

PKI applications (C2)

Basics and legal aspects

Pascal Steichen (MSSI-uni.lu) - 07/12/2007

- [Where it all started](#)
- [1. PKI basics](#)
 - [1.1. Data encryption using PKI](#)
 - [1.1.1. Example: SSL/TLS](#)
 - [1.2. Digital signature using PKI](#)
 - [1.3. Key management in PKI](#)
 - [1.4. CA and certificates](#)
 - [1.4.1. Example certificate](#)
- [2. Trust models \(or PKI vs PGP\)](#)
 - [2.1. PKI trust models \(architectures\)](#)
- [3. Ten risks of PKI](#)
- [4. Legal aspects](#)
 - [4.1. Electronic signature directive \(1999/93/EC\)](#)
 - [4.2. LU legal framework](#)
 - [4.3. CSP supervision/accreditation legal framework](#)
 - [4.4. CSP accreditation scheme](#)
 - [4.5. CSP supervision scheme](#)
- [5. Bibliographic references](#)

Where it all started

For most of the history of cryptography, a key had to be kept absolutely secret and would be agreed upon beforehand using a secure, but non-cryptographic, method; for example, a face-to-face meeting or a trusted courier. There are a number of significant practical difficulties in this approach to distributing keys. Public-key cryptography was invented to address these drawbacks — with public-key cryptography, users can communicate securely over an insecure channel without having to agree upon a shared key beforehand.

In 1874, a book by William Stanley Jevons described the relationship of one-way functions to cryptography and went on to discuss specifically the factorization problem used to create the trapdoor function in the RSA system. In July 1996, one observer commented on the Jevons book in this way:

In his book *The Principles of Science: A Treatise on Logic and Scientific Method*, written and published in the 1890s, William S. Jevons observed that there are many situations where the 'direct' operation is relatively easy, but the 'inverse' operation is significantly more difficult. One example mentioned briefly is that enciphering (encryption) is easy while deciphering (decryption) is not. In the same section of Chapter 7: Introduction titled 'Induction an Inverse Operation', much more attention is devoted to the principle that multiplication of integers is easy, but finding the (prime) factors of the product is much harder. Thus, Jevons anticipated a key feature of the RSA Algorithm for public key cryptography, though he certainly did not invent the concept of public key cryptography.

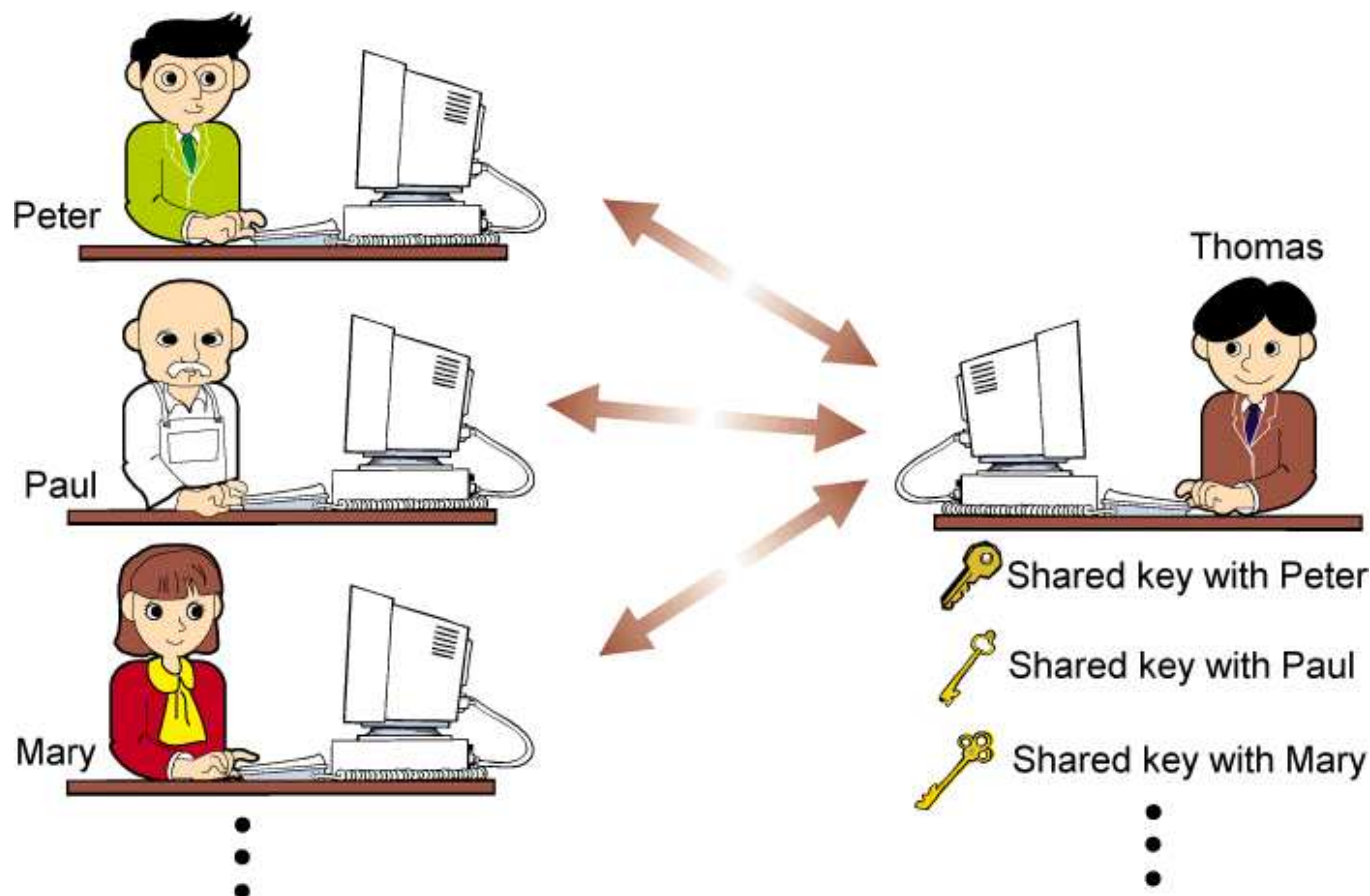
The first invention of asymmetric key algorithms was by James H. Ellis, Clifford Cocks, and Malcolm Williamson at GCHQ in the UK in the early 1970s; these inventions were what later become known as Diffie-Hellman key exchange, and a special case of RSA. The GCHQ cryptographers referred to the technique as "non-secret encryption". These inventions were not publicly disclosed at the time, and the fact that they had been developed was kept secret until 1997.

