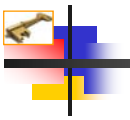


Universitatea Babes-Bolyai Cluj-Napoca

Masterat *Sisteme distribuite in Internet*

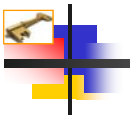
-2009-

CURS: Protocoale de securitate

Modul:

SEMNATURI ELECTRONICE SI INFRASTRUCTURI DE SECURITATE

Prof. Dr. Victor-Valeriu PATRICIU



Sumar modul

SEMNATURI ELECTRONICE SI INFRASTRUCTURI DE SECURITATE

1. Criptografia si semnaturile electronice
2. Infrastructuri de certificate digitale (PKI)
3. Servicii asociate semnaturilor electronice
4. Smart-carduri, biometrice & semnaturi electronice
5. Reglementarea documentelor & semnaturilor electronice

Bibliografie

Bibliografie in limba romana

Patriciu V.,Bica I.,"*Semnaturi electronice si securitate informatica*",Ed All, 2006

Patriciu V., Bica I., "*Securitatea comertului electronic***"**, Ed All, 2001.

Patriciu V., Vasiu I., "*Internet-ul şi dreptul***"**, Ed All, 1999.

Patriciu V., Bica I."*Securitatea informatică în UNIX şi INTERNET*",Ed Tehnică, 1998

Patriciu V.*"Criptografia si securitatea retelelor de calculatoare"*,Ed Tehnică,1994

Bibliografie in limba engleza

Stalling W., "*Cryptography & Network Security*", Prentice Hall, 2001.

O'Mahony D., "*Electronic Payment Systems for E-Commerce*", Artech House, 2001.

Housley R., "*Planning for PKI"*, John Wiley, 2000.

Fausse A., " *La signature electronique* "**,** Ed.Dunod 2001.

Ford W., "*Secure Electronic Commerce",* Prentice Hall, 2001.

Resurse Electronice

http://www.enisa.europa.eu/

http://people.csail.mit.edu/rivest/crypto-security.html

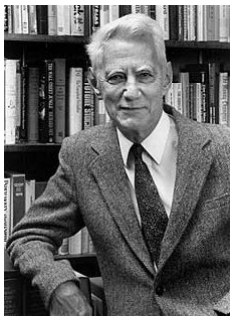
Cryptography & Information Security

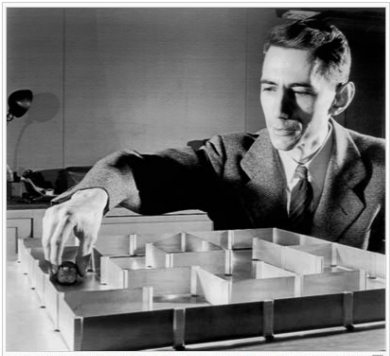
Peoples & History

Key Peoples in Cryptography

Claude Shannon, "the father of information theory"

(1916 –2001)





Shannon and his famous electromechanical mouse *Theseus*, named after the Greek mythology hero of Minotaur and Labyrinth fame, and which he tried to teach to come out of the maze in one of the first experiments in artificial intelligence.

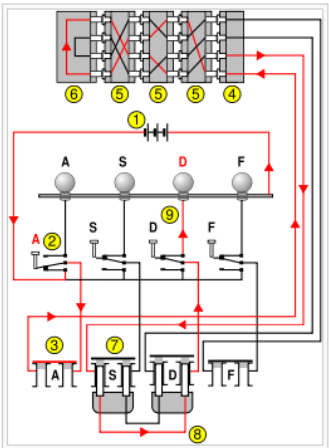
• In 1940 Shannon joined **Bell Labs** to work on **cryptography** during World War II, under a contract with section D-2 (Control Systems section) of the **National Defense Research Committee**

• His paper published in 1949 is ***Communication Theory of Secrecy Systems*** is a major contribution to the **development of a mathematical theory of cryptography** where **he proved that all theoretically unbreakable ciphers must have the same requirements as one-time pad**.

Prof.Dr.Victor-Valeriu PATRICIU

Key Peoples in Cryptography

Enigma machine

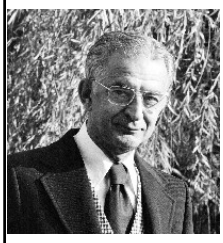


Enigma wiring diagram showing current flow. The 'A' key is encoded to the 'D' lamp. D yields A, but A never yields A.

Prof.Dr.Victor-Valeriu PATRICIU

Key Peoples in Cryptography

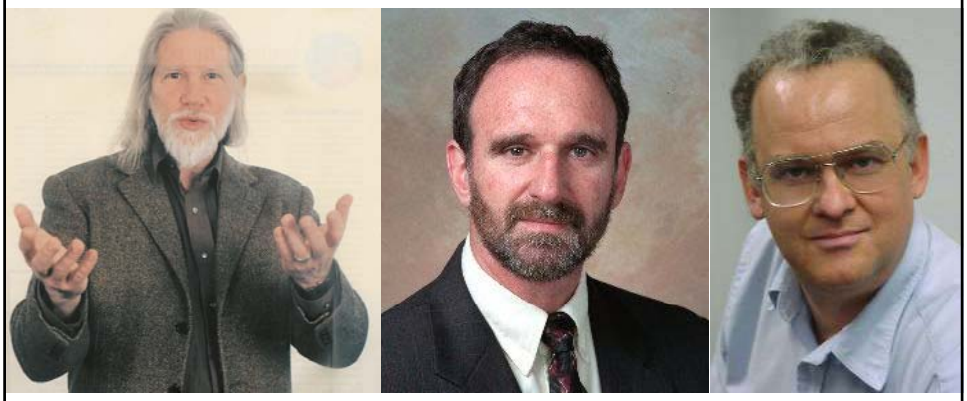
Horst Feistel (1915 - 1990)



- Known for his work on the **Feistel network construction** - a common **method for constructing encryption algorithms**.
- His work at IBM led to the development of the pioneering Lucifer and Data Encryption Standards (DES) ciphers, and as a result of his efforts, IBM announced the 3845 and 3846 data encryption devices and the IBM cryptographic subsystem.
- In 1977, he was recognized at the IBM Corporate Technical Recognition Event (CTRE) for *"devising a scheme encrypting binary data which is especially significant to IBM products and is the basis for the recently announced Federal Information Processing Standard adopted by the U.S. Commerce Department*"

Key Peoples in Cryptography

Diffie & Hellman & Markle

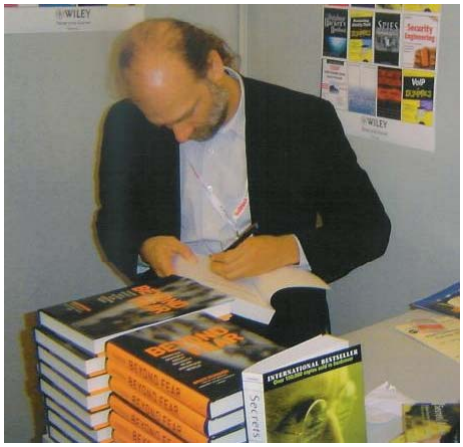


Key Peoples in Cryptography

Rivest & Shamir & Adleman

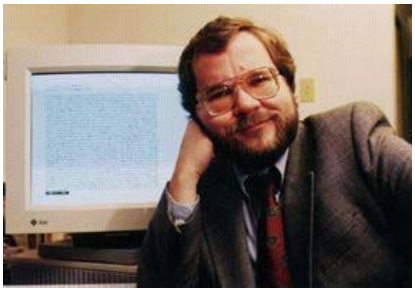
Key Peoples in Cryptography

Bruce Schneier- *BT Counterpane Internet*



Key Peoples in Cryptography

Philip Zimmerman- *PGP*



Key Peoples in Cryptography

Joan Daemen & Vincent Rijmen - *AES*

Key Peoples in Cryptography

David Chaum

Key Peoples in Cryptography

Jean-Jacques Quisquater

Crypto Group

Univerite Catolique Louvaine

Key Peoples in Cryptography

Prof.Dr.Claus-Peter Schnorr

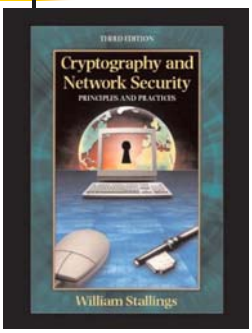
Key Peoples in Cryptography

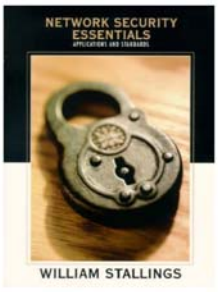
Prof. Jacques Stern

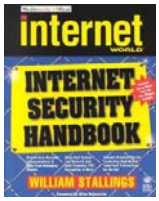
Professeur d'informatique
Directeur du DI (l'Ecole Normale Supérieure)
Directeur du laboratoire **Securite informatique** de l'ENS (LIENS)

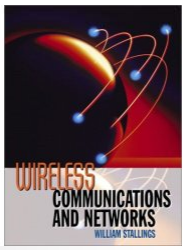
Key Peoples in Cryptography

William Stallings



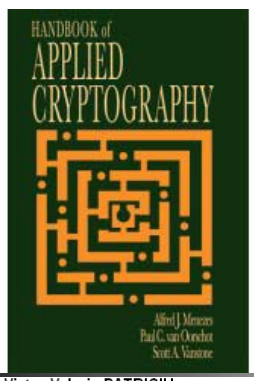


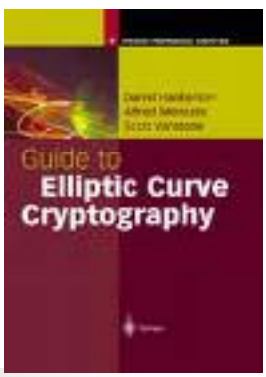




Key Peoples in Cryptography

Alfred J. Menezes





Key Peoples in Cryptography

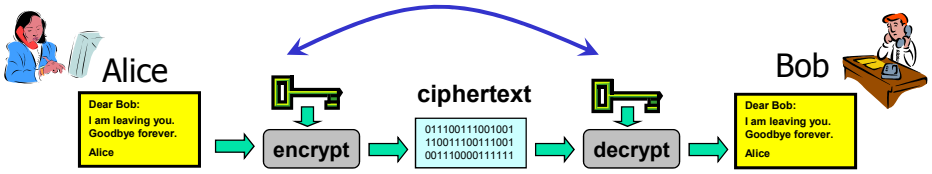
William Frederick Friedman

• (Born Chisinau, 1891 –Death 1969) - US Army cryptologist.
• He ran the research division of the Army's Signals Intelligence Service (SIS) in the 1930s, and its follow-on services into the 1950s.
In the late 1930s, subordinates of his led by Frank Rowlett broke Japan's PURPLE cipher, thus disclosing Japanese diplomatic secrets in the World War II era.
• Following World War II, Friedman remained in government signals intelligence. In 1949 he became head of the code division of the newly-formed Armed Forces Security Agency (AFSA) and in 1952 became chief cryptologist for the National Security Agency (NSA) when it was formed to take over from AFSA. Friedman produced a classic series of textbooks, "Military Cryptanalysis", used to train NSA students. (These were revised and extended, under the title "Military Cryptanalytics", by Friedman's assistant and successor Lambros D. Callimahos, and used to train many additional cryptanalysts.)
• Friedman retired in 1956 and, with his wife, turned his attention to the problem that had originally brought them together: examining Bacon's codes. In 1957 they wrote *The Shakespearean Ciphers Examined*, demonstrating flaws in Gallup's work and in that of others who sought hidden ciphers in Shakespeare's work. Records that Friedman had used to prepare *Six Lectures Concerning Cryptography and Cryptanalysis*, which he delivered at NSA, were confiscated from his home by NSA security staff.
• Friedman's wife donated his archives to the George C. Marshall Library, which also was raided by NSA security.
• Friedman has been inducted into the Military Intelligence Hall of Fame and has a building named after him and his wife, Elizebeth, at the NSA complex at Fort George G. Meade in Maryland.

1. CRIPTOGRAFIA & SEMNATURILE ELECTRONICE

- Introducere in criptografie
- Lungimea si managementul cheilor criptografice
- Semnătura bazata pe criptografia cu cheie publică
- Schema de semnătură RSA
- Schema de semnătură ElGamal
- Schema de semnătură DSA
- Semnaturi bazate pe curbe eliptice
- Semnături oarbe/incontestabile/proxy/de grup
- Semnaturi XML
- Standarde de format

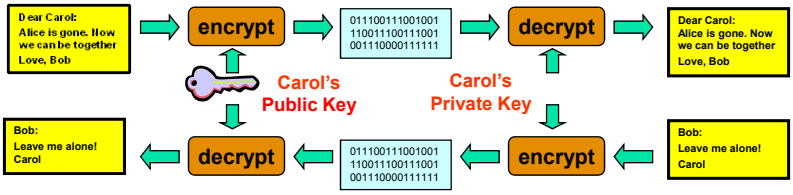
Symmetric Key Cryptography



- Computationally fast
- Data Encryption Standard (DES)
  - Block Cipher, 56 bit key
  - Triple DES 112 bit key
- Advanced Encryption Standard (AES)
  - Rijndael Algorithm
  - Belgian cryptographers, Joan Daemen and Vincent Rijmen.
  - 128, 192, 256 bit keys

Asymmetric Key Cryptography

- Two mathematically related keys
  - Unable to derive one from the other
  - Based upon hard problem
    - **RSA** - Integer Factorization (large primes)
    - **Diffie-Hellman** - Discrete Logarithms
    - **ECES** - Elliptic Curve Discrete Logarithm
- Public Key Cryptography
  - One *public key* published for all to see
  - Other is *private key* kept secret by owner



Brute Force Cryptanalysis

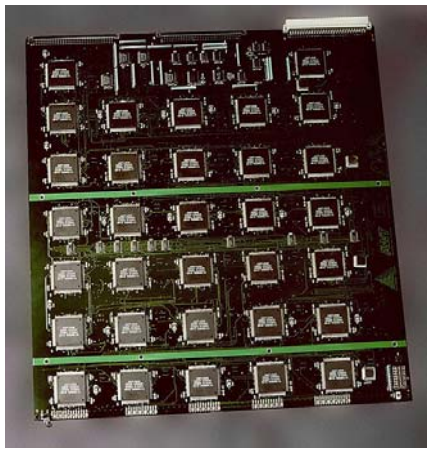
- It is always possible to break an algorithm by trying every possible key.
- This is independent of the algorithm.
- Brute force cryptanalysis is ideal for parallel processors and distributed computing.
- The only defense is a long key.

Brute Force Against Symmetric Cryptography

- **Average time to break an algorithm** with given key length using a custom machine costing $1 million:
  - 40 bits 0.2 seconds
  - 56 bits 3.6 hours
  - 64 bits 38 days
  - 80 bits 7,000 years
  - 112 bits 10**13 years
  - 128 bits 10**18 years
  - For every 5 years in the future, assume the attack is 10 times faster or cheaper
  - Techniques of differential cryptanalysis proposed by Biham and Shamir and linear cryptanalysis proposed by Matsui do not represent a threath for the use of cryptography, as they are chosen palintext attacks wich require large amounts of plaintext-chipertext pairs.

Brute Force Against Symmetric Cryptography

- From March 2007, dedicated machines such as Copacobana can break DES in an average time of 6.4 Days- FPGA-based machine (http://www.copacobana.org/).
- Also, the Deep Crack machine from Electronic Frontier Foundation (EFF) is capable of testing more than 90 billions DES keys per second, which means that the entire key space can be exhausted in about 9 days, the average time for finding a key will be 4.5 days (http://w2.eff.org).
- The EFF's US$250,000 DES cracking machine contained over 1,800 custom chips and could brute force a DES key in a matter of days — the photo shows a DES Cracker circuit board fitted with 32 Deep Crack chips



Brute Force and Public-Key Cryptography

- Public-key crypto gets its power from the difficulty of factoring large numbers
  - 512 bits — 30,000 mips-years
  - 768 bits — 200,000,000 mips-years
  - 1,024 bits — 10**11 mips-years
  - 2,048 bits — 10**20 mips-years
- Pentium-based PC: 50-100 mips
- 1600-node Paragon: 50,000 mips

MIPS-Year = 3.1×10^{13} arithmetic operations.

This is

1×10^{6} operations/sec x 3600sec/hr x 24hrs/day x 365 days/yr x 1 yr

A recent effort which factored a 200-digit number (RSA-200) took eighteen months and used over half a century of computer time

Electronic Signatures

Electronic Signature != Digital Signature

Electronic Signatures in Global and National Commerce Act (E-Sign) defines:

The term "electronic signature" means an electronic sound, symbol, or process, attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record.

Electronic Signature

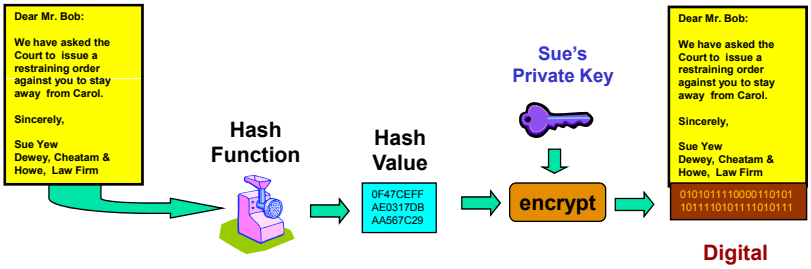
Potrivit *Asociaţiei Baroului American (American Bar Association–ABA)*, **semnarea documentelor** are urmatoarele proprietati:

- semnătura este **autentică** deoarece se verifică numai cu cheia publică a emiţătorului;
- semnătura este **nefalsificabilă** deoarece numai emiţătorul cunoaşte cheia secretă proprie;
- semnătura este **nereutilizabilă** deoarece ea este funcţie de conţinutul documentului, cel care este criptat;
- semnătura este **nealterabilă** deoarece orice alterare a conţinutului documentului face ca semnătura să nu mai fie verificabilă cu cheia publică a emiţătorului;
- semnătura este **nerepudiabilă** deoarece receptorul documentului nu are nevoie de ajutorul emiţătorului pentru verificarea semnăturii.

Digital Signatures

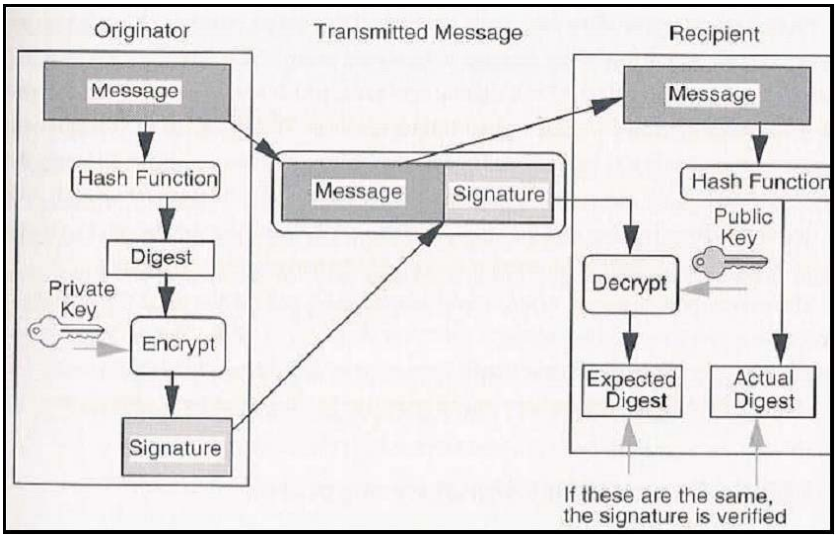
- A *digital signature* is a a type of *electronic signature*.
- It is a *hash* of a document encrypted with the author's private key

Sue



Digital (Electronic) Signature

-creating & verifying-



Digital Signatures

with Message Recovery

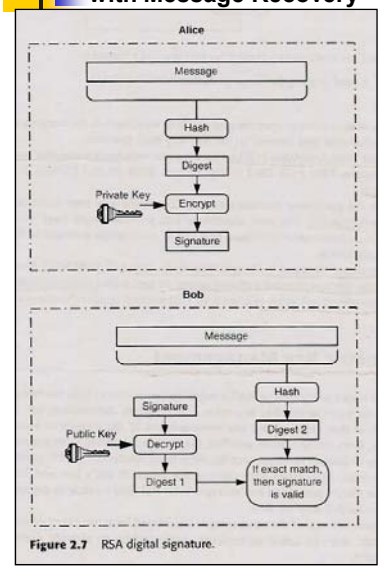


Figure 2.7 RSA digital signature.

without Message Recovery

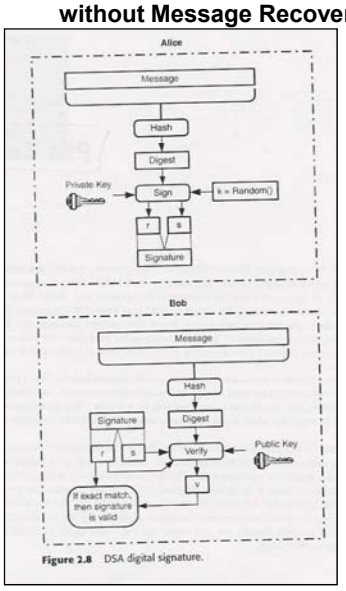


Figure 2.8 DSA digital signature.

