following sections:

- "Connection address to timestamp server" is the URL of the server;
- "Trusted timestamp authorities" is a list of time stamp certificates used to indicate their response. To add or delete certificates, right-click on the "Trusted timestamp authorities" field and choose the appropriate option.



Adresa de conectare la server-ul timestamp

http://172.20.100.138:1111

Autoritati timestamp de incredere

e=root@localhost,ou=Autoritate de Timestamp,o=UTI,c=RO,cn=172....

Fig. 9 Timestamp

To be able to encrypt documents without connecting to the LDAP server, digital encryption certificates must be installed in a certificate store. To install a certificate in the local certificate store, double-click on the certificate (a file with the extension .cer .p12 or .pfx) and the "Welcome to the Certificate Import Wizard" window will appear. Click "Next" to continue. In the window that opens click on the option "Place all certificates in the following store" and then click on the button "Browse ..." and choose the certificate store "shellSafe" click on the button "OK" then on "Next" and then "Finish".

5. CONCLUSIONS

The possibility of transmitting digitally signed documents is the first step towards the new technological world, based on the speed of reaction of those involved in the exchange of information, disregarding the geographical distance.

The digital signature, in addition to the convenience it offers in various operations, provides a higher degree of security than the holographic signature, given that an electronic document cannot be modified without invalidating the signature. The recipient of the digitally signed message can verify both that the original message belongs to the person whose signature was attached and that it has not been altered, intentionally or accidentally, since it was signed. Moreover, the digital signature cannot be denied, the signatory of the document cannot later apologize invoking the fact that it was forged.[9]

Regarding the applications described above, I emphasize that in order to make this presentation of the paper, certificates created by Microsoft Office 2007 are used. These are self-signed system certificates and can be used to digitally sign and encrypt documents using Microsoft Office 2007 being usually used by individuals or by various small and medium-sized enterprises, enterprises that do not have and do not want to set up a public key infrastructure. The disadvantage of using self-signed system certificates is that, since there is no third party to validate them, each person who receives a digitally signed document with such a certificate will have to decide whether or not to trust the certificate used when signing the document.

Larger organizations have two other options, namely to create their own PKI. In this scenario, the company establishes one or more certification authorities, which can create digital certificates for machines and users throughout the company. Another option is to use commercial certificates such as those used by the clickSign application. A commercial certificate is one that is purchased from a company whose line of business is to sell digital certificates. The advantage of using these certificates issued by CA is that the company ensures the issuance and management in the best conditions of security of digital certificates being automatically installed on Windows operating systems, so that the private key is not disclosed outside the cryptographic element and it is not even communicated to the signatory's computer, thus being able to automatically trust these certification authorities and at the same time the certainty that in this way recognized electronic documents can be obtained.[10]

An electronic document is recognized, so it has proven value, similar to any handwritten or handwritten signature, if three conditions are met: the signature is extended, the certificate is qualified and the signature creation device is secure. This does not mean that other types of signatures do not work, which may be part of various applications created on the Internet that may have digital signatures, even extended digital signatures, but which have no probative value before the court.

In conclusion, I emphasize that the digital signature provides a much greater security in terms of specific functions than in the case of the classic signature, which will impose it quite soon. Although the procedure is not widely used at present, in the coming years this type of signature will become mandatory. It will become, in the near future, a very common way to personalize an official document, a letter or an invitation. Reduced time and increased security are the main advantages of this new method of signing an act. Tomorrow's contracts will be concluded and signed digitally, thanks to information and communication technology.

6. REFERENCES

[1]. Patriciu, V., ‘*’Electronic Signatures and Computer Security’’*, All Publishing, 2006.

[2]. Andrew, S. Tanenbaum, ‘’*Computer Networking’’*, 4th Edition, Prentice Hall, 2003.

[3]. Atanasiu, A., ‘’*Information Security’’,* volume 1, INFODATA Publishing, 2007.

[4]. Atanasiu, A., ‘’*Information Security’’*, volume 2, INFODATA Publishing, 2009.

[5]. Salomon, D., ‘’*Coding for Data and Computer Communications’’*, Publisher. Springer, Verlag, pp. 271-328, 2005.

[6]. Omar, S., ‘’*End-to-End network security defense in dept*h’’, accessed 10.12.2020: www.ciscopress.com.

[7]. Avizienis, A., Laprie, J.C., Randell, B., Landwehr, C., ‘’*Basic concepts and Taxonomy of Dependable and Secure Computing’’*, IEEE Transactions on Dependable and Secure Computing, Vol. 1, No. 1, 2004.

[8]. Whitman, M.E., Mattord, H.J., ‘’*Priciples of Information Security’’*, Cengage Learning EMEA, 2009.

[9]. Lockhart, B., ‘’*Key management services. Provisioning systems for enterprise key management’’*, IEEE Key Management Summit, 2008.

[10]. Koblitz, N., Menezes, A., ‘’*Another Look at Provable Security’’*, In Journal of Cryptology Vol. 20, No. 1, pp 3-37, 2007.