An asymmetric-key cryptosystem was published in 1976 by Whitfield Diffie and Martin Hellman, who, influenced by Ralph Merkle's work on public-key distribution, disclosed a method of public-key agreement. This method of exponential-key exchange, which came to be known as Diffie-Hellman key exchange, was the first published practical method for establishing a shared secret-key over an unprotected communications channel without using a prior shared secret. Merkle's public-key-agreement technique became known as Merkle's Puzzles, and was published in 1978.

A generalisation of the Cocks method was reinvented in 1977 by Rivest, Shamir and Adleman, all then at MIT. The latter authors published their work in 1978, and the algorithm appropriately came to be known as RSA. RSA uses exponentiation modulo a product of two large primes to encrypt and decrypt, performing both public key encryption and public key digital signature, and its security is connected to the presumed difficulty of factoring large integers, a problem for which there is no known efficient (i.e., practicably fast) general technique.

Since the 1970s, a large number and variety of encryption, digital signature, key agreement, and other techniques have been developed in the field of public-key cryptography. The ElGamal cryptosystem (invented by Taher ElGamal then of Netscape) relies on the (similar, and related) difficulty of the discrete logarithm problem, as does the closely related DSA developed by the NSA and NIST. The introduction of elliptic curve cryptography by Neal Koblitz in the mid 1980s has yielded a new family of analogous public-key algorithms. Although mathematically more complex, elliptic curves appear to provide a more efficient way to leverage the discrete logarithm problem, particularly with respect to key size.

The problem with symmetric key crypto-systems:



© 1999 Department of Computer Science and Information Systems, The University of Hong Kong

1. PKI basics

Recap of the fundamentals and basic concepts:

Public key cryptography, also known as asymmetric cryptography, is a form of cryptography in which a user has a pair of cryptographic keys - a public key and a private key. The private key is kept secret, while the public key may be widely distributed. The keys are related mathematically, but the private key cannot be practically derived from the public key. A message encrypted with the public key can be decrypted only with the corresponding private key.

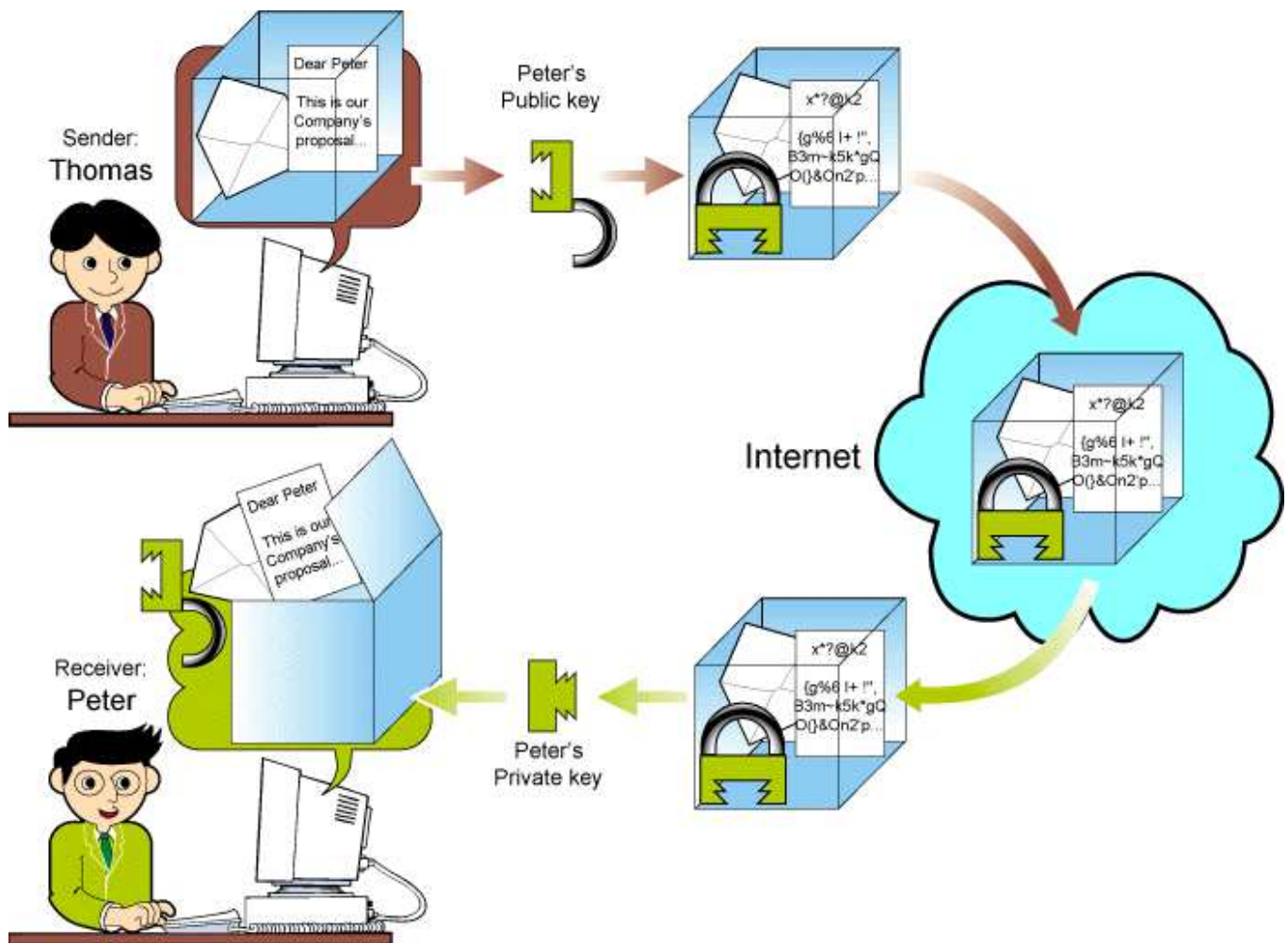
- asymmetric (public key) cryptography
 - key pair (private key & public key)
 - The two main branches of public key cryptography are:
 - public key encryption — a message encrypted with a user's public key cannot be decrypted by anyone except the user possessing the corresponding private key. This is used to ensure confidentiality and integrity.
 - digital signatures — a message signed with a user's private key can be verified by anyone who has access to the user's public key, thereby proving that the user signed it and that the message has not been tampered with. This is used to ensure authenticity (non-repudiation) and integrity.
- main usage branches
 - encryption
 - confidentiality
 - integrity
 - signing
 - non-repudiation
 - integrity
 - authentication