Recommended Signature Key Length and Algorithms

-for e-commerce use-

- **Signature Algorithms**

  -1024 bits key RSA;
  -1024 bits key DSA;
  -160 bits key DSA with elliptic curves

- **Hash Functions**:

  -RIPEMD – 160
  -SHA-1, SHA-2

RSA
-mathematical background-

- **Factoring probleme-** the difficulty of the task to find the 2 prime factors of an great integer.
- **Mathematical background:**

Euler's Theorem

$$M^{\varphi(n)} = 1 \mod n$$

- φ(n) is Euler's Totient function (the number of positive integers less than n and relatively prime to n)

- For a prime number n, **φ(n)=n-1.**

RSA
-mathematical background-

- Select **p** & **q** prime numbers (keep secrets)
- Calculate **n=p*q** (public)
- Calculate **φ(n)= φ(p)* φ(q)**
- Select integer **e** (public)
- Calculate **d** (secret), **e*d=1 mod φ(n), $d=e^{-1} \mod \varphi(n)$,**

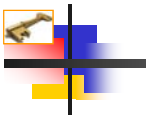
- **Public key- [e,n]**
- **Private key- [d,n]**

- **Encryption** $C = M^e \pmod n$
- **Decryption** $M = C^d \pmod n$
  $= (M^e)^d \pmod n$
  $= M^{e*d} \pmod n = M^{\varphi(n)+1} \pmod n$
  $= M^{\varphi(n)} * M = M$

RSA- PSS

-new PKCS #1 standard-

- **RSA PSS-** New signature scheme that is based on the RSA cryptosystem and provides increased security assurance. It was added in version 2.1 of PKCS #1
- "PSS" refers to the original Probabilistic Signature Scheme by Mihir Bellare and Phillip Rogaway on which RSA-PSS is based.
- RSA-PSS has recently been added to RSA Security's RSA BSAFE Crypto-C and Crypto-J toolkits
- Signature scheme has been recommended by the European NESSIE project (**N**ew **E**uropean **S**chemes for **S**ignatures, **I**ntegrity, and **E**ncryption), and has also received positive evaluations by from Japan's **CRYPTREC project**. RSA-PSS is also in the (nearly final) draft amendment IEEE P1363a. A companion scheme that also provides "message recovery" is included in the international standard ISO/IEC 9796-2:2002.



RSA- PSS

-new PKCS #1 standard-

RSA-PSS, like most digital signature schemes, follows the "hash-then-sign" paradigm.

Let *M* be a message to be signed. A signature is computed on the message *M* in three steps:

1. Apply a one-way hash function to the message *M* to produce a hash value *mHash*.
2. Transform the hash value *mHash* into an encoded message *EM*.
3. Apply a signature primitive to the encoded message *EM* using the private key to produce a signature *S*.

RSA- PSS
-new PKCS #1 standard-

This can be expressed in equation form as

S = SigPrim (private key, Transform (Hash (M)))

- Here, SigPrim denotes the signature primitive. With the RSA cryptosystem, this is the classic formula
- $S = EM^d \bmod n$
- where (n, d) is the private key, and EM and S are considered as integers.

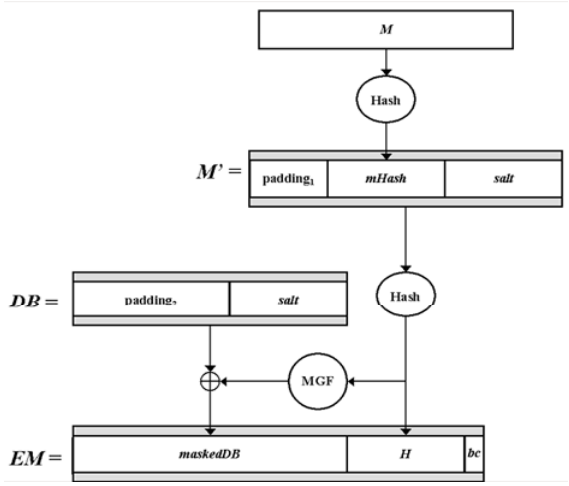
RSA- PSS
-new PKCS #1 standard-

- In the PKCS #1 v1.5 signature scheme, the Transform operation consists of fixed padding; the hash value is simply prepended with a header string of the form 00 01 ff ff … ff ff 00 (in hexadecimal) followed by a string that identifies the hash function. In RSA-PSS, the operation is much more "random." Instead of fixed padding, the scheme generates a random "salt" value then applies a hash function and a mask generation function to the salt and the hash value to produce the encoded message.
- The transformation, illustrated in Figure, consists of the following steps:

1. Generate a random salt value *salt*.
2. Concatenate fixed padding, the hash value *mHash*, and *salt* to form a string *M'*.
3. Apply the hash function to the string *M'* to compute a hash value *H*.
4. Concatenate fixed padding and the salt value to form a data block *DB*.
5. Apply the mask generation function to the string *M'* to compute a mask value *dbMask*.
6. XOR the mask value *dbMask* with data block *DB* to compute a string *maskedDB*.
7. Concatenate *maskedDB*, the hash value *H*, and fixed padding to compute the encoded message *EM*.

RSA- PSS

-new PKCS #1 standard-



RSA- PSS

-new PKCS #1 standard-

Advantages of RSA-PSS

- The primary advantage of RSA-PSS over the traditional PKCS #1 v1.5 signature scheme is that modern methods of security analysis can relate its security directly to that of the RSA problem. While no attacks are known on the traditional scheme, and while solving the underlying RSA problem (e.g., factoring the modulus) is the best method known for forging a signature, the connection of PKCS #1 v1.5 signatures to the RSA problem has never been proved. RSA-PSS, in contrast, has such a proof if one models its hash functions as "random oracles" as is commonly done.
- In recent years there has been a trend toward so-called "provably secure" cryptographic techniques that are more directly connected to underlying hard problems. If a signature scheme does not have a security proof, it is theoretically possible that signatures could be easy to forge, yet the underlying problem still be hard to solve. Ideally, one would like some assurance that the problems take about the same amount of time. Although the state of complexity theory does not let us prove that an underlying problem, e.g., RSA, is definitely hard to solve, we will still have the assurance that if the problem is indeed hard to solve, signatures are just as hard to forge.

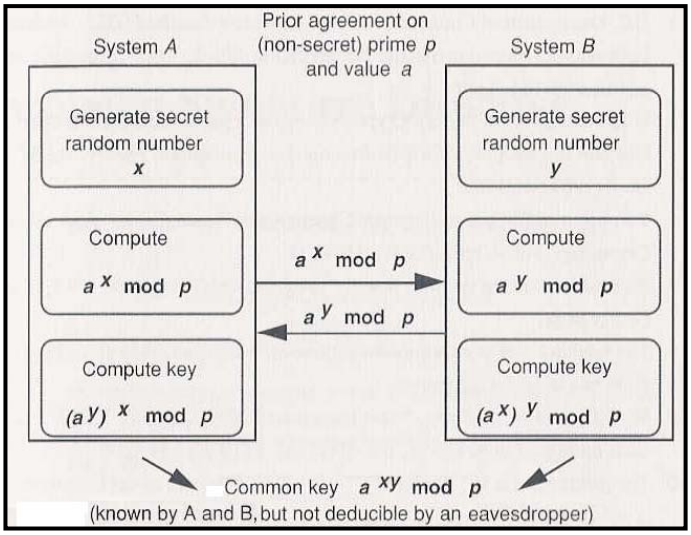
Key Management

- Key management is the hardest part
- Easy to implement algorithms and protocols
- Harder to handle keys correctly
  - generate, transfer, store, authenticate, use, update, destroy
- In the real world, *encryption schemes are defeated not by breaking the algorithm, but by poor key management!!*

- Two public key distribution algorithms:
  - **Key agreement**- exchange public keys for generating a symmetric encryption key
  - **Key transport**- use public/ private keys for encrypting (enveloping) symmetric encryption key

Key Management

-Diffie-Hellman key agreement scheme-

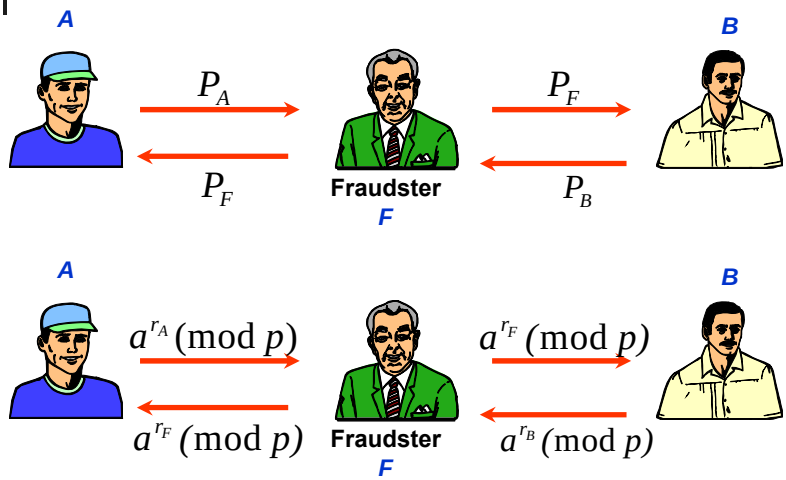


Key Management

-Diffie-Hellman key agreement scheme-

- User A:
  - Chooses $\mathbf{X_A}$ – A secret key
  - Calculates $\mathbf{Y_A}=a^{XA} \bmod n$ – A public key
- User B:
  - Chooses $\mathbf{X_B}$ – B secret key
  - Calculates $\mathbf{Y_B}=a^{XB} \bmod n$ – B public key
- A calculates the secret (simmetric) key:
  - $\mathbf{K_{AB}} = Y_B^{XA} \bmod n = a^{XB\,XA} \bmod n$
- B calculates the secret (simmetric) key:
  - $\mathbf{K_{AB}} = Y_A^{XB} \bmod n = a^{XA\,XB} \bmod n$

D-H Man in the Middle Attack

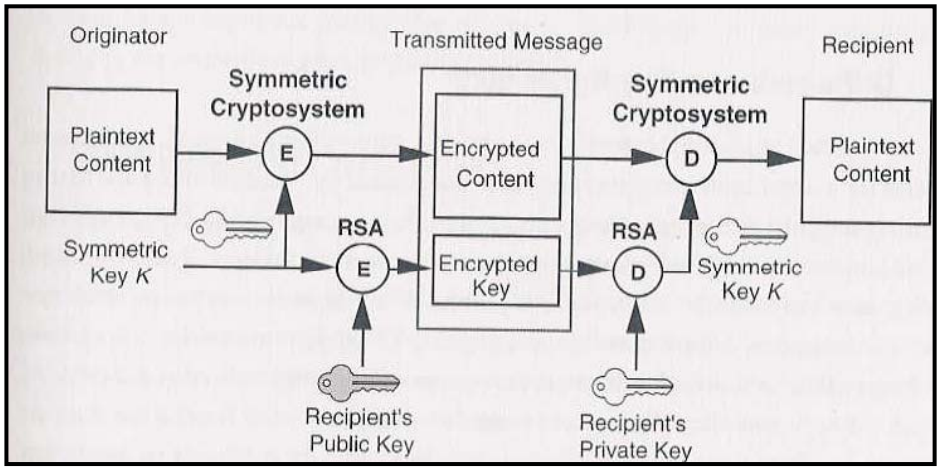


The Fraudster has agreed keys with both *A* and *B*
***A* and *B* believe they have agreed a common key**

Key Management

-Key transport -

in E-mail (Document) Encryption



Digital Signatures

-mathematical beckground for El Gamal-

-*cheia secretă*: $PRIV_A$, un număr natural aleator.

-*cheia publică:* $PUB_A = a^{PRIVA} \pmod n$, unde

a-este o constantă a sistemului cunoscută de toţi partenerii;

n-este un număr prim mare (sute de cifre zecimale).

$PRIV_A = \log PUB_A \pmod n$ la fel de dificil ca si factorizarea !!!

Digital Signatures

-mathematical beckground for El Gamal-

-M: un document electronic ce urmează a fi semnat,

-H(M) rezumatul documentului calculat cu *funcţie de hash H*, 0<=H(M)<=n -1.

Semnarea unui document M se face după următorul algoritm:

- se calculează rezumatul documentului, H(M);
- se generează aleator K în [0,n-1], a.i. cmmdc (K,n-1)=1
- se calculează $r = a^K \pmod n$
- se calculează apoi, folosind cheia secretă a emitentului (Dan), valoarea lui s din ecuaţia:

$$H(M)=PRIV_{dan} * r + K * s \pmod{(n-1)}$$

Semnătura lui Dan asupra lui M, este perechea: S=(r,s)

Digital Signatures

-mathematical beckground for El Gamal-

Fiind recepţionaţi documentul M şi semnătura S=(r,s), este uşor ca un alt user, de exemplu Ana, să verifice autenticitatea semnăturii lui Dan calculand două valori întregi:

$$\textbf{Valoare1} = a^{H(M)} \bmod n$$

si

$$\textbf{Valoare2} = (PUB_{dan})^r * r^s \bmod n$$
$$= (a^{PRIVdan})^r * a^{K s} \bmod n$$
$$= (a^{PRIVdan\ r + K s}) \bmod n$$
$$= a^{H(M)} \bmod n$$

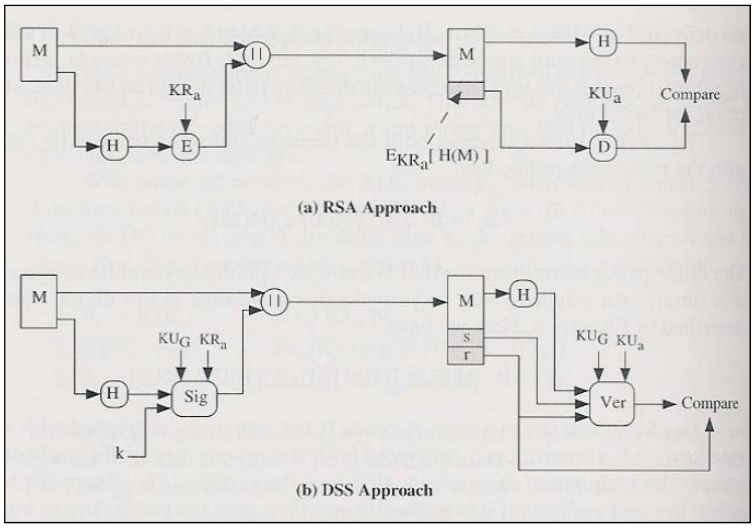
si le compara dacă sînt egale.

Digital Signature Algorithm DSA

- DSS Digital Signature Standard, NIST
- FIPS PUB 186, 1996
- Designed for digital signature only
- Based on the difficulty of computing discrete logarithms in great fields:
  - ✓ $Y=a^X \bmod n$ <u>easy to calculate</u>
  - ✓ $X= \log_a Y$ <u>difficult to calculate in great fields</u>

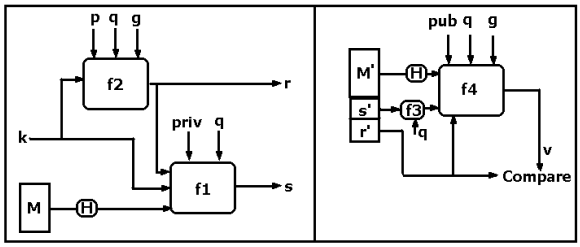
DSA

-digital signature approaches-



DSA

Signing & Verifying



Signing	Verifying
$\mathbf{r} = f2\ (k, p, q, g) = (g^k \bmod p) \bmod q$ $\mathbf{S} = f1\ (H(M), k, priv, r, q) = (k^{-1}\ (H(M) + priv * r)) \bmod q$	$\mathbf{W} = f3\ (s', q) = s'^{-1} \bmod q$ $\mathbf{V} = f4\ (pub, q, g, H(M'), w, r') = (g^{H(M') * w \bmod q} * (pub)^{r' * w \bmod q} \bmod p) \bmod q$

DSA

- **Parametrii sistemului**

Parametri globali (aceiaşi pentru toată lumea):

-**p**-nr.prim, p in $(2^{511};2^{512})$-512 biti

-**q**-un divizor prim al lui (p-1)-160 biţi, q în $(2^{159};2^{160})$

-**g**-un întreg cu proprietatea:

$$g = h^{(p-1)/q} \bmod p$$

unde h este un întreg relativ prim cu p, h în (0;p) astfel încît :

$$h^{(p-1)/q} \bmod p > 1.$$

-**H**-funcţie hash de calcul al rezumatului unui mesaj.

Parametrii utilizatorului (diferiţi de la un user la altul):

-***cheia secretă***: **PRIV**, un întreg în (0;q)

-***cheie publică***: **PUB**, un întreg, calculat astfel încât

$$PUB = g^{PRIV} \bmod p$$

Parametrii semnăturii (diferiţi de la o semnătură la alta):

-**M**-mesajul ce va fi semnat (documentul electronic sau fişierul)

-**k**- un întreg aleatoriu, k în (0;q), ales altul la fiecare semnătură.

DSA

- **Semnarea unui document**

Semnătura digitală S a unui document electronic M este **perechea S=(r,s)** şi se face folosind cheia secretă a user-ului emitent, de exemplu Dan, $\mathbf{PRIV_{Dan}}$

-se alege un întreg **k** în (0;q), prim cu q

-se calculează :

$$\mathbf{r=(g^k mod\ p)\ mod\ q}$$

$$\mathbf{s=((k^{-1})\ (H(M)+\ PRIV_{Dan}*\ r))\ mod\ q}$$

La recepţie se primesc **M, S=(r, s),** care pot eventual diferi de M şi S, transmise la origine, datorită unor încercări de fraudă.

DSA

- **Verificarea semnăturii unui document**

După ce un alt user, de exemplu Ana, a recepţionat documentul electronic M şi semnătura S=(r,s):

- calculează

$$\mathbf{w = s^{-1}\ mod\ q}$$ (s trebuie să fie inversabil)

-***semnătura este validă dacă se verifică ecuaţia:***

$$\mathbf{r = r'},$$

unde r' se calculează astfel:

$$\mathbf{r' = (\ g^{H(M)*\ w} * (PUB_{Dan})^{r*\ w}\ mod\ p)\ mod\ q}$$

Elliptic Curves

Key dimension CE (m)*	Key dimension RSA (bits)	MIPS-years
160	1024	1012
320	5120	1036
600	21000	1078
1200	120000	10160

* for an elliptic curve with $2m$ points, key dimension is defined to be m.

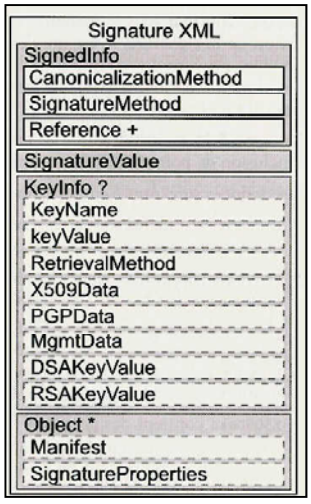
XML

- The explosive growth in the use of the Web for business-to-business (B2B) e-commerce has intensified attention on the **eXtensible Markup Language (XML)** — an open, Internet standard that facilitates data exchange over the Internet.
- Recognizing that existing Web technologies, such as HTML, are inadequate for implementing the scale and diversity of transaction protocols envisioned for the Web, the **World Wide Web Consortium (W3C)** & **Internet Engineering Task Force (IETF)** have developed XML technologies to meet this requirement.
- Like any data being exchanged over a network, **XML communications and transactions must be secured.** In this respect, to maintain the integrity of the transaction or communication, an **XML document**, just like any other document or transaction, should be capable of authentication and non-repudiation, and its content should remain intact (integrity) and confidential.

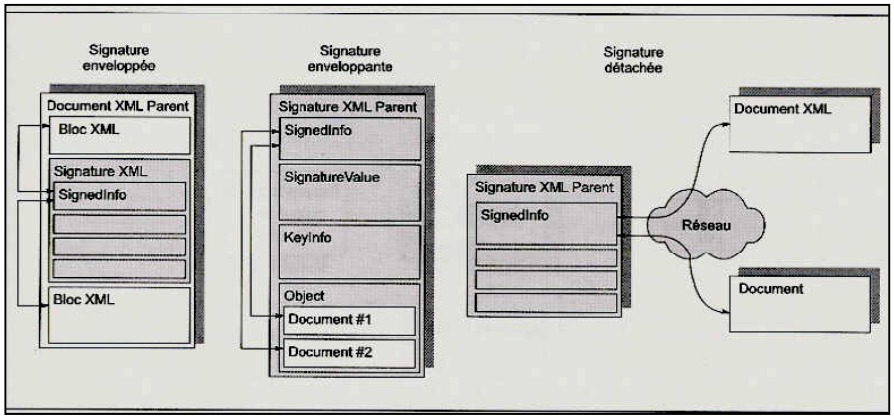
XML Signature

- W3C & IETF are elaborate the standard format and functions for **XML signing;**
- The **XML signature** – is a XML data structure wich containes
  - the signature value and
  - the data necessary in the verification process;
- The XML signature makes the following functions :
  - ➢ represent digital signature of documents (XML / non XML) in a XML format;
  - ➢ 3 types of digital signature :
    - the signature encapsulates the data being signed (enveloppante)
    - the object to be signed can have the XML Signature embedded within itself (enveloppe)
    - the object to be signed can be separate from the XML Signature, but reside within the same resource as the signature (détache)
  - ➢ it uses pointers for selection the document zones to be included in signature process;
  - ➢ permits URL references for documents.