A central problem for public-key cryptography is proving that a public key is authentic, and has not been tampered with or replaced by a malicious third party. The usual approach to this problem is to use a public-key infrastructure (PKI), in which one or more third parties, known as certificate authorities, certify ownership of key pairs by issuing certificates for the public keys.

- key management (PKI)
 - CA (trusted third party)
 - certificates

1.1. Data encryption using PKI

Public-key encryption uses a combination of a private key and a public key. The private key is known only to your computer, while the public key is given by your computer to any computer that wants to communicate securely with it. To decode an encrypted message, a computer must use the public key, provided by the originating computer, and its own private key.



© 1999 Department of Computer Science and Information Systems, The University of Hong Kong

1.1.1. Example: SSL/TLS

A popular implementation of public-key encryption is the Secure Sockets Layer (SSL). Originally developed by Netscape, SSL is an Internet security protocol used by Internet browsers and Web servers to transmit sensitive information. SSL has become part of an overall security protocol (from the IETF) known as Transport Layer Security (TLS).

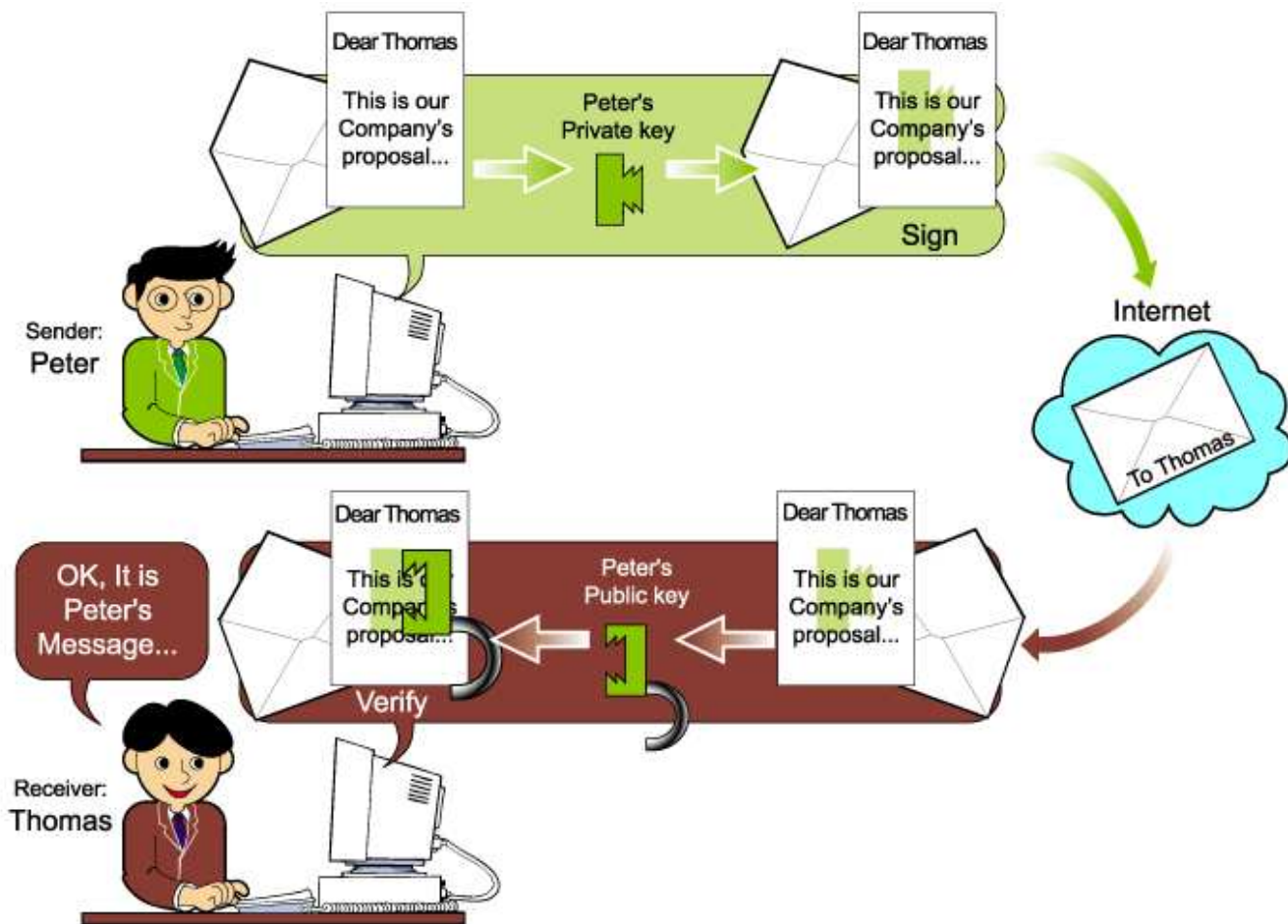


Look for the "s" after "http" in the address whenever you are about to enter sensitive information, such as a credit-card number, into a form on a Web site. In your browser, you can tell when you are using a secure protocol, such as TLS, in a couple of different ways. You will notice that the "http" in the address line is replaced with "https," and you should see a small padlock in the status bar of the browser window. The padlock symbol lets you know that you are using encryption.

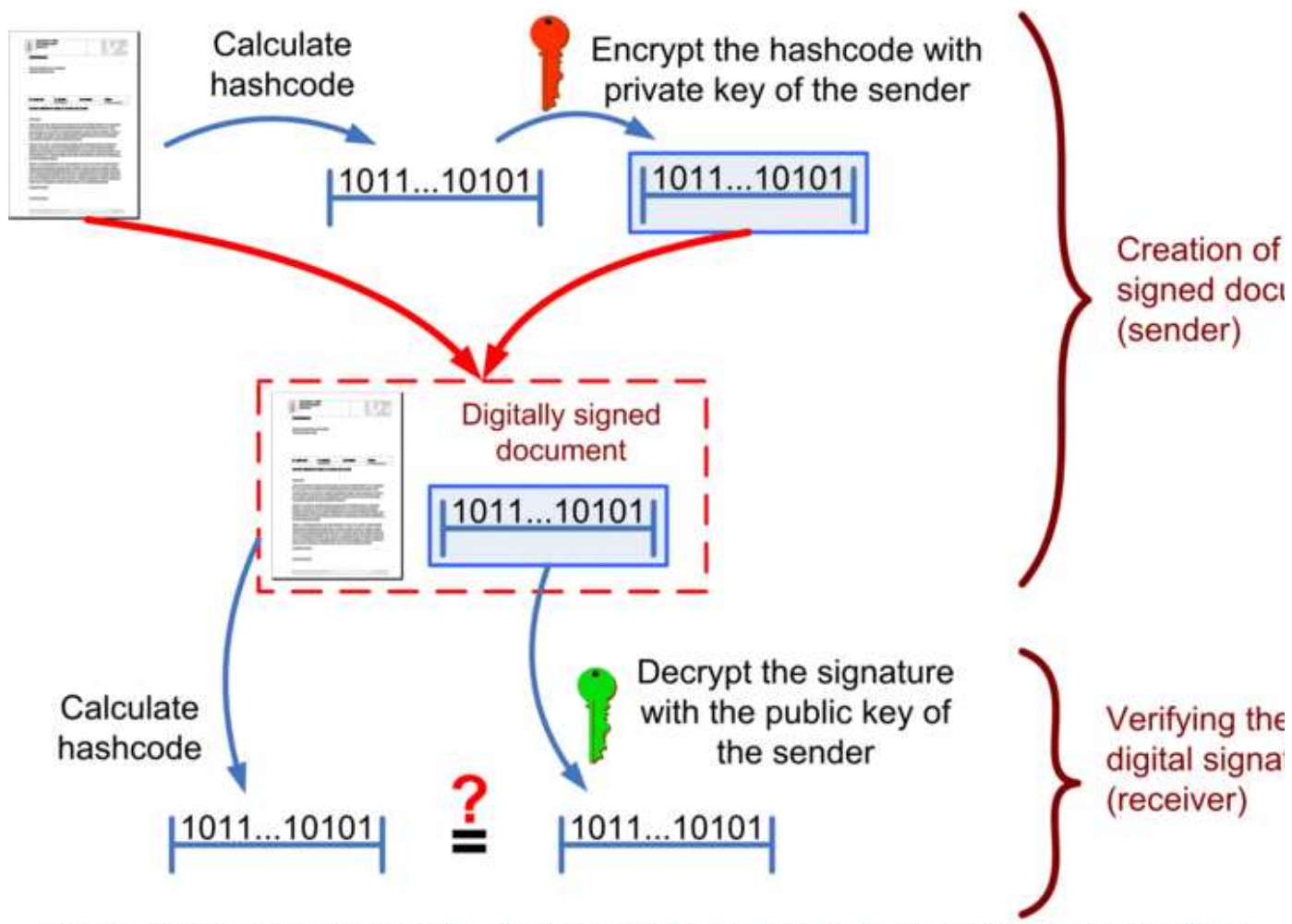
Public-key encryption takes a lot of computing, so most systems use a combination of public-key and symmetry. When two computers initiate a secure session, one computer creates a symmetric key and sends it to the other computer using public-key encryption. The two computers can then communicate using symmetric-key encryption. Once the session is finished, each computer discards the symmetric key used for that session. Any additional sessions require that a new symmetric key be created, and the process is repeated.

- The SSL hybrid crypto-system mechanism:
 1. generation of a symmetric session key
 2. encryption of data with the sessions key
 3. encryption of the session key with the destination's public-key
 4. concatenation of the both encrypted data-blocks
 5. destruction of session key at the end

1.2. Digital signature using PKI



Creating and verifying a digital signature

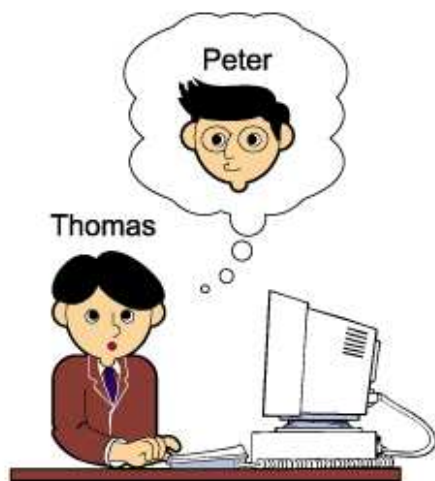


If the calculated hashcode does not match the result of the decrypted signature, either the document was changed after signing, or the signature was not generated with the private key of the alleged sender.