XML Signature Structure



XML Signature Types



XML Signature

Creation

1. Determine the resources to be signed.
2. Calculate the digest of each resource. In XML Signatures, each reference is specifed by a <**Reference**> element and its digest is placed in a <**DigestValue**> child element.
3. Collect <**Reference**> elements (with associated digests) within a <**SignedInfo**> element.
4. Calculate the digest of the <**SignedInfo**> element, sign the digest using a valid private signature key, and put the signature value in a <**SignatureValue**> element. Determine the resources to be signed.
5. If keying information is to be included, place it in the <**KeyInfo**> element.
6. Place the <**SignedInfo**>, <**SignatureValue**>, and <**KeyInfo**> elements into <**Signature**> element. The <**Signature**> element is the XML Signature.

Verification

1. Obtain the public key certificate, either from <**KeyInfo**> or from an external source, and retrieve the public verification key.
2. Re-calculate the digest of the <**SignedInfo**> element. Use the public verification key to verify that the value of the <**SignatureValue**> element is correct when compared with the digest of the <**SignedInfo**> element.
3. If step 2 passes, re-calculate the digests on the related data objects of the references contained within the <**SignedInfo**> element — using either the URI it contains, or by other means. Compare the calculated digests with the digest values expressed in each <**Reference**> element's corresponding <**DigestValue**> element.
4. If step 3 passes, validate the public verification certificate by finding a certificate path to the trusted certificate (root of trust), such that this path, and the certificates it contains, are valid.

2.INFRASTRUCTURI DE CERTIFICATE DIGITALE (PKI)

- Necesitatea infrastructurilor de certificate
- Certificate digitale
- Componente unei PKI
- Evaluarea validităţii certificatelor
- Arhitecturi PKI

Public Key Infrastructure

Public Key Infrastructure (PKI) provides the means to bind public keys to their owners and helps in the distribution of reliable public keys in large heterogeneous networks. NIST

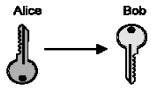
The set of hardware, software, people, policies and procedures needed to create, manage, store, distribute, and revoke Public Key Certificates based o public-key cryptography. IETF PKIX working group

"US Agencies will undertake a Federal Public Key Infrastructure (PKI) to promote digital signatures for transactions:
- *within the federal government,*
- *between government and businesses and*
- *between government and citizens"*

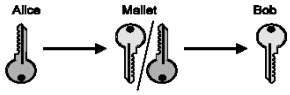
PKI is electronic identity management!

Key Distribution

Alice retains the private key and sends the public key to Bob



Mallet intercepts the key and substitutes his own key



Mallet can decrypt all traffic and generate fake signed message

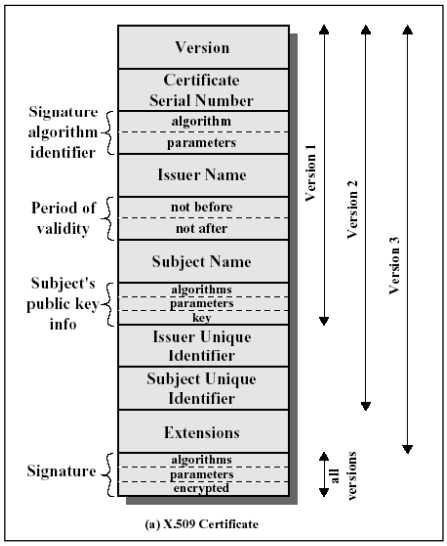
A certification authority (CA) solves this problem

CA signs Alice's key to guarantee its authenticity to Bob

- Mallet can't substitute his key since the CA won't sign it

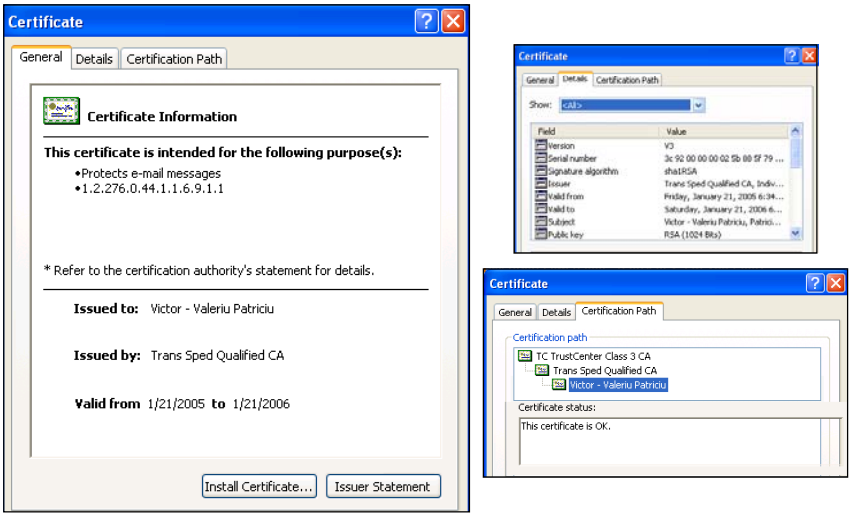
Digital Certificate X 509 V3

- Is a person really who claim?
- How do you know that the public key you got from a person really bellongs to this person?
- Solution: **CERTIFICATE-** like an *Information Highway Driver Licence*



Digital Certificate

Sample



Certificates

End-Entity

- Are issued to subjects that are not CA's
- Contain public keys used for verifying digital signatures or for performing key management
- Subject: human user or system (Web server or router)
- 2 types:
  - User certificates
  - System certificates

CA

- Are issued to subjects that are CA's
- Are part of certificate paths
- Contain public keys used for verifying digital signatures on certificates and CRL's
- Must contain sufficient information for certificate users to construct certification paths and locate CRL's
- Subject: other CA in the same enterprise or a CA in other enterprise or a bridge
- 3 types:
  - CA certificates within an enterprise PKI
  - CA certificates between enterprise PKI's
  - CA certificates in a Bridge CA Environment

Self-Issued Certificates

- Issuer and Subject are the same
- Used to establish trust points, distribute a new signing public key or modify the certificate policies supported in a PKI
- 3 types:
  - Trust point establishment
  - Rollover certificates -Introduce a new certificate or CRL signing key. A CA issues a pair of key rollover certificates simultaneously:
    - First-contain old public key, signed with the new private key.
    - Second-contain new public key, signed with the old private key.

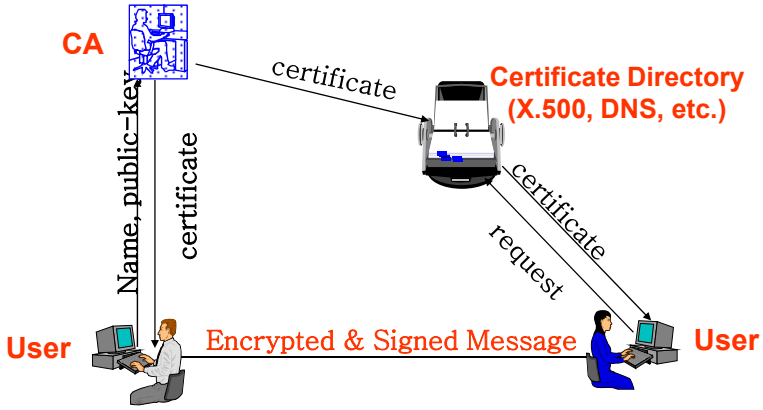
    In this way subscribers with certificates signed with the old private key and subscribers with certificates signed with the new private key can validate each other's certificates.
  - Policy rollover certificates

Certificate Authority

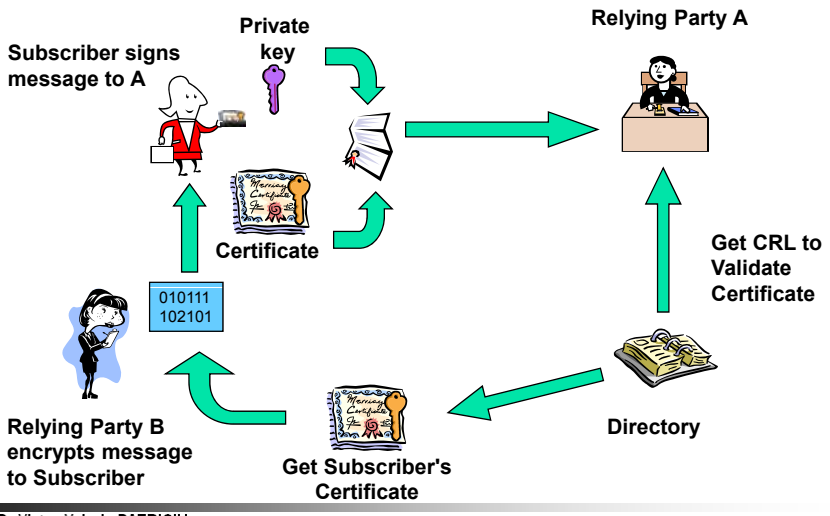
CA- a trusted authority -which provides a statement (***Digital Certificate***) that the enclosed public key belongs to the person whose name is attached

CA- a central administration - issues certificates:

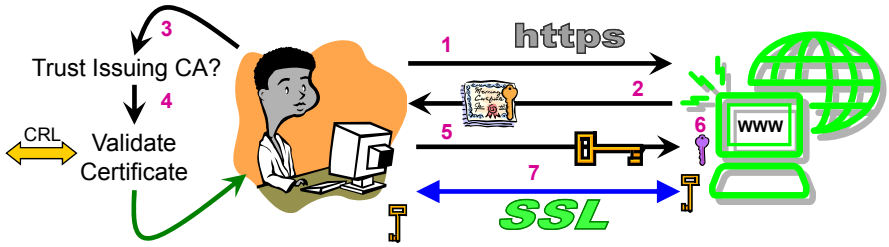
-organization to its employees
-company to its employees
-university to its students
-public CA (like VeriSign) to their clients



How Certificates are used



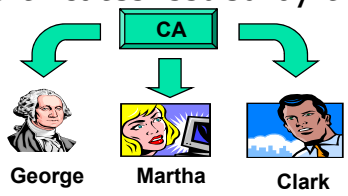
SSL Server Authentication



1. Client sends https request to server
2. Server sends its certificate to the client
3. Client decides if certificate (and issuing CA) is trustworthy
4. Client validates certificate
5. Client sends to server session key - encrypted with server's public key
6. Server decrypts session key with its private key
7. Client – Server transactions are now encrypted with session key

Single CA Model

- PKI is built upon the concept of the trusted third party (i.e., CA)
- Everyone trusts their own CA (***trust anchor***)
  - Trust all certificates issued by their CA

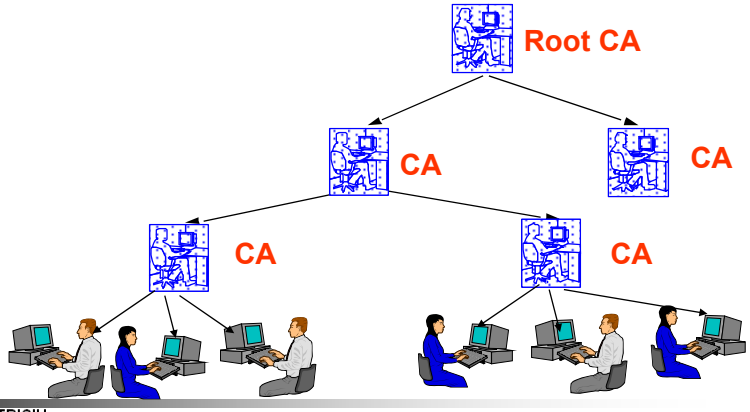


- Single CA model does not scale well
  - Difficult to manage across large or diverse user communities

Hierarchical PKI

CAs have superior-subordinate relationships
- Higher level CAs issue certificates to subordinate CAs
- Subordinate CA issues certificate to subscriber

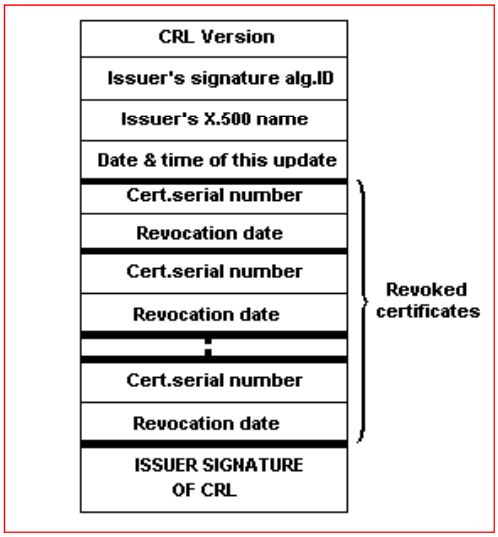
Forms a *certification path* (*certificate chain)*
- Chain of certificates from subscriber to root CA
- Root CA is top-level, self-signed (i.e., certified) CA



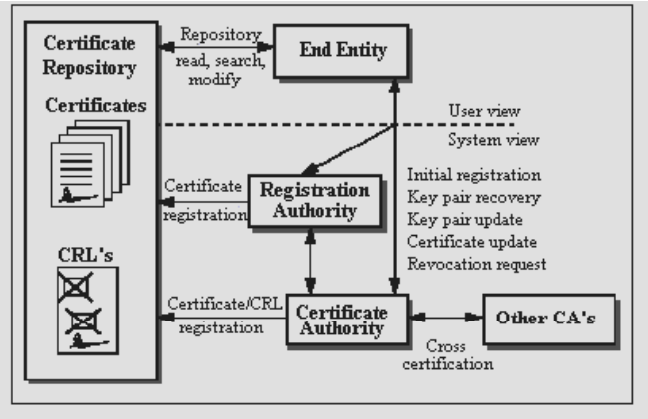
Certificate Revocation

- A **certificate must be revoked** when:
  - -the **private key** pair is **compromised**;
  - -the **private key** pair is **lost**;
  - -the **person leaves** the **company.**
- All users know to **no longer trust** in certificates;
- Relaying parties **check CRL** before using a certificate;
- Caching a CRL in a local cache
- Rather than one long CRL, keep multiple shorter CRLs .
- Distribute the CRL to multiple places and spread the load using the certificate extension field *cRLDistributionPoints*.
- Use a sufficiently scalable and powerful *CR server*.
- ***OCSP****-On-line Certificate Status Protocol:* inquires of issuing CA wheter a certificate is still valid. (resp. YES/NO)

X.509 CRL format



PKI Components



End-Entity (EE)

- An **End-Entity** is defined as a *user of PKI certificate* and/or *end-user system* that is the subject of a certificate
- In a PKI system, End-Entity is a generic term for a *subject* that ***uses some services or functions of the PKI system***, which may be a *certificate owner* (human being or organization or some other entities), or a *requestor* (it might be application program) for certificate or CRL.

Certificate Authority (CA)

• The **Certificate Authority (CA)** is the signer of the certificates. The CA, often together with the *RA*, "The Registration Authority (RA)", has the responsibility of the certificate subject entity's identification.
• The logical domain in which a CA issues and manages certificates is called security domain, which might be implemented to cover an organization, company, a large department, a test cell, or another logical community in real cases.
• A CAs primary operations include certificate issuance, certificate renewal, and certificate revocation.

Registration Authority

• **Registration Authority (RA)** is an optional component in a PKI.
• In some cases, the CA incorporates the role of an RA. Where a *separate RA* is used, *the RA is a trusted End-Entity certified by the CA, acting as a subordinate server of the CA*.
• The *CA can delegate some of its management functions to the RA*. For example, the RA may perform personal authentication tasks, report revoked certificates, generate keys, or archive key pairs.
• The **RA, however, does not issue certificates or CRLs**.

Certificate Repository (CR)

- **CR** – store, issues & revokes certificates.
- X.509 certificate format fit to an ***X.500 directory***, a CR is best implemented as a directory, accessed by *Lightweight Directory Access Protocol* (LDAP v3).
- RFC 2587, *Internet X.509 PKI Operational Protocols - LDAPv2*, defines the ***access method to a repository*** with which an *End-Entity or a CA can retrieve or modify the certificate and CRL information stored in a CR*. CR can be accessed with LDAP commands or procedures (*bind, search,modify, unbind).*
- RFC 2559, *Internet X.509 PKI LDAPv2 Schema*, defines the ***attributes*** and ***object classes*** to be ***supported by an LDAP CR server***.

Directories

- RFC 2587 specifies 3 object classes:
  - *PKI user-* used for certificate holder entries; must contain a user certificate attribute; all certificates whose subject name matches the name of entry should be stored in this attribute
  - *PKI CA-* used for CA entries; may contain a CA certificate, CRL, ARL and cross-certificate pair attributes; CA certificate attribute contains CA certificates whose subject name matches the name of entry; these certificates may be self-issued or issued by other CA's;
  - *CRL distribution point-* may include CRL, ARL, and delta CRL attributes; the name of the entry will match the name in the CRL distribution point extension;

X.500 Directories

- Various servers called Directory Server Agents (DSA)
- Clients called Directory User Agent (DUA)
- DSA responds to DUA queries with information
- X.500 Directory uses 2 basic *protocols*:
  - *Directory Access Protocol (DAP)*- supports information requests from a DUA to a DSA;
  - *Directory Service Protocol (DSP)*- supports information requests between DSA's; DSA's may augment DSP by *shadowing*, with the *Directory Information Shadowing Protocol (DISP*), used to replicate the contents of a DSA;

LDAP

Lightweight Directory Access

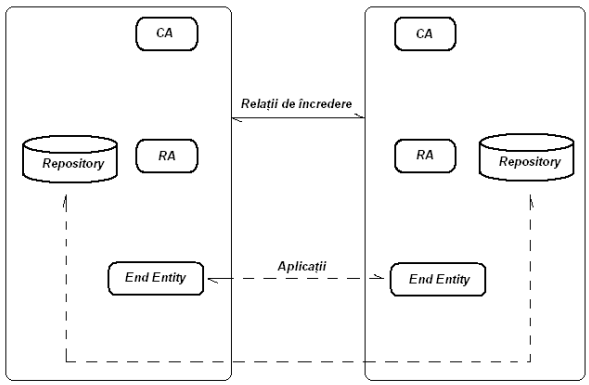
- Developed by the University of Michigan
- Standardised in IETF;
- If a LDAP directory receives a request for an entry that is not locally held, it checks a table of remote directories; if one directory is likely to contain the entry, the directory returns a referral to the other directory;
- The referral contains the directory name and the system that support them;
- The architecture does not provide transparency; a client must determine the physical location before it obtains any information;
- Generally, *if certificates or CRL's are not available in the first LDAP directory checked, they will not be found*.
- PKI repositories based on LDAP generally use a single repository.
- Most CA products include an LDAP client and can perform authenticated directory updates automatically.

PKI Interoperability

-different domains-

Interoperabilitatea între domenii PKI diferite se referă la relaţiile de încredere şi modul de interacţiune dintre componentele şi aplicaţiile PKI aparţinând unor organizaţii diferite. Acest tip de interoperabilitate permite efectuarea de tranzacţii sigure între organizaţii şi prin urmare reprezintă un factor cheie în promovarea pe scară largă a tehnologiei PKI.

Asigurarea interoperabilităţii între domenii PKI diferite necesită, pe lângă soluţionarea **problemelor** tehnice si administrative.



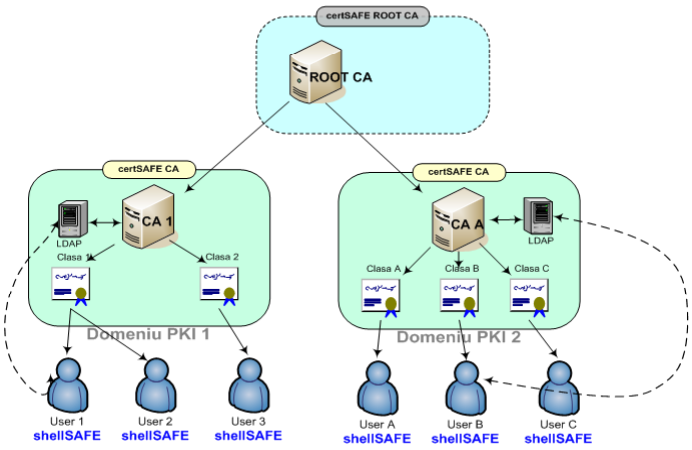
PKI Interoperability

-solutions-

În literatura de specialitate sunt sugerate o serie de **soluţii pentru asigurarea interoperabilităţii între domenii PKI diferite**:

- Liste cu Autorităţi de Certificare de încredere
- Cross-certificarea bilaterală
- Autorităţi de Certificare Punte (Bridge CA)
- Certificatele de acreditare
- Delegarea procesului de determinare şi validare a căi de certificare

PKI Interoperability
-solutions-



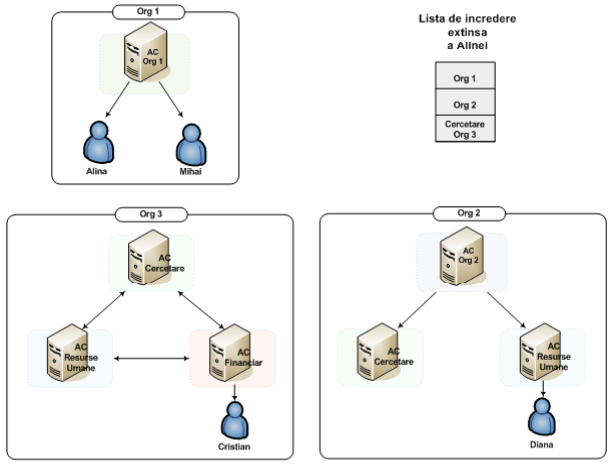
Model ierarhic

PKI Interoperability
-solutions-

Liste cu Autorităţi de Certificare de Încredere

- Listele cu Autorităţi de Certificare de încredere sunt folosite pe scară largă în momentul de faţă şi reprezintă o extensie a modelului arhitectural ierarhic prin declararea de încrederea a mai multor autorităţi de certificare rădăcină. Validarea certificatelor digitale se face în acelaşi mod, prin validarea căii de certificare (certification path) până la una din Autorităţile de Certificare Rădăcină din listă.
- Navigatoarele Web folosesc această abordare, având pre-instalate câteva zeci de Autorităţi de Certificare în această listă. Adăugarea sau ştergerea unei autorităţi din listă se poate face de către fiecare utilizator în parte sau centralizat, la nivelul întregii organizaţii.
- Pentru a rezolva aceste probleme a fost introduse *Listele de Încredere (CTL - Certificate Trust List)*. Un CTL reprezintă o structură de date PKCS#7 semnată digital de un terţ de încredere (emitentul listei) ce conţine o serie de Autorităţi de Certificare considerate a fi de încredere. O Autoritate de Certificare de încredere este identificată în cadrul listei prin intermediul valorii hash a certificatului său digital. De asemenea, un CTL poate conţine identificatori de politici şi permite adăugarea uneia sau mai multor extensii.