© 2006 Bart Van den Bosch

1.3. Key management in PKI

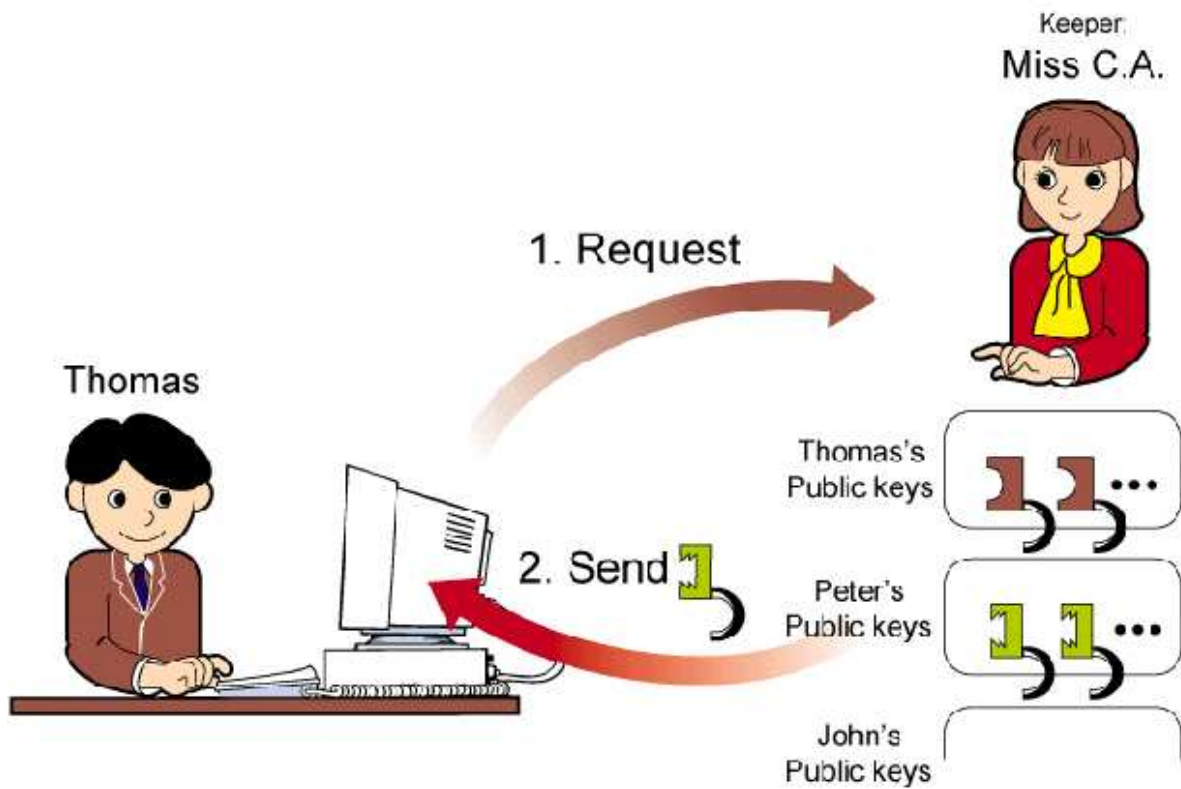
We are going to study the data encryption example in more details. This illustrates the key management issues for Public Key Crypto-Systems. Suppose Thomas wants to send a secret message to Peter.



Thomas wants to communicate with Peter

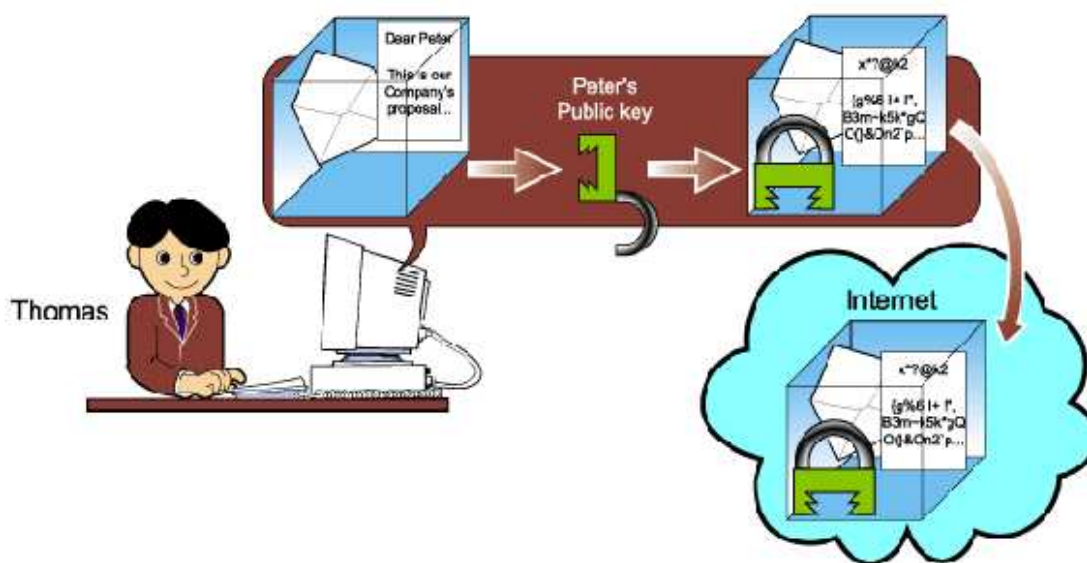
© 1999 Department of Computer Science and Information Systems, The University of Hong Kong

He needs to ask Miss C.A., the public-keys keeper, for Peter's public key. Miss C.A. will give out Peter's public key.



© 1999 Department of Computer Science and Information Systems, The University of Hong Kong

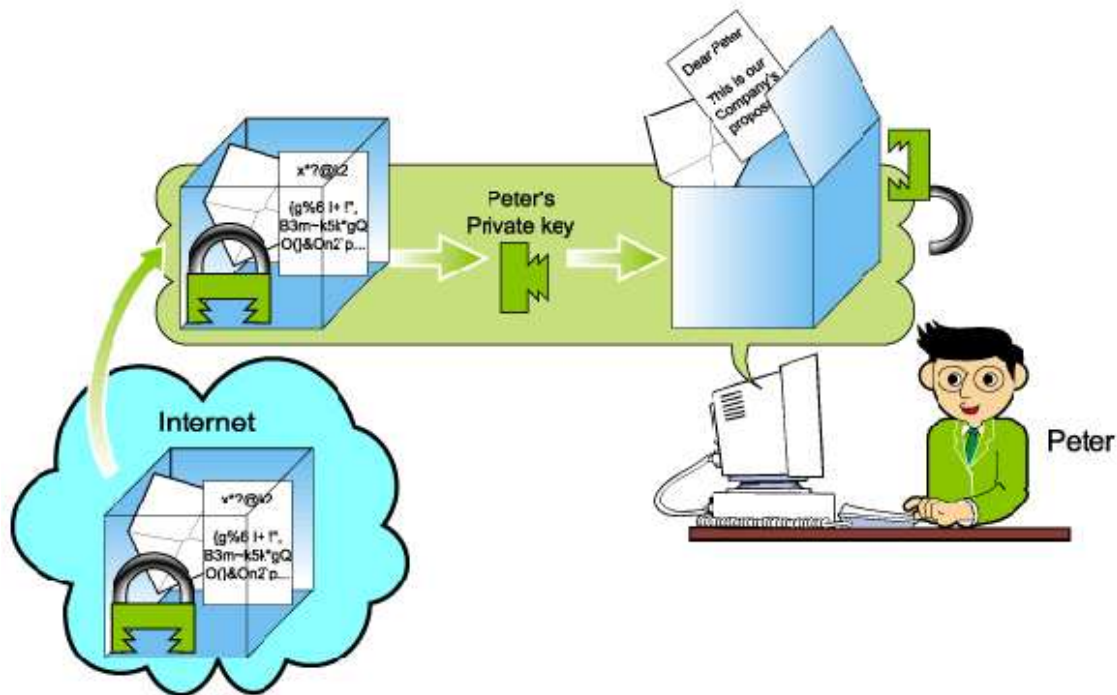
Then Thomas encrypts the message with Peter's public key. Note that this encrypted message can ONLY be decrypted by Peter's private key. Thomas then sends the encrypted message via the Internet.



Thomas encrypts the message and sends it.

© 1999 Department of Computer Science and Information Systems, The University of Hong Kong

After Peter receives the encrypted message from the Internet, he uses his own private key to decrypt it. The same public key can be used by others to send secret messages to Peter.



Peter decrypts the received message with his Private Key.

© 1999 Department of Computer Science and Information Systems, The University of Hong Kong

Note that for the whole system to work, there are two important key management issues:

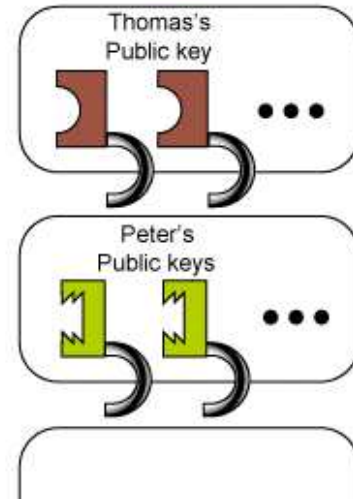
- Each user has to keep his private key really secret.
- Every user's public key has to be correctly known to all other people. Usually this is done by selecting a trustworthy third party to manage the public keys.

1.4. CA and certificates

A public key certificate (or identity certificate) is a certificate which uses a digital signature to bind together a public key with an identity — information such as the name of a person or an organization, their address, and so forth. The certificate can be used to verify that a public key belongs to an individual. In a typical public key infrastructure (PKI) scheme, the signature will be of a certificate authority (CA).



Keeper:
Miss C.A.



© 1999 Department of Computer Science and Information Systems, The University of Hong Kong

A certificate authority or certification authority (CA) is an entity which issues digital certificates for use by other parties. It is an example of a trusted third party. CAs are characteristic of many public key infrastructure (PKI) schemes.

1.4.1. Example certificate


```
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number: 1424 (0x590)
    Signature Algorithm: sha1WithRSAEncryption
    Issuer: C=LU, O=LuxTrust s.a, CN=LuxTrust Normalised CA
    Validity
      Not Before: Mar  2 11:07:48 2007 GMT
      Not After : Mar  2 11:07:48 2012 GMT
    Subject: C=LU, ST=Luxembourg, L=Luxembourg, O=Ministry of the Economy and Foreign Trade, OU=CASE
    CN=*.cases.lu/emailAddress=pst@cases.lu
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      RSA Public Key: (2048 bit)
        Modulus (2048 bit):
          00:da:34:1c:18:83:0e:96:24:54:0a:c9:58:95:85:
          2d:65:26:3f:1d:f6:c7:a0:6f:4c:0a:6e:af:ac:1c:
          0b:b1:4c:e7:ec:d5:4b:73:e6:9c:67:de:87:e5:cd:
          da:9d:e2:e8:1b:fe:13:27:65:6b:ab:66:d3:f3:1a:
          e0:92:00:f6:89:de:8d:f0:e4:d3:1a:15:da:44:f0:
          d8:0e:cb:61:f6:d8:5f:f1:65:ae:c5:f9:63:7b:8f:
          9e:8d:5c:72:d5:60:be:05:04:1e:14:35:c9:87:0f:
          fc:fd:e2:e1:3c:7b:a4:2f:de:f3:e9:b9:42:73:b1:
          52:9d:c8:e8:27:77:af:e3:03:68:44:7c:fd:cc:19:
          3d:13:41:1b:c3:df:2b:2f:63:76:9b:67:b6:ed:69:
          6b:77:0b:e8:03:97:10:a1:5b:e9:4c:7e:b2:7c:aa:
          d2:8b:96:57:da:1a:aa:58:8f:ac:fd:3b:96:57:77:
          2b:94:52:fb:ea:0b:ab:52:d5:51:39:07:26:f5:3f:
          67:43:57:6c:30:6c:e0:4a:af:74:c2:ed:98:27:67:
          36:19:f0:e5:f8:ec:21:43:0f:ec:6e:89:3b:ca:67:
          9c:e8:6f:fa:39:b1:c4:11:b1:44:14:a0:10:96:cb:
          1d:07:ca:cf:fd:28:08:2c:15:41:d1:9e:80:d9:b1:
          72:25
        Exponent: 65537 (0x10001)
    X509v3 extensions:
      X509v3 Basic Constraints: critical
        CA:FALSE
      Authority Information Access:
        OCSP - URI:http://ocsp.luxtrust.lu
        CA Issuers - URI:http://ca.luxtrust.lu/LTNCA.crt
      X509v3 Certificate Policies:
        Policy: 1.3.171.1.1.2.2.1
        User Notice:
          Explicit Text: LuxTrust Server Certificate.Not supported by SSCD, Key Generation by
and CPS on http://repository.luxtrust.lu
          CPS: http://repository.luxtrust.lu
```