PKI Interoperability
-solutions-



Lista de încredere extinsă

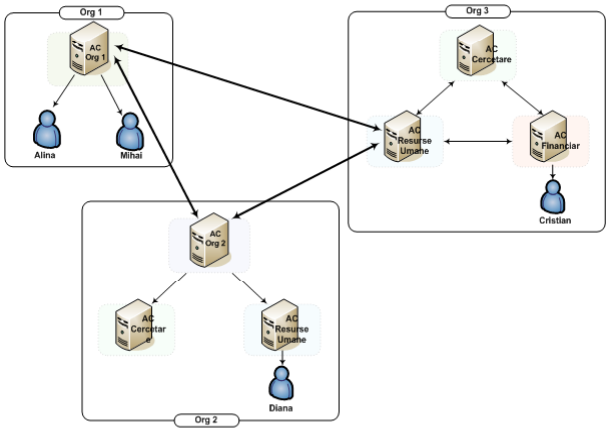
PKI Interoperability
-solutions-

Cross- Certificare

- Cunoscută şi sub denumirile de sau certificare reciprocă sau co-certificare presupune analiza şi stabilirea unei echivalenţe între politicile de certificare folosite în cadrul celor două domenii PKI.
- Sunt disponibile o serie de extensii ce pot fi folosite în cadrul certificatelor emise pentru cross-certificare:
  - *Constrângeri de Nume* (*Name Constraints*). Acestea pot fi folosite pentru a limita relaţia de încredere la unul sau mai multe subgrupuri (spaţii de nume) dintr-un domeniu PKI.
  - *Constrângeri de Politică* (*Policy Constraints*). Acestea au rolul de a limita relaţia de încredere numai la certificatele emise sub o anumită politică sau pentru a defini mapările de politici interzise.
  - *Constrângeri privind Lungimea Căilor (Path Length Constraints).* Constrângerile privind lungimea căilor din cadrul extensiei *Constrângeri de bază* (*Basic Constraints*) se folosesc pentru a limita numărul maxim de Autorităţi de Certificare dintr-o cale de certificare.
- Principalul **avantaj** al cross-certificării în reprezintă faptul că domeniile PKI îşi păstrează autonomia.

PKI Interoperability

-solutions-



Cross-certificare

PKI Interoperability

-solutions-

Bridge CA

Principala critică adusă certificării încrucişate bilaterale este scalabilitatea scăzută a soluţiei. Pentru a rezolva această problemă şi a simplifica procesele de echivalare a politicilor de certificare, a fost introdus conceptul de **Autoritate de Certificare de Tranzit** sau **Punte (*BCA – Bridge CA*)**.

Acest concept se bazează tot pe relaţii de certificare încrucişată însă model de încredere folosit este unul de tip stea. Numărul de certificări încrucişate în cazul BCA creşte liniar cu numărul domeniilor PKI

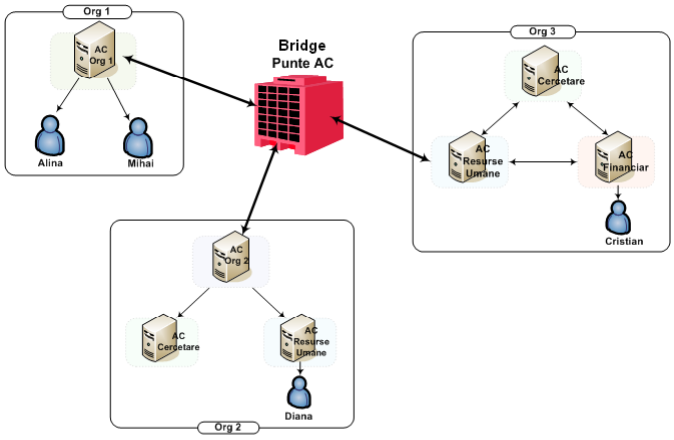
- **BCA nu trebuie considerat punct de încredere de către utilizatori**, el reprezentând doar o Autoritate de Certificare intermediară ce are rolul de a crea o punte de legătură între domenii PKI diferite.
- Fiecare BCA are definit un set clar de politici de certificare pe baza cărora se pot stabili relaţii de certificare încrucişată cu organizaţiile. Stabilirea unei căi de certificare între organizaţii este posibilă numai dacă există o echivalare a politicilor acestora cu una din politicile BCA.

PKI Interoperability
-solutions-

Bridge CA

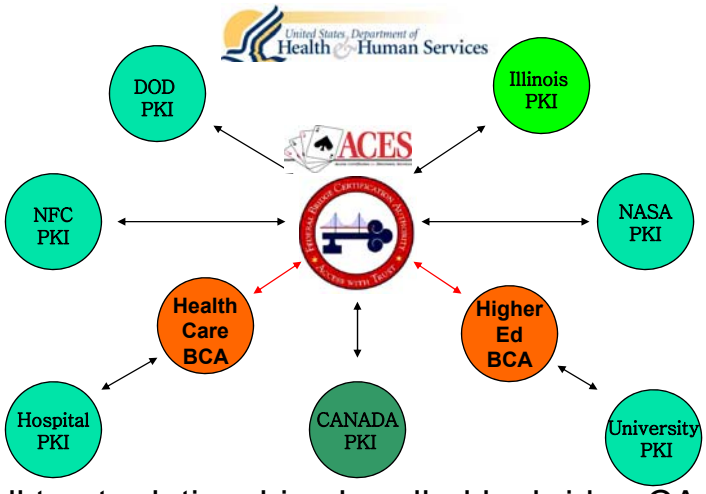
- BCA permite interconectarea de domenii PKI indiferent de arhitectura acestora.
- În cazul **infrastructurilor ierarhice**, BCA se certifică încrucişat cu Autoritatea de Certificare Rădăcină.
- Pentru **infrastructurile de tip reţea**, BCA se poate certifica încrucişat cu oricare din Autorităţile de Certificare din cadrul infrastructurii. În ambele cazuri, Autoritatea de Certificare care se certifică încrucişat cu BCA poartă denumirea de *Autoritate de Certificare Principală (Principal CA)*.
- Din perspectiva organizaţiilor, un BCA reduce semnificativ efortul suplimentar necesar stabilirii unor relaţii de încredere cu alte organizaţii care cad sub incidenţa aceleiaşi politici a BCA.
- Asta nu înseamnă că o organizaţie trebuie să se bazeze pe un singur BCA pentru a stabili relaţii de încredere cu toate organizaţiile partenere, ea putând apela şi la alte BCA în acest scop.

PKI Interoperability
-solutions-



BRIDGE
Punte AC

Federal Bridge Certificate Authority



All trust relationships handled by bridge CA

PKI Interoperability

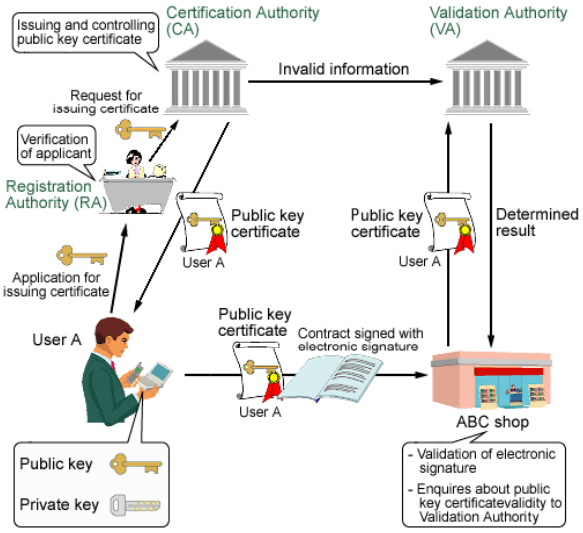
-solutions-

Delegarea validarii certificatelor

- Delegarea procesului de validare a căilor de certificare permite degrevarea clienţilor de procesările necesare validării certificatelor digitale. Pentru aceasta se pot folosi **terţi de încredere** (**Autorităţi de Validare**) care fac procesări în numele clientului.
- Dialogul dintre calculatorul clientului şi serverul Autorităţii de Validare trebuie să se poarte folosind un **protocol simplu de tip cerere / răspuns** care să permită obţinerea de informaţii despre starea unui certificat digital. Răspunsurile Autorităţii de Validare trebuie semnate pentru a asigura integritatea şi autenticitatea acestora.
- **Protocoale**:
  - *Protocolul de Determinare On-line a Stării Certificatelor (OCSP – Online Certificate Status Protocol)* [RFC2560]; reprezintă un protocol simplu de tip cerere/răspuns destinat exclusiv determinării stării de revocare a certificatelor
  - *Protocolul Simplu de Verificare a Certificatelor (SCVP – Simple Certificate Validation Protocol)* elaborate de IETF PKIX. SCVP reprezintă un protocol mult mai general decât OCSP ce permite clienţilor delegarea (parţială/completă) a procesului de verificare a unui certificat digital (construirea şi validarea căi de certificare) către un server SCVP:
    - Delegated Path Discovery and
    - Delegated Path Validation
- Banda de reţea şi puterea de procesare a serverelor Autorităţii de Validare reprezintă elemente cheie de care trebuie să se ţină cont într-o implementare de acest gen.

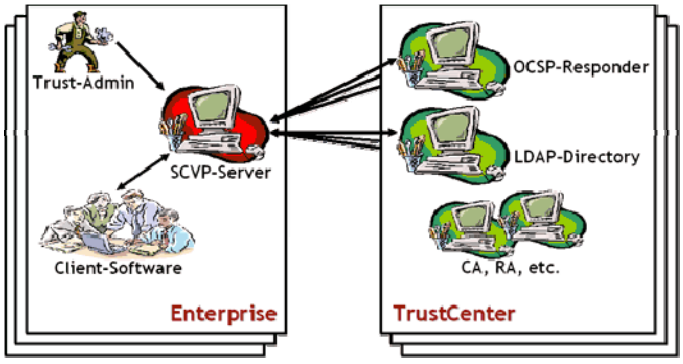
PKI Interoperability

-solutions-



PKI Interoperability

-solutions-

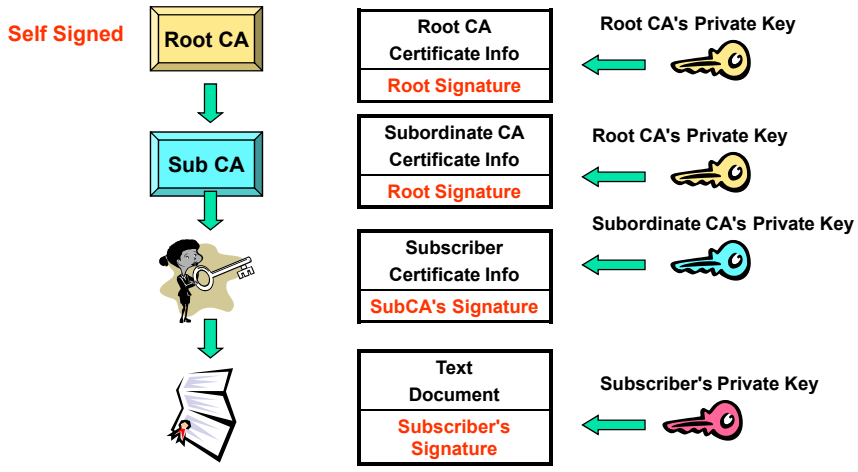


3.SERVICII ASOCIATE SEMNATURILOR ELECTRONICE

- Validarea stării certificatelor digitala
- Marcarea temporală
- Arhivarea semnăturilor electronice
- Formatul semnăturilor electronice
- Sisteme securizate pentru crearea semnăturilor
- Conceptul WYSIWYS
- Politica de semnare a documentelor
- Studiu de caz

Certificate Paths

- A **certification path** is an ordered sequence of certificates between the *end entity* and the *trusted point in the hierarchy* (i.e., root).
- The result forms a **certificate chain** that begins at the end entity and ends at the root CA



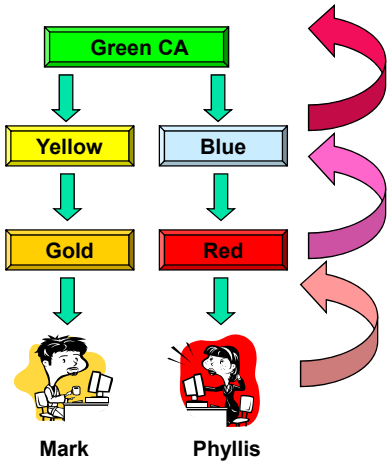
Relying Party

A relying party builds a certificate path from the other subscriber to the relying party's trust anchor

Mark gets cert from Phyllis

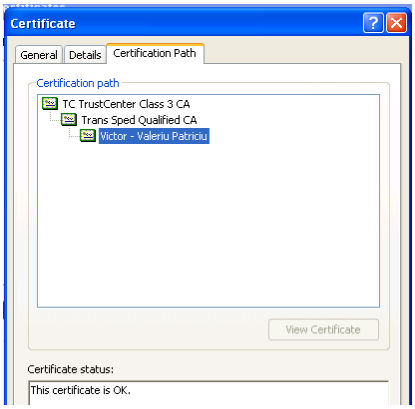
1. Phyllis's cert signed by Red CA
2. Red's cert signed by Blue CA
3. Blue's cert signed by Green CA

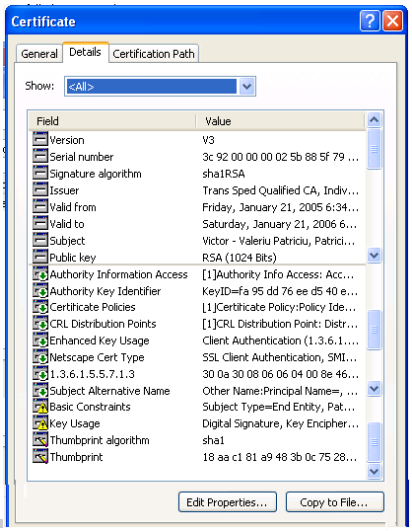
Green CA is Mark's trust anchor, therefore Mark trust's Phyllis's cert



My Certificate

- *TransSped* Certificate-
www.transsped.ro

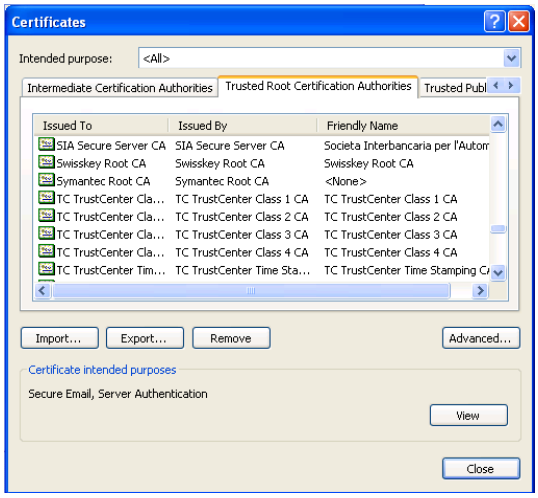




Trust Lists

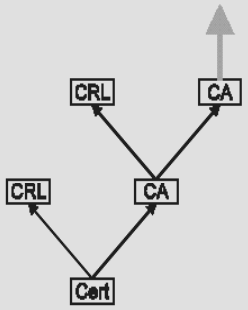
Commercial CAs often come pre-loaded

Why and how much do you trust a CA?



Certificate Verification with Directory

Checking works in reverse order to normal lookup



Check certificate
Check certificates CRL
repeat
  Check CA's certificate
  Check CA's CRL
until root reached

Scheme de validare bazate pe liste de certificate revocate

Cea mai folosită metodă de revocare a certificatelor digitale se bazează pe publicarea periodică a unei **Liste de Certificate Revocate (CRL – Certificate Revocation List),** semnată digital de Autoritatea de Certificare.

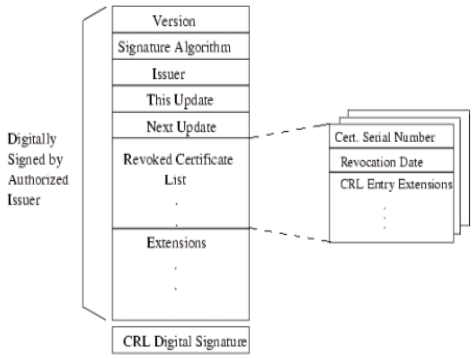


Figura 4.14. Structura unui CRL

Scheme de validare bazate pe protocoale on-line

•Protocolul de determinare on-line a stării certificatelorŞ
(OCSP – Online Certificate Status Protocol)
- protocol simplu de tip cerere/răspuns destinat exclusiv determinării stării de revocare a certificatelor.
•Clienţii OCSP trimit o **cerere** conţinând identificatorii certificatelor de validat către serverul OCSP iar acesta furnizează un răspuns privind starea fiecărui certificat.
•**Răspunsul** furnizat de serverele OCSP sunt întotdeauna semnate digital pentru a se asigura integritatea şi autenticitatea informaţiilor conţinute. Semnarea cererilor clienţilor este opţională şi se foloseşte pentru autentificarea acestora la serverul OCSP.
•Mecanismul folosit de serverul OCSP pentru obţinerea informaţiei de revocare poate fi prinŞ
- interogarea directă a bazei de date a Autorităţii de Certificare,
- procesarea CRL-urilor emise de Autoritatea de Certificare sau
- apel la serviciile unui alt server OCSP, autoritar pentru domeniul PKI în care a fost emis certificatul respectiv

•OCSP suportă extensii în cadrul mesajelor de cerere şi răspuns.

Serverele OCSP

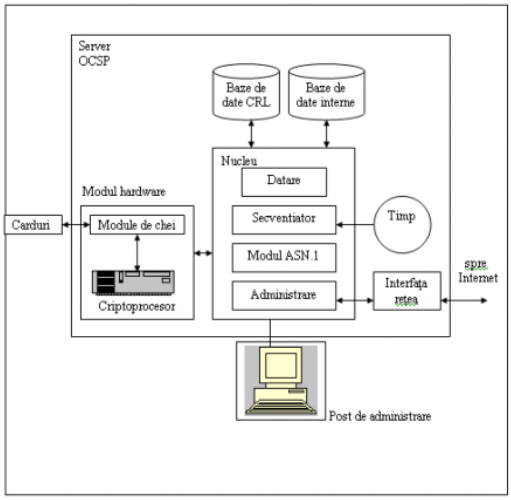
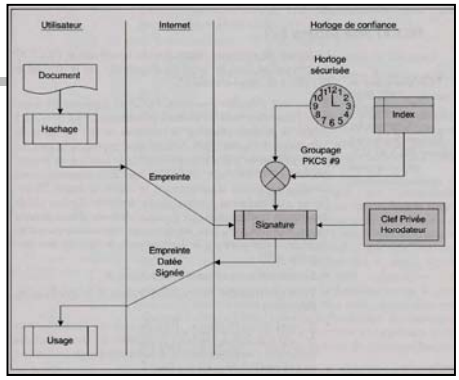


Figura 4.13 Arhitectura unui server OCSP

Time-Stamping

- PKI can enable new services between clients and Trusted-Third Parties (TTP) by supporting confidentiality and mutual authentication;
- Timestamp Servers- allow a client to prove at a later date that some datum existed before a particular time (ex. A signature was generated before a particular time);
- A protocol was completed by IETF PKIX Working Group and become RFC 3161 in 2001- *Internet X.509 PKI Time Stamp Protocol (TSP)*;
- TSP describes the format of a request sent to a Time Stamping Authority (TSA) and the response returned;

Time-Stamping



Alice has a document and she wishes to obtain a timestamp :

- Alice digitally signs the document;
- Alice sends the document hash and the signature to the TSA in a TSP request; Alice sends the hash, not the document (the contents of document remains secret)
- TSA authenticates Alice;
- TSA generates a signed response to Alice;
- Alice validates the digital signature and stores the response for later use before a legal authority;

Time-Stamp Authority

Funcţiile cerute unui ceas de încredere (**Time Stamp Authority**):

- să semneze datele urmărind protocolul TSP;
- să arhiveze durabil cererile şi răspunsurile;
- să distribuie termenul într-o manieră sigură;
- să permită consultarea arhivelor.

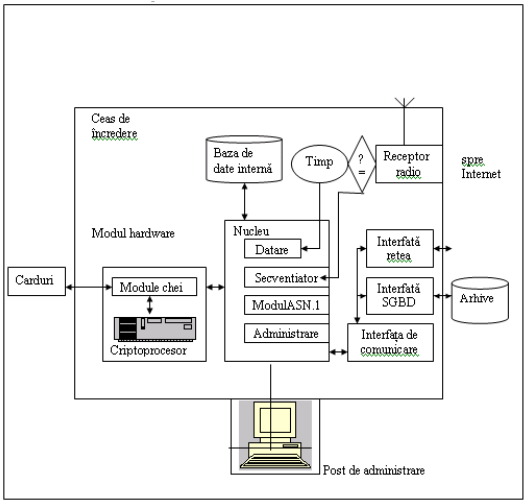
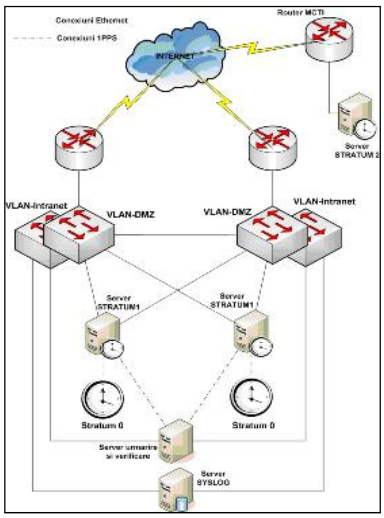


Fig. 4.7 Arhitectura unui ceas de încredere.

Time-Stamping in Romania

Solutia are la baza urmatoarele sisteme functionale:
-**Sistemul Stratum 1**, localizat la INM, compus din doua servere Stratum 1, capabile a se sincroniza cu semnalele exterioare provenite de la sursele de timp existente, in speta cu etalonul atomic de frecventa cu cesiu (etalonul national de timp si frecventa al Romaniei)
- **Sistem de logare**, cu posibilitate de cautare/arhivare a informatiilor pentru toate elementele sistemului
- **Sistem Stratum 2**, compus dintr-un server Stratum, cu acces nerestrictionat, trasabil la cele 2 servere Stratum 1
- **Sistem pentru verificarea serverelor NTP** capabil sa genereze un semnal 1PPS sincron cu orice server NTP care se doreste a fi verificat/urmarit
- **Conectivitate la Internet**, redundanta, prin 2 provideri diferiti
- **Sistem de rutare redundant**, independent de provider, compus din 2 echipamente router si doua switchuri layer 3, la nivelul caruia este implementata si solutia de control a accesului
- **Sistem de electroalimentare de siguranta**, compus din 5 UPS-uri dubla conversie de 1,5 KVA, avand o autonomie de functionare de 6 minute si un grup electrogenerator de 30 KVA, cu functionare de 50 de ore.



Algoritmul de validare a semnăturilor electronice folosind amprente de timp

Pentru a determina **validitatea semnăturii** (lui A) trebuie parcurşi următorii paşi:

- Se verifică amprenta de timp şi faptul că ea a fost generată pentru semnătura .
- Se extrage timpul de generare a semnăturii *Tg* din amprenta de timp.
- Se identifică şi se obţine certificatul digital al lui A din momentul semnării documentului.
- Timpul de generare a semnăturii *Tg* trebuie să se încadreze în perioada de validitate a certificatului digital al lui *A*.
- Certificatul digital al lui *A* nu trebuie sa fi fost revocat înainte de momentul *Tg*.
- Se verifică semnătura folosind cheia publică din certificatul digital al lui *A*.

Standards

PKCS « *Public-Key Cryptography Standards* »

- PKCS#1 : RSA Cryptography Specifications Version 2
- PKCS#2 : inclus dans PKCS#1
- PKCS#3 : Diffie-Hellman Key Agreement Standard Version
- PKCS#4 : inclus dans PKCS#1
- PKCS#5 : Password-Based Cryptography Standard Version 2
- PKCS#6 : Extended-Certificate Syntax Standard Version 1.5
- PKCS#7 : Cryptographic Message Syntax Standard
- PKCS#8 : Private-Key Information Syntax Standard
- PKCS#9 : Selected Attribute Types Version 2.0
- PKCS#10 : Certificate Signing Request (CSR)
- PKCS#11 : Cryptographic Token Interface
- PKCS#12 : Personnal Information Exchange Syntax
- PKCS#13 : Elliptic Curve Cryptography Standard
- PKCS#14 : Pseudorandom Number Generation Standard
- PKCS#15 : Cryptographic Token Information Format

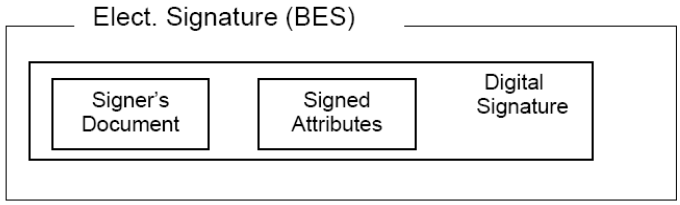
Electronic Signature Format Standards

Cryptographic Message Syntax(CMS) Standard

- Standard for cryptographic protected messages, used to digitally sign, digest, authenticate or encrypt any form of digital data.
- CMS is based on the syntax of **PKCS#7**
- The newest version of CMS (2004) is specified in **RFC 3852** (inlocuieste vechiul RFC 3369).
- The architecture of CMS is built around certificate-based key management, such as profile defined by PKIX working group.
- CMS is used as cryptographic component of other standards
  - RFC 2633/2634- **S/MIME** & **Enhanced Security Services for S/MIME**,
  - RFC 3369/vechiul 3852 **Cryptographic Message Syntax (CMS)**
  - RFC 3280 **X.509 PKI (PKIX) Certificate and CRL Profile**
  - RFC 3161 **Digital timestamping protocol**
  - RFC 3126 **Electronic Signature Formats -long term signatures**
  - RFC 3125- **Electronic Signature Policies**
  - RFC 5126 **CMS Advanced Electronic Signatures (CAdES)**-vechiul 3126

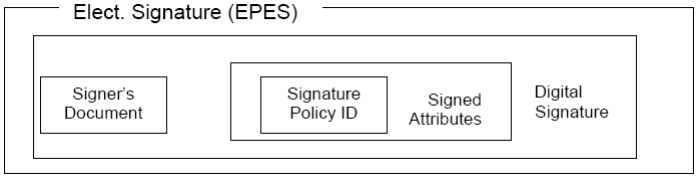
ETSI TS 101 733 V1.5.1
Electronic Signature Formats

1. Basic Electronic Signature (BES) contains:
- The signed user data (e.g. the signer's document) as defined in CMS (RFC 3369);
- A collection of mandatory signed attributes as defined in CMS (RFC 3369) and in ESS (RFC 2634);
- Additional mandatory signed attributes defined in the present document;
- The digital signature value computed on the user data and, when present, on the signed attributes, as defined in CMS (RFC 3369).



ETSI TS 101 733 V1.5.1
Electronic Signature Formats

2. Explicit Policy-based Electronic Signature (EPES)
- Extends the definition of an electronic signature to conform to the identified signature policy.
- Incorporates a **signed attribute (signature-policy-identifier)** indicating that a signature policy that is mandatory to use to validate the signature and specifies explicitly the signature policy that shall be used.
- This signed attribute is protected by the signature. The signature may also have other signed attributes required to conform to the mandated signature policy.



ETSI TS 101 733 V1.5.1
Electronic Signature Formats

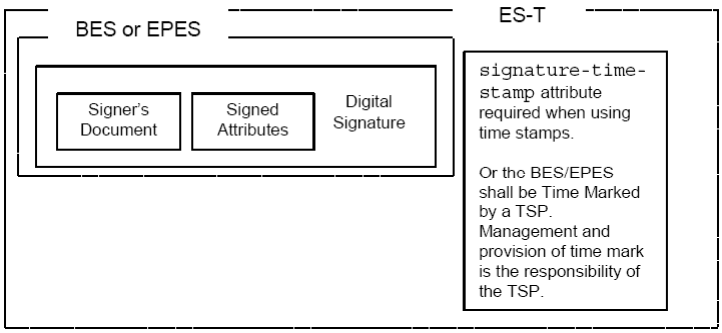
3. Electronic signature formats with validation data

Validation of an electronic signature requires additional validation data needed to validate the electronic signature:

- CA certificates
- Revocation status information in the form of Certificate Revocation Lists (CRLs) or certificate status information (OCSP) provided by an on-line service.
- Evidence that the signature was created before a particular point in time this may be either a time-stamp token (created by a TSA) or time-mark (information in an audit trail from a TMA- Trust Mark Authority - trusted third party that creates records in an audit trail in order to indicate that a datum existed before a particular point in time that binds a representation of a datum to a particular time, thus establishing evidence that the datum existed before that time.
- Details of a signature policy used to verify electronic signature.

ETSI TS 101 733 V1.5.1
Electronic Signature Formats

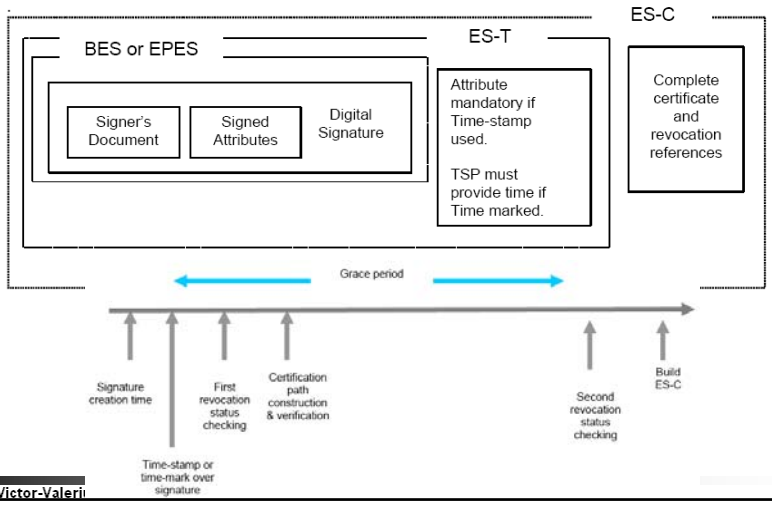
3.1 Electronic Signature with TimeStamp (ES-T)



Prof.Dr.Victor-Valeriu PATRICIU

ETSI TS 101 733 V1.5.1
Electronic Signature Formats

3.2 ES with Complete validation data references (ES-C)

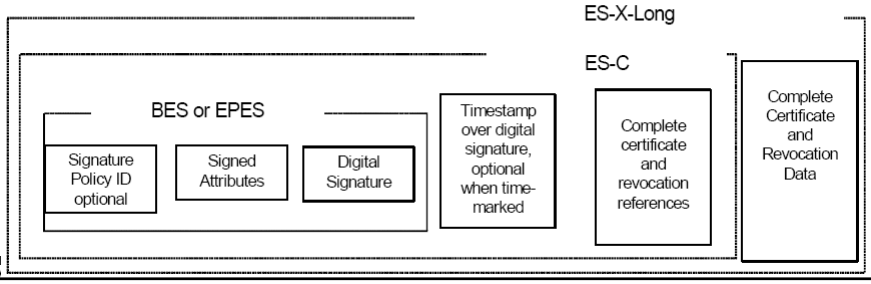


Prof.Dr.Victor-Valeri

ETSI TS 101 733 V1.5.1
Electronic Signature Formats

3.3 Extended electronic signature formats- ES-C can be extended by adding *unsigned attributes* to the electronic signature.

3.3.1. EXtended Long Electronic Signature (ES-X Long)- adds to the ES-C format the certificate-values and revocation-values attributes. The first one contains the whole certificate path required for verifying the signature; the second one the CRLs and/or OCSP responses required for the validation of the signature. This provides a know repository of certificate and revocation information required to validate an ES-C and prevents such information getting lost.

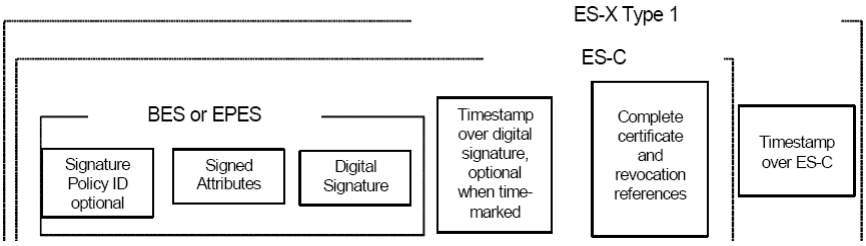


Pro

ETSI TS 101 733 V1.5.1
Electronic Signature Formats

3.3 Extended electronic signature formats

3.3.2. EXtended Electronic Signature with Time Type 1 (ES-X Type 1)- adds to the ES-C format the ES-C-time-stamp attribute, whose content is a time-stamp token on the ES-C itself. This provides an integrity and trusted time protection over all the elements and references. It may protect the certificates, CRLs and OCSP responses in case of a later compromise of a CA key, CRL key or OCSP issuer key

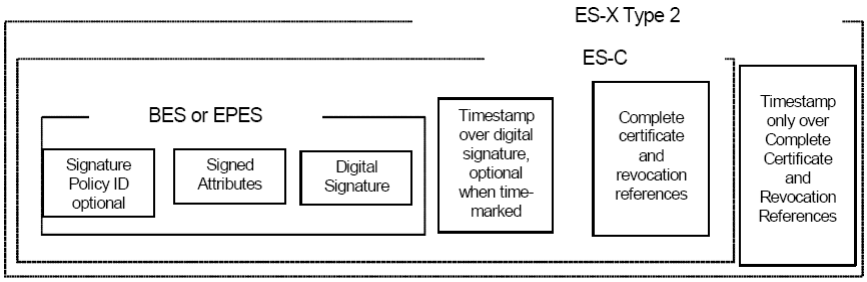


Prof.Dr.Victor-Valeriu PATRICIU

ETSI TS 101 733 V1.5.1
Electronic Signature Formats

3.3 Extended electronic signature formats

3.3.3. EXtended Electronic Signature with Time Type 2 (ES-X Type 2)- adds to the ES-C format the ES-C-time-stamped-certs-crls-references attribute, whose content is a time-stamp token on the certification path and revocation information references. This provides an integrity and trusted time protection over all the references. It protect the certificates, CRLs and OCSP responses in case of a later compromise of a CA key, CRL key or OCSP issuer key.

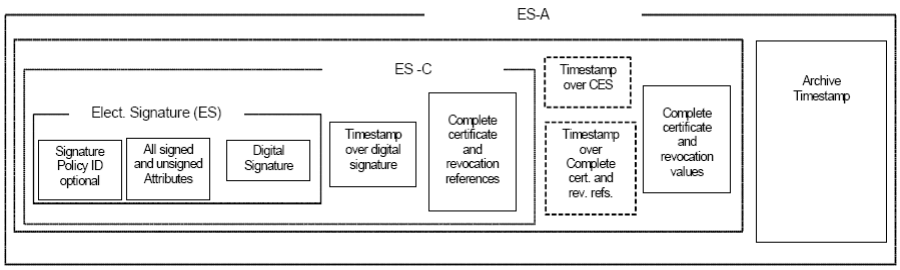


Prof.Dr.Victor-Valeriu PATRICIU

ETSI TS 101 733 V1.5.1
Electronic Signature Formats

3.3 Extended electronic signature formats

3.3.4. Archival Electronic Signature (ES-A) - builds on an ES-X Long or an ES-X Long Type 1 or 2 by adding one or more archive-time-stamp attributes. This form is used for archival of long-term signatures. Successive time-stamps protect the whole material against vulnerable hashing algorithms or the breaking of the cryptographic material or algorithms.



PKI Policies

- Certificate Policy (CP)
  - High level document
  - Describes security policy for operating the CA
  - Defines roles and responsibilities
    - How CA will be managed
    - How registration will be performed (i.e., identity proofing requirements)
    - How subscribers use and handle their certificates and keys
- Certification Practices Statement (CPS)
  - Detailed document
  - Describes mechanisms and procedures followed by CA to meet the requirements of their CP
  - Effectively the CA's operations manual.
- Together, Determines *Assurance Level*
  - How much you should trust the CA's certificates

PKI Organizational- studiu de caz

Infrastructura PKI organizationala va asigura:

•identitatea utilizatorilor electronici
•autentificarea si autorizarea accesului la sistemele informatice ale organizatiei
•servicii de securizare a schimbului de informatii intre utilizatorii si/sau sistemele informatice ale organizatiei
•servicii de validare in timp real a certificatelor digitale
•servicii de recuperare a cheilor private de criptare
•servicii de marcare temporala
•suport pentru interconectarea cu PKI ale institutiilor externe ca element de baza pentru schimbul securizat de informatii intre acestea si organizatie
•scalabilitate pentru dezvoltari ulterioare.

La **nivel central** vor exista componente cel putin pentru urmatoarele servicii:

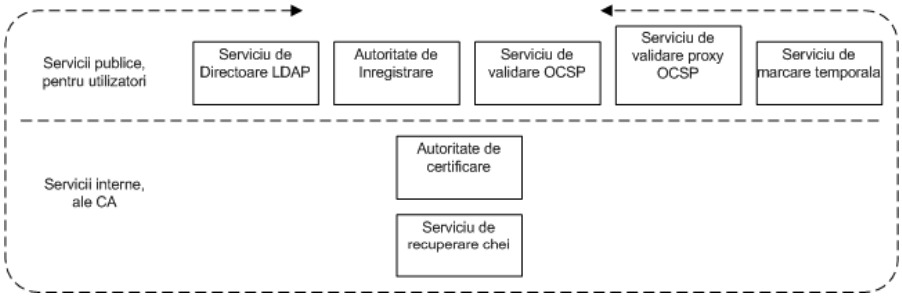
• **LDAP** – prin care se va asigura posibilitatea de acces controlata la directoarele LDAP din toate structurile organizatiei
• **OCSP Proxy** – prin care se va asigura rutarea tuturor mesajelor de tip OCSP din cadrul organizatiei
• **Server de timp** – va reprezenta sursa unica de timp in organizatie si va fi conectata la sursa unica de timp nationala gestionata de MCSI -Legea marcii temporale (451/2004)
• **Autoritatea de Certificare (CA)** este elementul de baza al unei PKI- este compusa din elemente hardware, software si din personalul care le utilizeaza. Functiile de baza:
  •Emite certificate (le creeeaza si le semneaza)
  •Mentine informatii despre starea certificatelor si emite liste de certificate revocate (CRL)
  •Publica certificatele neexpirate si CRL
  •Mentine arhive cu informatii despre certificatele revocate sau expirate

PKI Organizational

La **nivelul fiecarei structuri componenta a organizatiei** se vor implementa urm. **servicii PKI**:

• **Autoritati de Certificare** ce emit certificate digitale utilizatorilor si echipamentelor din structura
• **Autoritate de Inregistrare** ce permite primirea cererilor de certificate digitale in mai multe locatii din teritoriu, verificarea utilizatorilor si transmiterea certificatelor emise catre utilizatorii finali.
• **Serviciu de directoare LDAPv3** utilizat pentru publicarea certificatelor emise si a CRL.
• **Serviciu OCSP** de validare on-line a starii certificatelor emise de CA-ul/CA-urile structurii
• **Serviciu proxy OCSP** de validare on-line a starii certificatelor digitale emise de un alt CA.
• **Serviciu de recuperare a cheilor private** de criptare in conditii maxime de securitate – existenta acestui serviciu implica automat cerinta ca acele chei care se vor utiliza in scop de criptare sa nu poata fi utilizate si in scop de semnare, deoarece existenta unei copii pentru cheia de semnare presupune incalcarea cerintei de non-repudire (utilizatorul poate nega ca a semnat).
• **Serviciul de marcare temporala** pentru adaugarea informatiilor privind momentul de timp la care o semnatura electronica era atasata unui document.