==

```

User Notice:
  Explicit Text: LuxTrust Server Certificate.Not supported by SSCD, Key Generation by
and CPS on http://repository.luxtrust.lu
  CPS: http://repository.luxtrust.lu
  Policy: 0.4.0.2042.1.3

Netscape Cert Type:
  SSL Server
X509v3 Key Usage: critical
  Digital Signature, Key Encipherment, Data Encipherment
X509v3 Extended Key Usage:
  TLS Web Server Authentication
X509v3 Authority Key Identifier:
  keyid:CE:FE:46:9D:63:2F:89:FD:F2:38:16:25:D8:F1:6C:DE:47:F8:CE:C1

X509v3 CRL Distribution Points:
  URI:http://crl.luxtrust.lu/LTNCA.crl

X509v3 Subject Key Identifier:
  66:2B:FD:C1:89:E5:54:1B:87:A8:3C:5B:BC:20:84:33:CE:57:FF:40
Signature Algorithm: sha1WithRSAEncryption
  3a:c3:89:1a:8d:c0:17:35:ac:9c:73:23:33:4f:b4:cc:9d:5f:
  08:38:ed:cb:af:86:64:67:66:61:ff:de:66:55:c6:31:c9:ff:
  eb:75:bd:51:d6:24:af:e6:14:cb:91:92:0b:0b:ec:96:39:8f:
  fc:5d:7a:fe:d4:4d:89:92:5e:f6:45:89:5d:bc:e0:4e:0b:9b:
  1f:e1:4a:41:3d:59:3e:d0:65:08:44:58:bf:f3:eb:78:d4:7d:
  c0:15:cd:8e:7c:9b:b3:af:39:8d:cb:8d:4c:bc:e1:f0:ef:7d:
  52:03:11:af:a5:d0:4d:d0:2a:ff:9d:63:b1:d8:5b:ad:1b:ba:
  9d:c0:14:b5:68:33:d5:6e:40:cb:c8:72:26:ef:f7:95:0a:e2:
  3f:18:01:dd:95:22:02:ea:37:08:eb:13:48:64:40:54:2b:10:
  06:80:cd:31:ef:1f:b6:2c:24:dc:6f:3f:64:07:84:a2:d0:9f:
  2d:97:71:92:f7:19:93:55:92:6f:60:05:88:35:ce:49:e0:ba:
  53:38:31:22:53:48:3f:94:7b:5d:5d:29:75:92:d6:2a:69:7c:
  40:33:35:bb:c4:6e:f4:ba:27:d5:95:46:2d:f2:17:e1:d6:36:
  62:06:fc:e8:51:eb:42:ac:86:65:bf:8d:7d:31:7a:37:96:34:
  4f:82:f3:17
-----BEGIN CERTIFICATE-----
MIIFGjCCBQgqAwIBAgICBZAwDQYJKoZIhvcNAQEFBQAwRTELMAkGA1UEBhMCTFUX
FTATBgNVBAAoTDExleFRydXN0IHMuYTEfMBOGA1UEAxMwTHV4VHJ1c3QgTm9ybWFs
aXNlZCBBDQTAeFw0wNzAzMDIxMTA3NDhaFw0xMjAzMDIxMTA3NDhaMIIG4MQswCQYD
VQQGEwJMTETMBEGA1UECBMKTHV4ZW11b3VyZzETMBEGA1UEBxMKTHV4ZW11b3Vy
ZzEyMDAGA1UEChMPTWluaXN0cnkgb2YgdGh1IEVjb25vbXkgYW5kIEZvcmlvZ2Z2
VHJhZGUXGTAXBgNVBAsTEENBU0VTElExleGVtYm91cmcxEzARBgNVBAMUCiouY2Fz
ZXNubHUXGzAZBgkqhkiG9w0BCQEWDHBzdEBjYXNlcysdTCCASiWdQYJKoZIhvcN
AQEBBQADggEPADCCAQoCggEBANo0HBiDDpYkVArJWJWFLWUmPx32x6BvTApur6wc
C7FM5+zsV3PmnGfeh+XN2p3i6Bv+Eydl6t6m0/Ma4JIA9onejfdk0xoV2kTw2A7L

```

2. Trust models (or PKI vs PGP)

- Web of trust (the PGP model)

The phrase "Public Key Infrastructure" has become synonymous with "Certificate Authority", but what we call a PKI in the OpenPGP world is actually an emergent property of the sum total of all the keys in the user population, all the signatures on all those keys, the individual opinions of each OpenPGP user as to who they choose as trusted introducers, all the OpenPGP client software which runs the OpenPGP trust model and performs trust calculations for each client user, and the key servers which fluidly disseminate this collective knowledge.

This is more often called a web of trust, which uses self-signed certificates and third party attestations of certificates. Examples of implementations of this approach are PGP (Pretty Good Privacy) and GnuPG (The GNU Privacy Guard; a free implementation of OpenPGP, the standardised specification of PGP). Because of PGP's (and clones') extensive use in email, the Web of Trust originally implemented by PGP is the most widely deployed bidirectional PKI existing.

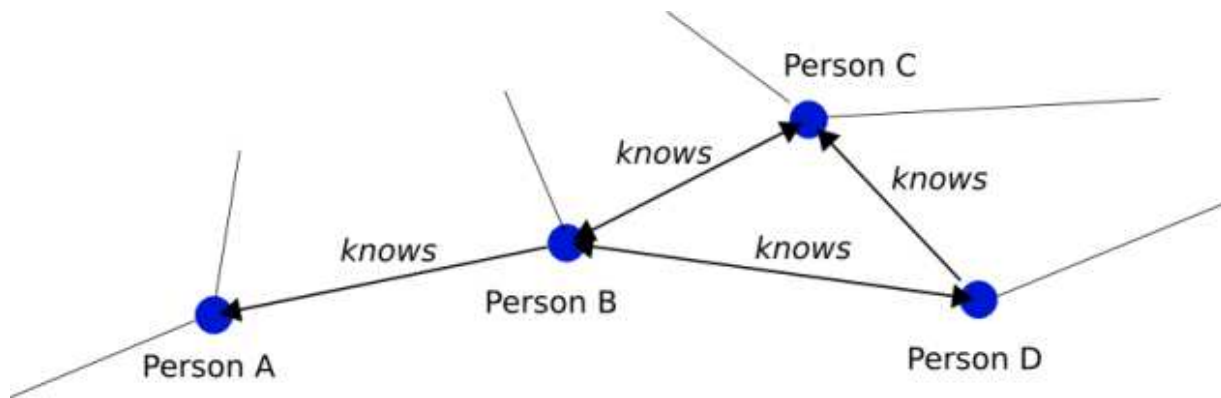
The web of trust concept was put forth by PGP creator Phil Zimmermann in the manual for PGP version 2.0:

As time goes on, you will accumulate keys from other people that you may want to designate as trusted introducers. Everyone else will each choose their own trusted introducers. And everyone will gradually accumulate and distribute with their key a collection of certifying signatures from other people, with the expectation that anyone receiving it will trust at least one or two of the signatures. This will cause the emergence of a decentralized fault-tolerant web of confidence for all public keys.