PKI Organizational



PKI Organizational

Aplicatii ce utilizeaza PKI

- Aplicatie pentru autentificare unitara la aplicatii Web pe baza de certificat digital
- Aplicatie de securitate pentru statiile de lucru
  - Asigurarea confidentialitatii informatiilor
  - Criptarea informatiilor la nivelul partitiilor sistemului de operare
  - Criptarea fisierelor individuale
  - Criptarea mesajelor e-mail
  - Distrugerea informatiilor prin rescriere cu date aleatoare
  - Asigurarea autenticitatii, integritatii si non-repudierii informatiilor
- Semnarea digitala a fisierelor
- Semnarea digitala a mesajelor e-mail
- Aplicatie pentru management securizat de documente
- Sistem pentru mesagerie electronica securizata

4.SMART-CARDURI, BIOMETRICE & SEMNATURILE ELECTRONICE

- Carduri pentru semnatura digitala
- ID Cards
- Clasificarea metodelor biometrice
- Folosirea sistemelor biometrice pentru semnăturile electronice

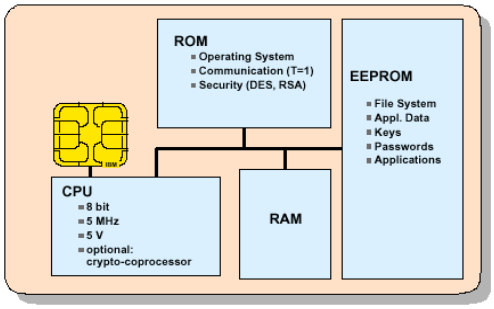
How the Card Became Smart

- **Memory cards**

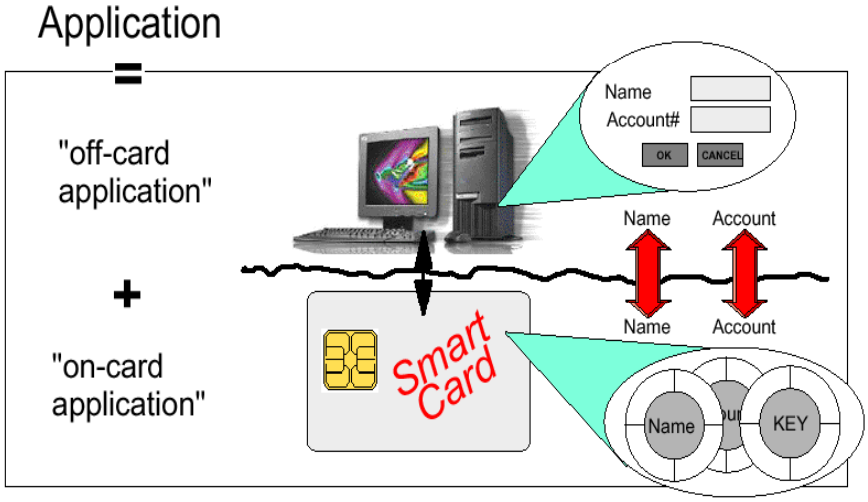
- **Magnetic stripe**

- **Embossing**

- **Processor cards (Smart Cards)**
  - More secure
  - Multi-application capable
  - Added functionality
  - Coexistence of contact and contactless option



Parts of a Smart Card Application



DoD Smart-Card for Military Use

*US DoD **Common Access Card** contains a computer chip with 32-kilobytes of memory. The memory stores three software certificates that are managed by NSA and DISA*

*This **fingerprint reader** combines PKI and biometrics. In use, a smart card with a fingertip pattern of the user in its memory is inserted into the end of the reader. When the user places a finger on the reader, software matches the user's fingerprint with the stored template in the card.*

e-Passport

Yesterday

- Machine readable passport

Today

- Electronic passport with digital image

Tomorrow

- From 2009 passport with secondary biometric information

The European Electronic Passport

- Council decision of 13 December 2004 (Regulation (EC) 2252/2004):
  - The facial image will be required at the latest **18** months- February 2005, deadline August 2006
  - the fingerprints will be required mandatory at the latest **36** months- June 2006, deadline June 2009

  after the date of adoption of technical specifications necessary for the implementation of the Regulation
- Facial images:
  - Comission decision 409(2005) - Technical specifications on the standards for security features and biometrics in passports and travel documents issued by Member States
- Fingerprints:
  - Comission decision 2909 (2006)- echnical specifications on the standards for security features and biometrics in passports and travel documents issued by Member States
- Participants: all MS except UK, IRL + NOR

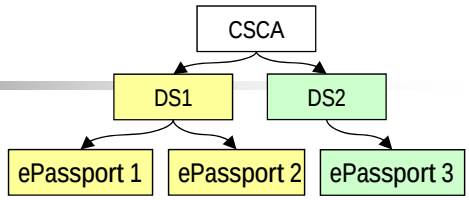
Electronic passport

- Classical passport booklet + passive contactless smartcard
- Chip & antenna integrated in a page or cover
- Technical specification standardized by ICAO (International Civil Aviation Organization)
  - Standard 9303, 6th edition
  - References many ISO standards
- Communication is based on ISO 14443 & 7816
- Data is organised in
  - 16 data groups (DG1-DG16)
  - 2-3 meta files (EF.COM, EF.SOD, EF.CVCA)

Authentication & ePassports

- ICAO Obligatory
  - Passive authentication (authenticity of data)
- ICAO Optional
  - Basic Access Control (limits remote readability)
  - Active Authentication (authenticity of chip)
- European Extended Access Control
  - Chip Authentication (authenticity of chip)
  - Terminal Authentication (authorization to read biometric data)
- Holder Authentication
  - Facial image, Fingerprint, Iris
  - Signature

Passive Authentication



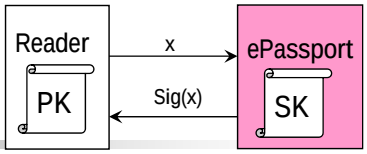
- The list of the hashes (SHA-1/2) of all present data groups is digitally signed by the issuing organisation (Document Signer)
  - State printer
  - Embassy
  - Etc.
- The X.509 certificate of the Document Signed issued by the CA of the issuing country (CSCA- Country Signer CA – e.g. the ministry of interior) is included.
- The CSCA certificates (Country Signer Certification Authority) must be exchanged bilaterally.
- A central ICAO directory for CRLs and DS certificates is planned.
- Passive authentication is a mandatory security feature of all ePassports.

Passive Authentication

- The file EF.SOD contains a CMS (PKCS#7) SignedData structure (file is read and validated by inspection system)
  - The signed data is the list of hashes of the data groups
  - The DS certificate is included (ICAO optional, EU mandatory)
  - Data is signed by the DS
  - Interoperability problems: hash algorithm mismatch, the order of RDNs of Issuer
- Signature algorithms
  - RSA with PKCS#1 v1.5 padding
  - RSA with PSS padding
  - DSA (not standardized for key lengths > 1024)
  - ECDSA (domain parameters must be specified)
- Message Digest algorithms
  - SHA-1 and all SHA-2 (*SHA-224*, *SHA-256*, *SHA-384*, and *SHA-512)* algorithms

Active Authentication

- Active authentication verifies whether the chip is authentic (not cloned)
- Asymmetric key pair is stored in the chip
  - The public key is accessible in DG15 (i.e. integrity protected by PA)
  - The private key does not leave the chip, no way to read the key, but possible to verify whether the chip can access the private key
- Reader generates a random number and send to chip to sign
  - The signature is verified using the public key from DG15
- AA is an optional feature of electronic passports (chip must support cryptographic operations)
- In practice only RSA implementations (DSA and ECDSA theoretically permitted as well)
- ISO 9796-2 scheme 1



Basic Access Control (BAC)

- Contactless interface is both advantage and disadvantage
- BAC allows to read the data only after the reader (in fact mutual) authentication
  - The reader must prove the knowledge of the MRZ (Machine Readable Zone) of the passport
- BAC is ICAO optional (recommended) feature, in EU mandatory
- The authentication key is derived from document#, DoB, DoE
  - Low entropy (3DES max 112b, BAC max 56/74b, in practice 30-50b)
- Interoperability issues
  - Modification of the derivation of the static key rejected by ICAO in order not to break interoperability
  - How to find out the passport is BAC-protected → try & error

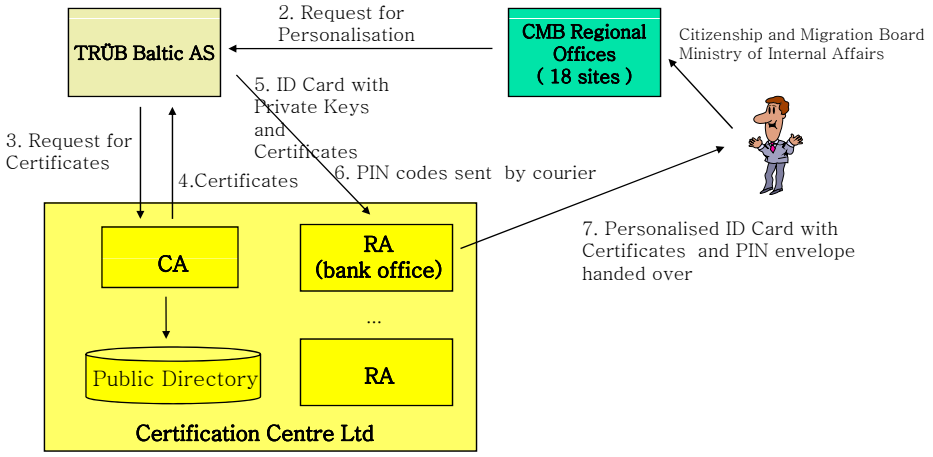
Extended Access Control (EAC)

- **Fingerprints** (DG3) in the EU passports will be protected by additional mechanism
- Reading is allows only by those who got authorisation of the issuing country
- Authorisation is based on two-level PKI and challenge-response protocol
  - So called Terminal Authentication
  - CV certificates (encapsulation in 7F21 tag, coding of integers,…)
- EAC specification also introduces chip authentication, which replaces AA (and restarts SM with stronger keys)
  - DH and ECDH, public key stored in DG14
  - Format of DG14 - to enable worldwide interoperability (DG14 is not specific to European EAC)

Passport Biometrics

- Biometric authentication of the passport holder
  - Facial image (DG2, ISO 19794-5 [facial image])
    - JPEG or JPEG2000 image
    - Basic, Full Frontal, Token Image
    - Feature points (e.g. eyes)
    - Coding of some values changed between CD and FDIS
  - Fingerprint (DG3, ISO 19794-1 [finger image])
    - Uncompressed, WSQ, PNG, JPEG or JPEG2000
    - How to indicate the fingerprint cannot be enrolled (no DG3, empty DG3, no template), how to store 2 fingerprints (2 images, 2 templates)
  - Iris image (DG4, ISO 19794-6 [iris image])
- Quality of biometric data

Estonia Card issuance



Why Biometrics ?

- Only biometrics can verify *you* as *you*
- Tokens (smartcards, etc.) aren't you and,
  - can be lost
  - can be stolen
  - can be duplicated (some)
  - can be forgotten
- Passwords aren't you and,
  - can be forgotten
  - can be shared
  - can be observed
  - can be broken

Biometrics & Electronic Signatures

- In the last decade, many investigations have been made in the field of **biometrical authentication**, i.e. verification or identification of a person by using biometrical features.
- In several countries, the Public Key Infrastructure (PKI) - reached a stage where Certificate Service Providers are able to produce Qualified Certificates and to offer directory and time stamp services
- The smartcard technology as the most important representative of technologies for secure signature creation devices (SSCDs),is capable to execute:
  - signature algorithms and
  - to provide storage for certificates

Biometrics & Electronic Signatures

- Creation of an electronic signature is a security function which has to be protected against unauthorised use
- The usual way for the signer authentication is a **know-ledge based mechanism:**
  - Personal Identification Number (PIN)
  - Password
- **Biometrical authentication mechanisms** are suitable as addition or alternative for electronic signatures
- Electronic signatures are produced at signature creation systems (SCS) using secure signature creation devices (SSCDs). A SSCD may be:
  - under signer´s control and used at home, in the office or mobile at any place or
  - under service provider´s control (e.g. a Public Signature Terminal at an airport or a banking terminal).

Biometrics & Electronic Signatures

- Biometric authentication - advantage over knowledge-based methods that it is not possible to give the biometric feature to someone else (intentionally or not)
- The EU directive for electronic signatures requires that an "advanced electronic signature shall be uniquely linked to the signatory":
  - for knowledge-based mechanisms the SSCD has to verify that the presented PIN or password is identical with the reference data stored in the SSCD
  - for biometric mechanisms, the SSCD has to compare the biometric verification data derived from the live presented biometric feature with the biometric reference data stored in the SSCD and to verify whether the probability is high enough to ensure that the person presenting the biometric feature is the legitimate user.

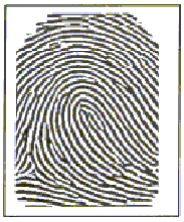
Biometric Methods and Characteristics

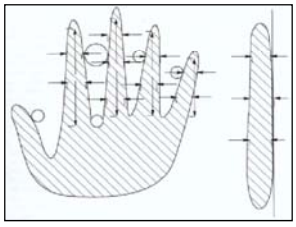
Static Methods
- Fingerprint
- Facial Features
- Hand Geometry Measurement
- Iris Feature
- Retina Identification
- Vein Recognition

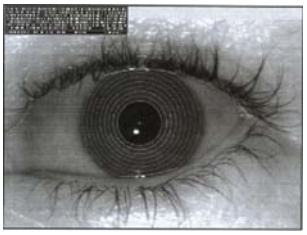
Dynamic Methods
- Speaker Recognition
- Signature Dynamics
- Keystroke Dynamics

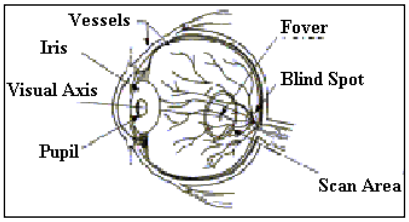
New Biometric Methods under Development
- Skin/ epithel structure – ultrasound finger identification
- Facial thermogram – infrared identification (IRID)
- Palmprint
- Odour measurements
- Ear shape recognition
- DNA-based identification

Biometric Methods









Signature & Biometrics

Standards and Specifications

ISO/IEC 7816 -"Personal verification through biometric methods in integrated circuit(s) cards". consists of 3 sections:

- the main part, in which the commands VERIFY, GET CHALLENGE and EXTERNAL AUTHENTICATE together with the biometrics related data objects BDT and BIT are specified
- annex A, which provides information about biometric authentication processes
- annex B, which contains examples for enrollment & verification

ANSI/NIST Standard for Coding Biometric Data - standards for formats of the following biometric data:

- Facial images
- Fingerprint images
- Fingerprint minutiae.

Signature & Biometrics

Standards and Specifications

Crypto Standards PKCS

-PKCS#15: Cryptographic Token Information Syntax Standard

-PKCS#11: Cryptographic Token Interface Standard

BioAPI -BioAPI Consortium was founded in April 1998 in order to develop a widely available and widely accepted API that will serve for various biometric technologies. In March 1999, the Human Authentication API (HA-API) merged their activities with the Bio-API Consortium. The following goals are defined in:

- Rapid development of applications employing biometrics
- Flexible deployment of biometrics across platforms & OS
- Ability to exploit price performance advances in biometrics
- Enhanced implementation of multiple biometric alternatives (fingerprint, voice, face, iris, etc.)

Common Biometric Exchange File Format (CBEFF) enable interoperability of biometric based application programs from different vendors.

Signature & Biometrics

Conclusions

The use of biometric authentication in the context of electronic signatures - the **favourite candidates** for this context will be

- fingerprint
- face recognition
- signature dynamics,

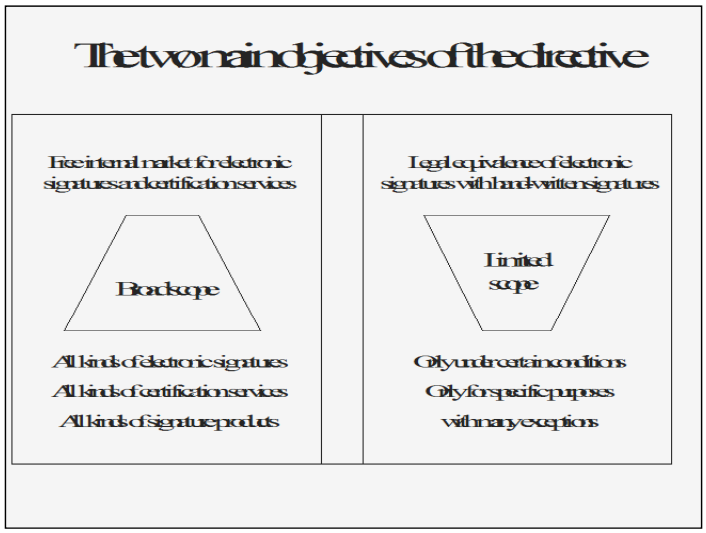
There are still considerable problems:

- the resistance against attacks is not sufficient
- in many cases, the overall performance should be improved
- no crypto sensor units with feature extraction are available for methods where biometric verification data needs to be secured
- the reliability of some solutions seems not to be sufficient
- the realisation of smartcards with sensor, feature extraction and feature matching remains still a great challenge
- there are no standardised algorithms to ensure interoperability, - there is less experience in evaluation, testing, determination of strength of function and comparison of biometric solutions.

5. LEGISLATIA DOCUMENTELOR & SEMNATURILOR ELECTRONICE

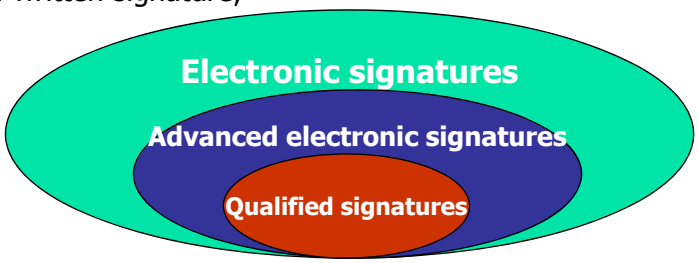
- **Semnături electronice versus semnături digitale**
- **Reglementările Uniunii Europene**
- **Standardizarea semnăturilor electronice în UE**
- **Reglementări in Romania**
  - Legea semnaturii electronice
  - Legea marcii temporale
  - Legea notarilor electronici
  - Acreditarea Furnizorilor de Servicii de Certificare

EU Directive on Electronic Signature - 1999/93/EC



Legal Recognition

- General principle: Legal effect for all electronic signatures;
- Second principle: Certain electronic signatures get the same legal effect as hand-written signature;



Qualified signature:
- ✓advanced electronic signature +
- ✓qualified certificate +
- ✓secure signature creation device.

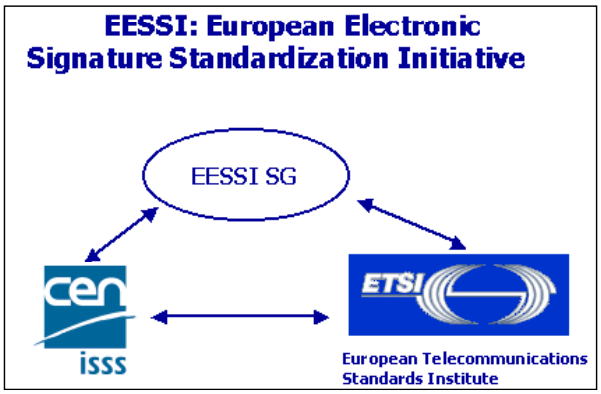
Technical Framework for Qualified Electronic Signatures

- Although "technology neutral", the Directive implicitly defines a technical framework
- A proposed first set of components that can be used:
  - ✓Asymmetric cryptography: RSA, DSA, ECDSA
  - ✓Certificate based verification using ITU X.509
  - ✓Public Key Infrastructure with CAs and Directories
  - ✓Smart-cards/hardware tokens for private key protection
- Reasons for this selection:
  - ✓Generally accepted, existing standards
  - ✓ *Urgent need for standardized use of these technologies*!

Annexes of Directive

- **Annex I:** Requirements for qualified certificates
- **Annex II:** Requirements for certification-service-providers issuing qualified certificates
- **Annex III:** Requirements for secure signature-creation devices
- **Annex IV:** Recommendations for secure signature verification

EESSI: European Electronic Signature Standardization Initiative



CEN/E-SIGN Workshop

Security Requirements for Trustworthy Systems

CWA 14167: Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures,

- Part1: System Security Requirement
- Part2: Cryptographic Module for CSP Signing Operations- Protection Profile

CWA 14170: Security Requirements for Signature Creation Systems,

CWA 14171: Procedures for Electronic Signature Verification

CWA 14172: EESSI Conformity Assessment Guidance

- Part1: General
- Part2: Certification Authority Services and Processes
- Part3:Trustworthy Systems Managing Certificates for Electronic Signatures
- Part4: Signature Creation Applications & Procedures for Signature Verification
- Part5: Secure Signature Creation Devices

SSCD

CWA 14168: Secure Signature-Creation Devices, version 'EAL 4',

CWA 14169: Secure Signature-Creation Devices, version 'EAL 4+'

ETSI/ESI Working Group

Requiremets for CSP

ETSI TR 102 030 **Provision of harmonized Trust Service Provider status information**
ETSI TR 102 040 **International Harmonization of Policy Requirements for CAs issuing Certificates**
ETSI TS 102 042 **Policy requirements for certification authorities issuing public key certificates**
ETSI TS 101 456 **Policy requirements for certification authorities issuing qualified certificates**

Qualified Certificate Format (Profile) and Policy

ETSI TS 101 862 **Qualified certificate profile**
ETSI TR 102 041 **Signature Policies Report**
ETSI TR X **XML Format for Signature Policies**

Electronic Signature Format

ETSI TS 101 733 **Electronic Signature Formats**
ETSI TS 101 903 **XML Advanced Electronic Signatures (XAdES)**

Time-stamping Protocol

ETSI TS 101 861 **Time stamping profile**
ETSI TS 102 023 **Policy requirements for time-stamping authorities**

ROMANIA
LEGE
privind semnatura electronica

- Adoptata de Palamentul Romaniei in iulie 2001- **LEGE nr.455 din 18 iulie 2001**;
- Stabileste:
  - regimul juridic al inscrisurilor in format electronic,
  - conditiile furnizarii de servicii de certificare a semnaturilor electronice.

LEGE privind semnatura electronica
-Definitii-

- **Semnatura electronica** reprezinta o colectie de date in format electronic incorporate, atasate sau asociate unui inscris in format electronic cu intentia de a produce efecte juridice si care permite identificarea formala a semnatarului.
- **Semnatura electronica extinsa** reprezinta acea semnatura electronica care indeplineste cumulativ urmatoarele conditii:
  - este legata in mod unic de semnatar;
  - asigura identificarea semnatarului;
  - este creata prin mijloace controlate exclusiv de catre semnatar;
  - este legata de inscrisul electronic la care se raporteaza in asa fel incat orice modificare ulterioara a acestuia este identificabila
- **Semnatar** reprezinta o persoana fizica ce detine un mecanism de creare a semnaturii si care actioneaza fie in nume propriu, fie ca reprezentant al unui tert

LEGE privind semnatura electronica
-Definitii-

- **Date de creare a semnaturii** reprezinta orice date in format electronic cu caracter de unicitate, inclusiv coduri sau *chei criptografice private*, care sunt folosite de semnatar pentru crearea unei semnaturi electronice.
- **Date de verificare a semnaturii** reprezinta orice date in format electronic, inclusiv coduri sau *chei criptografice publice*, care sunt folosite in scopul verificarii unei semnaturi electronice.
- **Certificat** reprezinta un inscris in format electronic care cuprinde atestarea legaturii ce exista intre o persoana si datele de verificare a semnaturii electronice (chei criptografice publice) si care confirma identitatea acelei persoane.
- **Certificat calificat** reprezinta un certificat care satisface conditiile prevazute in lege si care este eliberat de un furnizor de servicii de certificare ce satisface conditiile legii.

LEGE privind semnatura electronica
-Definitii-

- **Mecanism de creare a semnaturii** - un program informatic, insotit de echipamentul tehnic adecvat, configurat pentru punerea in aplicare a datelor de creare a semnaturii.
- **Mecanism securizat de creare a semnaturii** reprezinta acel mecanism de creare a semnaturii care indeplineste cumulativ urmatoarele conditii:
  - datele de creare a semnaturii, nu pot aparea practic decat o singura data si confidentialitatea acestora poate fi asigurata;
  - datele de creare a semnaturii, nu pot fi deduse si semnatura este protejata impotriva falsificarii prin mijloacele tehnice disponibile la momentul respectiv;
  - datele de creare a semnaturii pot fi protejate in mod efectiv de catre semnatar impotriva utilizarii acestora de catre persoane neautorizate;
  - sa nu modifice inscrisul electronic ce trebuie semnat si nici sa nu impiedice ca acesta sa fie prezentat semnatarului inainte de finalizarea semnarii.
- **Mecanism de verificare a semnaturii** - un program informatic, insotit de echipamentul tehnic adecvat, configurat pentru punerea in aplicare a datelor de verificare a semnaturii.

LEGE privind semnatura electronica
-Definitii-

- **Furnizor de servicii de certificare** reprezinta orice persoana, romana sau straina, care elibereaza certificate sau presteaza alte servicii legate de semnatura electronica
- **Furnizor de servicii de certificare calificata** este acel furnizor de servicii de certificare care elibereaza certificate calificate.
- **Produs asociat semnaturii electronice** reprezinta orice program informatic sau echipament tehnic destinat a fi utilizat de un furnizor de servicii de certificare pentru prestarea serviciilor legate de semnatura electronica sau destinat a fi utilizat pentru crearea sau verificarea semnaturii electronice .

LEGE privind semnatura electronica
-Regimul juridic inscrisurilor electronice -

- **Inscrisul in format electronic** caruia i s-a incorporat, atasat sau asociat:
  - o semnatura electronica extinsa,
  - bazata pe un certificat calificat nesuspendat sau nerevocat la momentul respectiv
  - generata cu ajutorul unui mecanism securizat de creare a semnaturii

este **asimilat**, in ce priveste conditiile si efectele sale, cu **inscrisul sub semnatura privata**;

LEGE privind semnatura electronica
-Regimul juridic inscrisurilor electronice -

- Partea care invoca inaintea instantei o **semnatura electronica extinsa** trebuie sa probeze ca aceasta indeplineste conditiile prevazute de lege:
  - Semnatura electronica extinsa
  - Bazata pe un certificat calificat
  - Eliberat de un furnizor de servicii de certificare acreditat

LEGE privind semnatura electronica
-Furnizarea serviciilor de certificare -

- Furnizarea serviciilor de certificare de catre persoanele fizice sau juridice *nu este supusa nici unei autorizari prealabile*;
- Furnizarea serviciilor de certificare de catre furnizorii stabiliti in statele membre ale Uniunii Europene se face in conditiile prevazute in Acordul European instituind o asociere intre Romania, statele membre ale UE;
- Persoanele care intentioneaza sa furnizeze servicii de certificare au obligatia de a notifica **autoritatea de reglementare si supraveghere (ARS)** cu privire la data inceperii acestor activitati;
- O data cu notificarea, **furnizorii de servicii de certificare (FSC)** au obligatia de a comunica ARS toate informatiile referitoare la procedurile de securitate si de certificare utilizate, precum si alte informatii cerute de ARS.
- FSC au obligatia de a comunica ARS orice modificare a procedurilor de securitate si de certificare;
- FSC sunt obligati sa respecte pe parcursul desfasurarii activitatii procedurile de securitate si de certificare declarate.

LEGE privind semnatura electronica
-Furnizarea serviciilor de certificare -

- FSC au obligatia de a crea si mentine un **registru electronic de evidenta a certificatelor eliberate (REECE)**, care trebuie sa faca mentiune despre:
  - data si ora exacta la care certificatul a fost eliberat;
  - data si ora exacta la care expira certificatul;
  - daca este cazul, data si ora exacta la care certificatul a fost suspendat sau revocat, inclusiv cauzele care au condus la suspendare sau revocare.
- Registrul trebuie sa fie disponibil permanent pentru consultare, inclusiv prin Internet sau alte tehnici de comunicatie la distanta

LEGE privind semnatura electronica
-Furnizarea serviciilor de certificare -

- FSC calificata sunt obligati sa foloseasca numai mecanisme securizate de creare a semnaturii
- FSC calificata trebuie sa dispuna de suficiente resurse financiare pentru acoperirea prejudiciilor pe care le-ar putea cauza cu prilejul desfasurarii activitatilor legate de certificarea semnaturilor electronice
- Asigurarea se realizeaza fie prin subscrierea unei polite de asigurare la o societate de asigurari, fie prin intermediul unei scrisori de garantie din partea unei institutii financiare de specialitate, fie printr-o alta modalitate stabilita printr-o decizie a autoritatii de supraveghere
- Suma asigurata, respectiv suma acoperita prin scrisoarea de garantie vor fi stabilite prin normele metodologice de aplicare ale legii;

LEGE privind semnatura electronica
-Autoritatea de Reglementare si Supraveghere (ARS)-

- Responsabilitatea aplicarii dispozitiilor prezentei legi si ale normelor de aplicare ale acesteia revine ARS
- Pana la infiintarea unei autoritati publice specializate, **ARS este Ministerul Comunicatiilor si Tehnologiei Informatiei**
- MCTI poate delega, in tot sau in parte, atributiile sale ca ARS catre o alta autoritate publica;
- Se infiinteaza la ARS **Registrul Furnizorilor de Servicii de Certificare (RFSC)**, care constituie evidenta oficiala a furnizorilor de servicii de certificare care au domiciliul sau sediul in Romania ;
- Inregistrarea FSC se efectueaza pe baza de cerere individuala, la ARS cu cel putin 30 de zile inainte de data inceperii activitatii;
- RFSC este public si se actualizeaza permanent

LEGE privind semnatura electronica
-Acreditarea voluntara-

- Pentru asigurarea unui securitatii operatiunilor si protejarii drepturilor si intereselor beneficiarilor de servicii de certificare, FSC care doresc pot solicita obtinerea unei **acreditari** din partea unei agentii de acreditare agreate de ARS
- FSC acreditati au dreptul de a folosi o mentiune distinctiva care sa se refere la aceasta calitate in toate activitatile legate de certificarea semnaturilor pe care le desfasoara.
- FSC acreditati sunt obligati sa solicite efectuarea unei mentiuni in acest sens in Registrul Furnizorilor de Servicii de Certificare
- AS vegheaza la respectarea de catre agentiile de acreditare a prevederilor legii, a normelor metodologice, precum si a dispozitiilor cuprinse in decizia de agreare;
- Control exercitat de ARS asupra act. agentiilor de acreditare

LEGE privind semnatura electronica

-Omologarea-

- Conformitatea mecanismelor securizate de creare a semnaturii cu prevederile legii se verifica de catre **agentii de omologare**, persoane juridice de drept public sau de drept privat, agreate de ARS,
- In urma procedurii de verificare se emite certificatul de omologare a mecanismului securizat de creare a semnaturii. Certificatul poate fi retras in cazul in care agentia de omologare constata ca mecanismul securizat de creare a semnaturii nu mai indeplineste una din conditiile prevazute in prezenta lege
- ARS vegheaza la respectarea de catre agentiile de omologare a prevederilor legii, ale normelor metodologice de aplicare, precum si a dispozitiilor cuprinse in decizia de agreare;
- Control exercitat de ARS asupra act. agentiilor de omologare

NORME METODOLOGICE

privind aplicarea
LEGII SEMNATURII ELECTRONICE

-detalii tehnice-

• Generarea cheii private a ARS se face utilizând un sistem izolat, fiabil, proiectat special în acest scop, protejat împotriva utilizării neautorizate
• ARS foloseşte doar funcţia hash-code SHA-1 şi algoritmul de criptare RSA. Este interzisă utilizarea metodei CRT
• Lungimea minimă a cheii private utilizate de un semnatar pentru crearea semnăturii electronice extinse trebuie să fie de minim:
-1024 de biţi pentru algoritmul RSA;
-1024 de biţi pentru algoritmul DSA;
-160 de biţi pentru algoritmul DSA bazat pe curbe eliptice
• Pentru semnături electronice extinse, se pot utiliza următoarele funcţii hash:
- -RIPEMD – 160
-SHA-1
• Registrul electronice de evidenţă a certificatelor eliberate trebuie să corespundă unui format recunoscut internaţional:
-CCITT (ITU-T) X.500 / ISO IS9594
-RFC 2587 Internet X.509 PKI LDAPv2 Schema
-RFC 2587 Internet X.509 PKI Certificate and CRL Profile
-RFC 2589 Lightweight Directory Access Protocol (LDAPv3) Extensions

MCTI: Ordin privind procedura acreditatii FSC (2005)

ACREDITAREA VOLUNTARA A FSC

- FSC care doreşte să îşi desfăşoare activitatea ca FSC acreditat trebuie să solicite obţinerea acreditării din partea ARS.
- Durata acreditării este de 3 ani şi se poate reînnoi.
- FSC trebuie:
  - ✓ să îndeplinească condiţiile necesare emiterii de certificate calificate ,
  - ✓ să utilizeze dispozitive securizate de generare a semnăturii electronice, omologate de o agenţie de omologare agreată de ARS.
- Verificările se fac atât asupra:
  - ✓ declaraţiilor conţinute în documentaţia depusă la ARS,
  - ✓ concordanţei dintre sistemele, procedurile şi practicile afirmate şi cele existente în realitate

MCTI: Ordin privind procedura acreditarii FSC (2005)

ACREDITAREA VOLUNTARA A FSC

- Auditul este realizat de ARS sau de o terţă parte numită de aceasta, conform normelor europene pentru acest gen de activitate.
- ARS trebuie să informeze în termen de maximum 30 de zile FSC cu privire la îndeplinirea condiţiilor şi să solicite, dacă e cazul, completarea documentaţiei.
- În cazul în care se constată că toate criteriile sunt îndeplinite, ARS decide acreditarea FSC
- Decizia de acreditare, condiţiile şi efectele suspendării sau ale retragerii sunt comunicate FSC pe suport de hârtie şi în format electronic, semnat digital de ARS
- ARS actualizează registrul prin înscrierea noului statut de FSC acreditat. Se introduc informaţii despre garanţii, omologarea dispozitivelor, agenţia de omologare, perioada de acreditare.
- ARS trebuie să verifice un FSC cel puţin o dată la 2 ani sau când se modifică procedurile de lucru.

Legea privind arhivarea documentelor în formă electronică nr.135/2007

- Legea stabileşte regimul juridic aplicabil creării, conservării, consultării şi utilizării documentelor în formă electronică arhivate sau care urmează a fi arhivate într-o arhivă electronică, orice persoană fizică sau juridică având dreptul de a depune spre păstrare documente în formă electronică în cadrul unei arhive electronice.
- Totodată, Legea defineşte termeni specifici domeniului de aplicare:

a) *administrator al arhivei electronice*

b) *arhivă electronică* – sistemul electronic de arhivare, împreună cu totalitatea documentelor în formă electronică arhivate

c) *furnizor de servicii de arhivare electronică*

Legea privind arhivarea documentelor în formă electronică nr.135/2007

Furnizarea serviciilor de arhivare a documentelor electronice

- Persoana fizică / juridică are dreptul de a depune spre păstrare documente în formă electronică în cadrul unei arhive electronice.
- Furnizarea serviciilor de arhivare electronică nu este supusă niciunei autorizări prealabile şi se desfăşoară în concordanţă cu principiile concurenţei libere şi loiale, cu respectarea actelor normative în vigoare.
- Cu 30 de zile înainte de începerea activităţilor legate de arhivarea documentelor în formă electronică, persoanele care intenţionează să furnizeze servicii de arhivare electronică au obligaţia de a notifica autoritatea de reglementare şi supraveghere specializată în domeniu cu privire la data începerii acestor activităţi.
- Odată cu efectuarea notificării prevăzute administratorul arhivei electronice are obligaţia de a comunica autorităţii de reglementare şi supraveghere specializate în domeniu toate informaţiile referitoare la procedurile de securitate şi de conservare utilizate, precum şi orice alte informaţii cerute de către autoritatea de reglementare şi supraveghere specializată în domeniu.

Legea privind arhivarea documentelor în formă electronică nr.135/2007

- Administratorul arhivei electronice are obligaţia de a comunica autorităţii de reglementare şi supraveghere specializate în domeniu, cu cel puţin 10 zile înainte, orice intenţie de modificare a procedurilor de securitate şi de conservare, cu precizarea datei şi orei la care modificarea intră în vigoare, precum şi obligaţia de a confirma, în termen de 24 de ore, modificarea efectuată.
- În cazurile de urgenţă în care securitatea serviciilor de arhivare este afectată, administratorul arhivei electronice poate efectua modificări ale procedurilor de securitate şi de conservare, urmând să comunice, în termen de 24 de ore, autorităţii de reglementare şi supraveghere specializate în domeniu, modificările efectuate şi justificarea deciziei luate.
- Administratorul arhivei electronice este obligat să respecte, pe parcursul desfăşurării activităţii, procedurile de securitate şi de conservare declarate

Legea privind arhivarea documentelor în formă electronică nr.135/2007

Crearea arhivei electronice

- Primirea unui document în formă electronică în arhiva electronică este condiţionată de îndeplinirea următoarelor cerinţe:
  a) semnarea documentelor în formă electronică, cu semnătura electronică extinsă a titularului dreptului de dispoziţie asupra documentului, denumită în continuare semnătură electronică;
  b) valabilitatea semnăturii electronice a titularului dreptului de dispoziţie asupra documentului;
  c) depunerea cheii de criptare şi decriptare pentru documentele criptate care cad sub incidenţa Legii Arhivelor Naţionale nr. 16/1996, cu modificările şi completările ulterioare;
- Documentul în formă electronică este semnat electronic de către administratorul arhivei electronice, cu semnătura electronică, în care se atestă şi faptul că documentul respectiv are valoare de original sau copie, conform hotărârii titularului dreptului de dispoziţie asupra documentului. Documentul în formă electronică, astfel identificat, este arhivat în locaţia stabilită de administratorul arhivei electronice.

Legea privind arhivarea documentelor în formă electronică nr.135/2007

- **Administratorul arhivei electronice ataşează, pentru fiecare document în formă electronică arhivat, o fişă în formă electronică, ce va conţine cel puţin următoarele informaţii:**
  - a) proprietarul documentului în formă electronică;
  - b) emitentul documentului în formă electronică;
  - c) titularul dreptului de dispoziţie asupra documentului;
  - d) istoricul documentului în formă electronică;
  - e) tipul documentului în formă electronică;
  - f) nivelul de clasificare a documentului în formă electronică;
  - g) formatul digital în care este arhivat documentul în formă electronică;
  - h) cuvintele-cheie necesare identificării documentului în formă electronică;
  - i) elementele de localizare a suportului fizic;
  - j) identificatorul unic al documentului în formă electronică, în cadrul arhivei electronice;
  - k) data emiterii documentului;
  - l) data arhivării;
  - m) termenul de păstrare a documentului.

Legea privind arhivarea documentelor în formă electronică nr.135/2007

- **În cazul în care documentul în formă electronică a fost generat prin transferarea informaţiei de pe suport analog pe suport digital, fişa va conţine în plus următoarele informaţii:**
  - **a**) referiri la proprietarul originalului şi locaţia în care se găseşte originalul;
  - b) metoda de transfer utilizată;
  - c) dispozitivul hardware utilizat;
  - d) programul de calculator utilizat.
- **Administratorul arhivei electronice este obligat să înregistreze şi să ţină evidenţa tuturor documentelor în formă electronică, intrate în arhiva electronică în cadrul unui registru în formă electronică.**
- **Accesul la registrul arhivei electronice este public numai pentru documentele pentru care titularul dreptului de dispoziţie asupra documentului a stabilit un regim de acces public.**
- **Referinţa, în registrul arhivei, la un document care face parte din categoria documentelor clasificate, poate fi obţinută în funcţie de drepturile de acces ale solicitantului.**

Legea privind arhivarea documentelor în formă electronică nr.135/2007

Conservarea arhivei electronice

- Administratorul arhivei electronice este obligat să păstreze codul-sursă al tuturor programelor utilizate pentru construirea şi exploatarea arhivei electronice, în fişiere semnate electronic.
- Administratorul arhivei electronice este obligat să depună la Arhivele Naţionale o copie a codului-sursă al tuturor programelor utilizate pentru construirea şi exploatarea arhivei electronice.
- În cazul în care administratorul arhivei electronice nu dispune de codul-sursă, prevederile se aplică pt. codul-sursă executabil.
- arhivei electronice are obligaţia să pună la dispoziţie programe informatice, care să permită translatarea oricărui document în formă electronică, arhivat din formatul în care a fost generat într-un format care să permită vizualizarea, reproducerea şi stocarea documentului respectiv la nivelul tehnologiilor în uz.
- În momentul arhivării unui document generat într-un format nerecunoscut de produsele existente în biblioteca de programe informatice, administratorul arhivei electronice are obligaţia ca, odată cu arhivarea documentului, să adauge în bibliotecă descrierea formatului acestuia, precum şi programele informatice cu care documentul a fost generat şi poate fi vizualizat.

Legea privind arhivarea documentelor în formă electronică nr.135/2007

Consultarea arhivei electronice

- Regimul de acces la un document în formă electronică, precum şi modificarea acestuia se stabilesc exclusiv de către titularul dreptului de dispoziţie asupra documentului printr-un act, care va fi semnat atât de titularul dreptului de dispoziţie asupra documentului, cât şi de administratorul arhivei electronice.
- Regimul de acces la documentul în formă electronică, va fi înscris în fişa de format electronic a documentului, iar actul prin care s-a stabilit acest regim, generat electronic sau transferat în format electronic, va constitui o anexă a documentului arhivat.
- Administratorul arhivei electronice este obligat să respecte regimul de acces la document, atât la arhivare, cât şi la acordarea accesului la documentul în formă electronică din arhivă.
- Răspunderea pentru stabilirea regimului de acces la un document în formă electronică revine în exclusivitate titularului dreptului de dispoziţie asupra documentului, iar răspunderea pentru respectarea regimului de acces la documentul în formă electronică, atât la arhivare, cât şi la acordarea accesului la document, revine administratorului arhivei electronice.

Reglementarea marcii temporale

- **Marca temporala** reprezinta o colectie de date in forma electronica, atasata in mod unic unui document electronic; ea certifica faptul ca anumite date in forma electronica au fost prezentate la un moment de timp determinat furnizorului de servicii de marcare temporala.
- Tot mai multe activitati care necesita masuri de securitate complexe precum si cunoasterea exacta a momentului de timp la care acestea au avut loc (e-business, e-banking, e-signature, notar electronic, sisteme de autorizare si certificare, servicii publice electronice etc.). Pentru ca aceste servicii sa poata fi utilizate trebuie sa existe o referinta unica pentru data/timp si sa fie asigurata securitatea comunicatiilor.
- Ministerul Comunicatiilor si Tehnologiei Informatiei a finalizat si pus in functiune in anul **2006** proiectul "**Sistem informatic, disponibil permanent, pentru furnizarea online a orei oficiale a Romaniei".** Realizarea unui sistem de sincronizare via Internet utilizand **protocolul NTP** permite sincronizarea in timp a unui server de timp sau calculator cu informatia de timp furnizata de etalonul national.
- Corpul de **proiecte normative** privind marca temporala cuprinde:
  - Proiectul de **ordin privind desemnarea furnizorului unic de baza de timp**,
  - **Normele Tehnice si Metodologice pentru aplicarea Legii nr.451/2004 privind marca temporala**
  - **Normele de acces la Sistemul Informatic destinat Furnizarii Orei Oficiale a Romaniei.**

Legea Marcii temporale

-Lege nr. 451/2004 privind marca temporala -

Marca temporală este un set de tehnici prin care se permite oricărei persoane să constate dacă un document electronic a fost creat sau semnat la (sau înaintea) unui moment de timp. In practică, cele mai multe sisteme de tipul mărcii temporale folosesc o a treia parte de încredere. Marca temporală este o atestare digitală a acestei părţi de încredere că un anume document electronic exista la un anumit moment de timp.

Acţionând ca o „**ştampilă temporală**", marca este utilizată în legătură cu validitatea certificatului de semnătură electronică, în sisteme de licitaţii desfăşurate pe Internet sau pentru a da o dată certă unor documente electronice necesare în activităţi de e-business, e-commerce sau e-banking.

Regimul juridic. Marca temporală emisă de către un furnizor de servicii de marcare temporală şi semnată cu semnătura electronică extinsă a acestuia, face dovada legală împotriva oricărei terţe părţi a existenţei documentului electronic prezentat la data şi ora menţionate în certificat

Legea Marcii temporale

-Lege nr. 451/2004 privind marca temporala -

Marca temporală este formată din:

- date în formă electronică sau funcţia hash de identificare a acestora;
- data, ora şi minutul specficate, subscrise digital informaţiilor;
- informaţii verificate la furnizorul de servicii şi modalitatea de generare a mărcii temporale:
  - identificatorul emitentului;
  - numărul seriei mărcii temporale;
  - algoritmul de subscriere a mărcii temporale;
- identificatorul certificatului relativ la cheia ce verifică marca;
- identificarea algoritmului hash utilizat pentru generarea amprentei;
- semnătura electronică extinsă.

Data şi ora conţinute în marca temporală sunt specificate în conformitate cu **data si ora Europei Centrale**, eroarea maximum admisă este de 1 minut.

Marca temporală este generată de un **sistem informatic** sigur astfel încât:

- menţine data şi ora în conformitate cu ceea ce este cerut prin prezenta lege;
- generează structura de date conţinând informaţiile specificate;
- subscrie digital structura de date;
- asigură că este imposibil să fie emisă o marcă temporală corectă pentru un timp anterior sau ulterior decât momentul când a fost primit documentul sau să se schimbe ordinea în care mărcile de timp sunt emise.

Legea Marcii temporale

-Lege nr. 451/2004 privind marca temporala -

Obligaţiile furnizorilor de marcă temporală sunt :

- să asigure indicaţii corecte pe marca temporală;
- să menţină înregistrări ale mărcilor temporale emise;
- să păstreze documentaţia astfel încât să se poată verifica mărcile temporale emise;
- să asigure că este posibil să se obţină şi să se verifice mărcile temporale prin Internet . Verificarea trebuie să fie gratuită;
- să asigure realizarea unui audit anual al sistemelor informatice care certifică îndeplinirea condiţiilor prevăzute şi existenţa unei securităţi minime a sistemului şi să trimită rezultatele auditului autorităţii;
- să publice Politica referitoare la protecţia datelor cu caracter personal pe pagina de Internet;
- să publice informaţiile referitoare la mijloacele tehnice şi procedurile ce sunt folosite la emiterea mărcii temporale care să fie disponibile public, inclusiv pe pagina de Internet a furnizorului.

Decizia ANRC nr. 896/2008 privind normele tehnice si metodologice pentru aplicarea Legii privind marca temporala

În înţelesul prezentelor norme tehnice şi metodologice:

- **serviciu de marcare temporala** - serviciul prin care unor date in forma electronica li se asociaza, printr-un mecanism de incredere, o marca temporala;
- **furnizor de servicii de marcare temporala (furnizor**) - orice persoana, fizica sau juridica, care ofera servicii de marcare temporala in conformitate cu prevederile Legii nr. 451/2004;
- **cheie privata** - codul digital, cu caracter de unicitate, generat printr-un dispozitiv hardware si/sau software specializat;
- **cheie publica** - codul digital, pereche a cheii private, necesar verificarii marcii temporale;
- **date de verificare a marcii temporale** - date in forma electronica, cum ar fi coduri sau chei publice, utilizate in scopul verificarii unei marci temporale;
- **dispozitiv criptografic securizat** - un dispozitiv hardware cu un inalt grad de fiabilitate, protejat impotriva modificarilor si a utilizarii neautorizate, care asigura un grad inalt de securitate a operatiilor criptografice in conformitate cu Legea semnaturii electronice;
- **politica de marcare temporala** - regulile si principiile generale aplicate de furnizor in procesul de emitere si administrare a marcilor temporale;
- **functie hash-code** - algoritmul care creeaza o amprenta unica a unui document;
- **extensie de tip critic pentru marcare temporala** - extensia unui certificat digital care trebuie procesata obligatoriu, limitand folosirea cheii private asociate certificatului exclusiv la aplicarea semnaturii digitale din cadrul unei marci temporale.

Decizia ANRC nr. 896/2008 privind normele tehnice si metodologice pentru aplicarea Legii privind marca temporala

Autoritatea de reglementare si supraveghere

- ANC exercita atributiile de reglementare si supraveghere in domeniul marcarii temporale.
- In Registrul furnizorilor de servicii de certificare, ANC va crea o sectiune distincta pentru inregistrarea furnizorilor de servicii de marcare temporala.
- ANC gestioneaza Registrul furnizorilor de servicii de marcare temporala
- ANC va face publice, spre consultare, urmatoarele date din registru:
  a) tipul furnizorului - persoana fizica sau juridica;
  b) numele si prenumele sau denumirea furnizorului, dupa caz;
  c) forma de organizare a furnizorului persoana juridica;
  d) domiciliul sau sediul ;
  e) cetatenia, pentru persoana fizica, sau nationalitatea, pentru persoana juridica;
  f) data la care si-a inceput activitatea de furnizare de servicii de marcare temporala;
  g) cheia publica a furnizorului;
  h) descrierea politicii de marcare temporala a furnizorului;
  i) situatia activitatii furnizorului - operationala, suspendata, incetata, in curs de transferare, in curs de remediere a unor probleme identificate de ANC, cu indicarea termenului-limita;
  j) istoricul furnizorului - data de incepere a activitatii, perioade de suspendare.

Decizia ANRC nr. 896/2008 privind normele tehnice si metodologice pentru aplicarea Legii privind marca temporala

Furnizorii de servicii de marcare temporala

- Cu 30 de zile inainte de inceperea activitatii, furnizorul de servicii de marcare temporala va notifica ANC.
- Furnizorii au obligatia de a comunica ANC, cu cel putin 30 de zile in avans, orice intentie de modificare a procedurilor de securitate a sistemului informatic utilizat
- Furnizorii de servicii de marcare temporala sunt obligati sa respecte, pe parcursul desfasurarii activitatii, procedurile de securitate si de certificare declarate Acestia vor furniza servicii de marcare temporala in conformitate cu politica de marcare temporala declarata.
- Furnizorul este obligat sa genereze sau sa achizitioneze o pereche functionala cheie privata-cheie publica si sa isi protejeze cheia privata prin utilizarea unui dispozitiv criptografic securizat, luand masurile necesare pentru a preveni pierderea, dezvaluirea, modificarea sau utilizarea neautorizata a cheii sale private.
- Perechea va fi folosita exclusiv pentru semnaturi electronice asupra marcilor temporale.
- Cheia privata nu poate fi dedusa in niciun fel din cheia sa publica pereche.
- Furnizorul de servicii de marcare temporala trebuie sa detina certificatul corespunzator cheii publice, pe baza caruia se va putea verifica semnatura asupra marcii temporale.
- Certificatul utilizat pentru marcarea temporala va fi transmis ANC, in forma electronica, la data notificarii inceperii activitatii.

Decizia ANRC nr. 896/2008 privind normele tehnice si metodologice pentru aplicarea Legii privind marca temporala

Furnizorii de servicii de marcare temporala

- Furnizorii de servicii de marcare temporala au obligatia de a crea si mentine un registru electronic operativ de evidenta a marcilor temporale, care sa contina:
  a) toate marcile temporale emise;
  b) inregistrari ale evenimentelor aparute in sistemul informatic utilizat pentru generarea marcilor temporale.
- Furnizorii de servicii de marcare temporala trebuie sa aduca la cunostinta tuturor utilizatorilor termenii si conditiile care privesc utilizarea serviciilor de marcare temporala:
  a) datele de contact ale furnizorului;
  b) politica de marcare temporala aplicata;
  c) standardele tehnice aplicabile;
  d) precizia timpului din marcile temporale;
  e) orice limitari in folosirea serviciului de marcare temporala;
  f) obligatiile utilizatorului;
  g) informatii despre cum trebuie verificata marca temporala;
  h) descrierea practicilor, procedurilor si sistemelor (codul de practici si proceduri);
  i) politica privind protectia datelor cu caracter personal;
  j) perioada de timp in care sunt pastrate inregistrarile referitoare la evenimente ale furnizorului;
  k) disponibilitatea serviciilor.

Prof.Dr.Victor-Valeriu PATRICIU

Decizia ANRC nr. 896/2008 privind normele tehnice si metodologice pentru aplicarea Legii privind marca temporala

Furnizorii de servicii de marcare temporala

- Furnizorul de servicii de marcare temporala trebuie sa indeplineasca urmatoarele conditii:
  a) sa dispuna de mijloace financiare si de resurse materiale, tehnice si umane corespunzatoare pentru garantarea securitatii, fiabilitatii si continuitatii serviciilor oferite;
  b) sa dovedeasca ANC ca dispune de resursele financiare pentru acoperirea prejudiciilor pe care le-ar putea cauza cu prilejul desfasurarii activitati de marcare temporala si ca este capabil sa acopere pierderile suferite de catre o persoana care isi intemeiaza conduita pe efectele juridice ale marcilor temporale, in conditiile prevazute la art. 10 din Legea nr. 451/2004, pana la concurenta echivalentului in lei al sumei de 10.000 euro pentru fiecare risc asigurat. Riscul asigurat este fiecare prejudiciu produs, chiar daca se produc mai multe asemenea prejudicii ca urmare a neindeplinirii de catre furnizor a unei obligatii prevazute de lege. Furnizorul va trebui sa depuna la ANC o scrisoare de garantie din partea unei institutii financiare de specialitate sau o polita de asigurare la o societate de asigurari, in favoarea ANC, in valoare cel putin egala cu echivalentul in lei al sumei de 300.000 euro;
  c) sa foloseasca personal avand cunostinte de specialitate, experienta si calificare necesare pentru furnizarea serviciilor respective;
  d) sa utilizeze numai dispozitive criptografice securizate pentru efectuarea operatiilor criptografice implicate in procesul generarii marcii temporale;
  e) sa utilizeze un sistem informatic care sa respecte cerintele de securitate prevazute la art. 4 alin. (1) din Legea nr. 451/2004;

Decizia ANRC nr. 896/2008 privind normele tehnice si metodologice pentru aplicarea Legii privind marca temporala

Mecanismul marcarii temporale a documentelor

- Marcarea temporala este realizata cu respectarea urmatoarelor etape:
  a) utilizatorul transmite furnizorului o cerere de emitere a marcii temporale pentru un anumit document electronic. Cererea va contine amprenta digitala a documentului pentru care se face cererea, amprenta creata prin intermediul aplicarii unei functii hash-code asupra documentului;
  b) intr-un interval de timp stabilit prin politica de marcare temporala, furnizorul de servicii de marcare temporala executa urmatoarele operatiuni asupra amprentei digitale :
    1. aplica informatia de timp, raportandu-se la baza de timp;
    2. aplica celelalte date prevazute de Legea nr. 451/2004 si orice alte date prevazute in politica sa de marcare temporala care nu contravin prevederilor legale si standardelor recunoscute in materie;
    3. o semneaza electronic utilizand un certificat digital calificat;
  c) in urma acestor operatiuni rezulta marca temporala care este transmisa utilizatorului.
- Autenticitatea marcii temporale poate fi verificata de catre terti pe baza documentului original, a marcii temporale, a cheii publice a furnizorului de servicii de marcare temporala si a functiei hash-code utilizate pentru crearea amprentei digitale a documentului.

Decizia ANRC nr. 896/2008 privind normele tehnice si metodologice pentru aplicarea Legii privind marca temporala

Mecanismul marcarii temporale a documentelor

- Furnizorul de servicii de marcare temporala trebuie sa utilizeze informatia de timp furnizata de furnizorul unic de baza de timp.
- Furnizorul unic de baza de timp este Sistemul informatic pentru furnizarea orei oficiale a Romaniei, realizat de Ministerul Comunicatiilor si Tehnologiei Informatiei.
- Sursa de timp folosita de catre furnizorul de servicii de marcare temporala trebuie sa fie sincronizata cu referinta de timp oferita de furnizorul unic de baza de timp, abaterea maxim admisa fiind de +/- 1 secunda.
- Furnizorul de servicii de marcare temporala este obligat sa puna la dispozitia utilizatorilor software-ul necesar pentru utilizarea serviciului. Software-ul pus la dispozitie de catre furnizorul de servicii de marcare temporala trebuie sa permita utilizatorului sa verifice daca marcarea temporala a fost realizata in mod corect, prin analiza automata a cel putin urmatoarelor elemente:
  a) structura marcii temporale;
  b) amprenta din marca temporala;
  c) semnatura electronica a marcii temporale, respectiv validitatea certificatului folosit pentru semnare.

Legea Notarului electronic

-Legea nr. 589/2004 privind regimul juridic al activitatii electronice notariale -

Legea oferă **documentului notarial posibilitatea de a fi stocat, accesat şi replicat** foarte uşor; documentul electronic va fi securizat în condiţii incomparabil mai bune decât documentul pe hârtie. Actele pe care notarul public le instrumentează în formă electronică trebuie să îndeplinească, sub sancţiunea nulităţii, următoarele condiţii:

- să fie prezentate notarului public în **formă electronică**
- să fie semnate cu **semnătura electronică extinsă**
- să **îndeplinească condiţiile de fond** prevăzute de lege pentru operaţiunea juridică pe care o consemnează

Cererile pentru îndeplinirea unui act notarial electronic vor fi înaintate notarului public în formă electronică si semnate cu semnătura electronică extinsă a solicitantului. În cazul în care cererea este făcută de o altă persoană decât părtile actului, se va anexa actul în baza căruia părtile sunt reprezentate, în formă electronică si semnat cu semnătura electronică extinsă a părţilor

Cererile pentru autentificarea electronică a unui document electronic, odată cu dovada de achitare a taxelor de timbru si a onorariului, părtile vor prezenta notarului public o declaratie în formă electronică si semnată cu semnătura electronică extinsă a fiecăreia, prin care vor mentiona că sunt de acord cu continutul actului si consimt la autentificarea electronică a actului

Legea Notarului electronic

-Legea nr. 589/2004 privind regimul juridic al activitatii electronice notariale -

Încheierea notarialã electronicã prin care se constatã îndeplinirea unui act notarial electronic va cuprinde urmãtoarele elemente:

- adresa electronicã a notarului public
- denumirea încheierii si numãrul acesteia
- data si ora îndeplinirii actului notarial electronic
- numele si prenumele notarului public
- locul unde s-a îndeplinit actul notarial electronic
- semnãtura electronicã extinsã a pãrtilor
- semnãtura electronicã extinsã a solicitantului, în cazul în care acesta este o altã persoanã decât partea.
- semnãtura electronicã extinsã a notarului public
- semnãtura electronicã extinsã a biroului notarial
- numãrul si data eliberãrii autorizaţiei de îndeplinire a actelor notariale electronice, precum şi data expirãrii autorizaţiei.

Notarul public este obligat sã **pãstreze timp de 10 ani în arhiva electronicã actele notariale electronice** pe care le instrumenteazã. Notarul public va ţine la zi un registru în formã electronicã al tuturor actelor notariale electronice pe care le efectueazã, în ordine cronologicã

Legea Notarului electronic

-Legea nr. 589/2004 privind regimul juridic al activitatii electronice notariale -

In vederea emiterii autorizatiei, **notarii publici trebuie sa indeplineasca urmatoarele conditii**:

a) sa dispuna de mijloace financiare si resurse materiale, tehnice si umane corespunzatoare pentru garantarea securitatii, fiabilitatii si continuitatii serviciilor notariale in forma electronica;

b) sa utilizeze un sistem informatic omologat, in conformitate cu normele emise de autoritatea de reglementare si supraveghere specializata in domeniu;

c) sa asigure operarea rapida si sigura a inregistrarii actelor notariale in forma electronica, cu respectarea structurii registrelor notariale stabilite prin regulamentul aprobat de Ministerul Justitiei;

d) sa asigure posibilitatea de a se determina cu precizie data si ora exacta a intocmirii actului notarial;

e) sa dispuna de mijloace corespunzatoare, conform dispozitiilor legale si procedurilor descrise in reglementarile emise de autoritatea de reglementare si supraveghere specializata in domeniu, pentru verificarea identitatii solicitantului si valabilitatea semnaturii electronice extinse a acestuia;

f) sa foloseasca personal cu cunostinte de specialitate in domeniul tehnologiei semnaturii electronice si o practica suficienta in ceea ce priveste procedurile de securitate corespunzatoare;

Legea Notarului electronic

-Legea nr. 589/2004 privind regimul juridic al activitatii electronice notariale -

g) sa aplice procedurile administrative si de gestiune adecvate si care corespund standardelor recunoscute;
h) sa adopte masuri de securitate impotriva falsificarii actelor notariale in forma electronica si sa garanteze confidentialitatea in cursul procesului de generare si arhivare a acestora;
i) sa pastreze toate informatiile cu privire la un act notarial in forma electronica pe perioada stabilita in conformitate cu normele tehnice privind activitatea de pastrare a documentelor create si primite de birourile notarilor publici, Camerele notarilor publici si Uniunea Nationala a Notarilor Publici din Romania, conform normelor emise de autoritatea de reglementare si supraveghere specializata in domeniu;
j) sa utilizeze sisteme omologate pentru arhivarea actelor notariale in forma electronica;
k) orice alte conditii stabilite de autoritatea de reglementare si supraveghere specializata in domeniu.

Ordinul MCTI nr. 221 / 16 iunie 2005

Norme tehnice si metodologice pentru aplicarea Legii nr. 589/2004 privind regimul juridic al activitãtii electronice notariale

- În cadrul activitãtii electronice notariale se utilizează **certificate calificate**, eliberate de furnizori de servicii de certificare care functionează în baza legii privind semnãtura electronicã, **acreditati de cãtre autoritate**, precum si **servicii de marcare temporalã** furnizate conform privind marca temporalã.
- Certificatul calificat utilizat de notarul public în activitatea electronicã notarialã va contine **mentiunea cã acesta a fost eliberat în scopul prestării activitãtii notariale**.
- Certificatul calificat emis notarului public va contine **informatiile privind biroul notarial**, care se referã la:
  - -denumirea biroului notarial în cadrul cãruia notarul public îsi desfãsoarã activitatea;
  - -sediul biroului,

  asa cum sunt ele precizate în certificatul eliberat de Curtea de Apel în circumscriptia cãreia notarul public îsi desfãsoarã activitatea.
- **Autorizatia privind activitatea electronicã notarialã** se emite pentru o perioadã de 3 ani, cu revizuirea anualã a conditiilor tehnice
- **Verificãrile** se fac de cãtre:
  a) auditori certificati de sisteme informatice, iar rezultatul verificãrilor este prezentat autoritãtii sub forma de opinie de audit;
  b) agentii de omologare agreate de cãtre autoritate

Ordinul MCTI nr. 221 / 16 iunie 2005

Norme tehnice si metodologice pentru aplicarea Legii nr. 589/2004 privind regimul juridic al activitãtii electronice notariale

- Pentru desfãsurarea activitãtii electronice notariale **sistemul informatic utilizat trebuie sã îndeplineascã cerintele** privind:
  a) asigurarea securitãtii fizice;
  b) protectia antivirus;
  c) asigurarea unui mecanism de autentificare a utilizatorilor;
  d) asigurarea confidentialitãtii si integritãtii comunicatiilor, a datelor receptionate, transmise si stocate,
  e) mentinerea unei arhive electronice locale;
  f) mentinerea unui registru automatizat de audit care cuprinde evenimentele legate de utilizarea si administrarea sistemului informatic; aceste informatii vor fi pãstrate pentru o perioada de cel putin 10 ani si în arhiva de sigurantã;
  g) accesul (eventual pe baze contractuale) la servicii calificate de arhivare electronicã de sigurantã, unde va fi pãstratã o copie a fiecãrui act electronic notarial efectuat, o copie a registrului electronic al notarului prevãzut la art. 25 alin (1) din legea 589/2004 privind regimul juridic al activitãtii electronice notariale, precum si o copie a registrului de audit mentionat la pct. f).
- **Serviciile calificate de arhivare electronicã** utilizate de notarii publici trebuie sã respecte legislatia referitoare la arhivarea documentelor notariale si accesul la acestea precum si standardele în domeniul managementului securitãtii informatiei si al managementului înregistrãrilor electronice.

Ordinul MCTI nr. 221 / 16 iunie 2005

Norme tehnice si metodologice pentru aplicarea Legii nr. 589/2004 privind regimul juridic al activitãtii electronice notariale

- Pentru pãstrarea sub **forma criptatã a documentelor în arhive**, notarul public va depune cheia si aplicatia de decriptare la Uniunea Nationalã a Notarilor Publici din România. Cheia si aplicatia de decriptare vor fi pãstrate pe toatã durata legalã de pãstrare a arhivelor. Cheia de decriptare se pãstreazã în conditii de securitate corespunzãtoare si sub control dual al accesului.
- **Standardele de referintã** în evaluarea sistemelor de management al securitãtii informatiei si în omologarea sistemelor informatice sunt **ISO 17799/2000** respectiv **ISO/IEC 15408/1999** (pãrtile 1, 2 si 3).
- Pentru **verificarea semnatarilor care solicitã încheierea actelor notariale în formã electronicã**, notarul public trebuie sã verifice cel putin urmãtoarele:
  a) semnãtura electronicã extinsã a solicitantului se bazeazã pe un certificat calificat valabil, nerevocat si nesuspendat de cãtre furnizorul de servicii de certificare care l-a eliberat;
  b) certificatul semnatarului nu a fost eliberat pe baza unui pseudonim;
  c) data si ora semnãrii documentului de cãtre solicitant sunt afisate corect si sunt credibile.
- Încheierea actelor notariale în formã electronicã va fi precedatã de un **avertisment al sistemului informatic asupra operatiunii ce urmeazã a fi efectuatã si se va realiza printr-un mecanism care presupune confirmarea expresã a notarului public**.