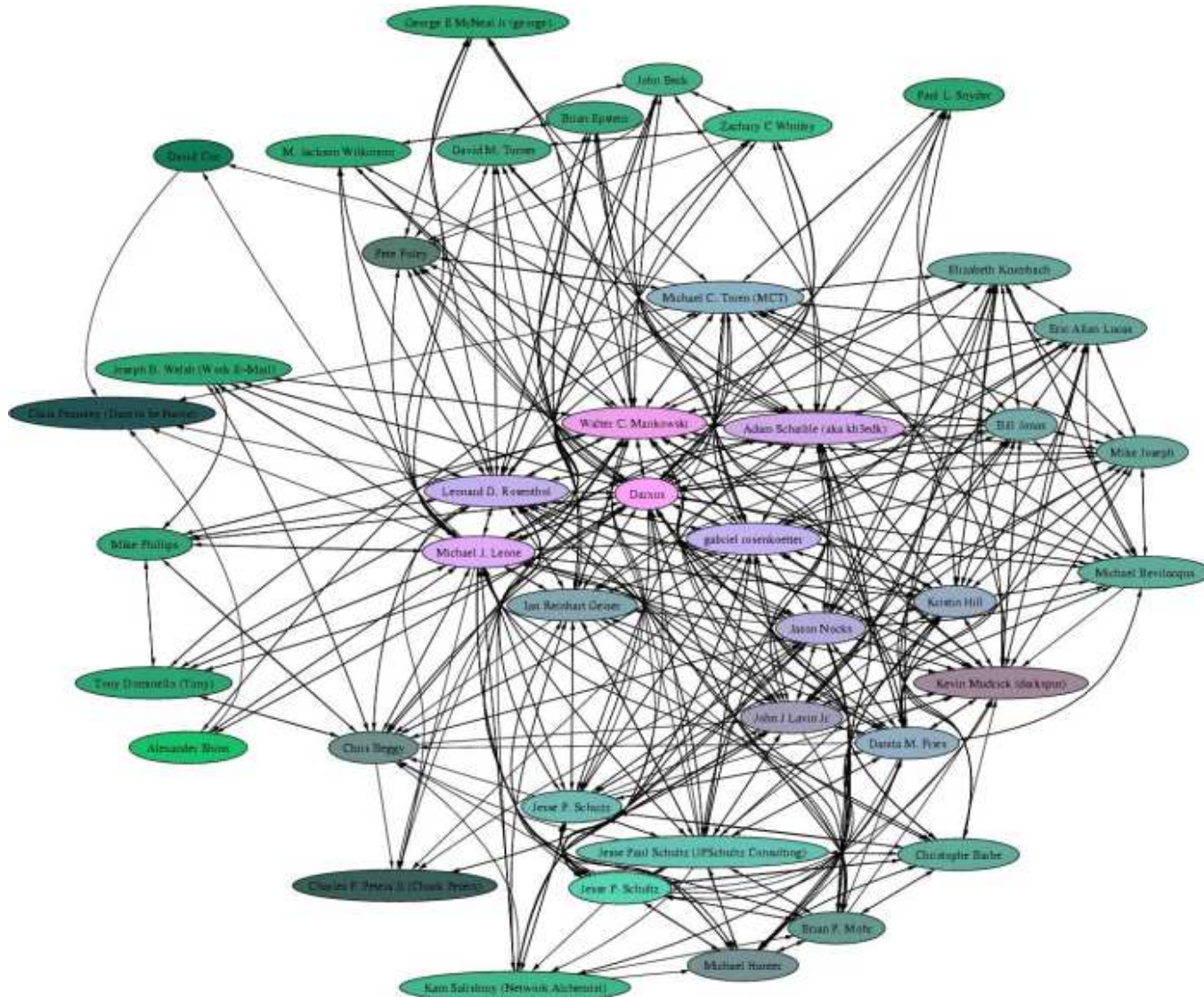
- certificates are signed by other users (during "key signing parties"),
- trust **decisions** are in the hands of the users,
- different levels of trust exist,

(based on the verification process or authentication/identification method used/available)

- flexible (non-hierarchical),



© 2006 World Wide Web Conference Committee (IW3C2)

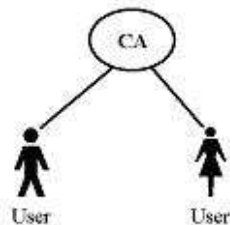


© 2007 The Philadelphia area Linux User Group (PLUG)

- Drawbacks:
 - everyone needs to manage its own trust relations,
 - different levels of trust exist,
 - gets complex relatively fast,
 - limited usability for normal users.

2.1. PKI trust models (architectures)

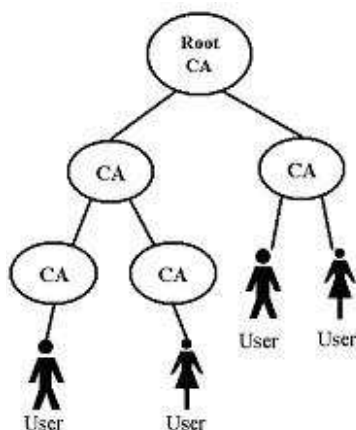
- Basic *flat* architecture:



© 2004 Eliana Stavrou

A single architecture is the most basic PKI model that contains only a single (you wouldn't expect more, would you?) CA. All the users of the PKI place their trust on this CA. The CA will be responsible in handling all the users requesting a certificate. As there is only one CA, every certification path will begin with its public key.

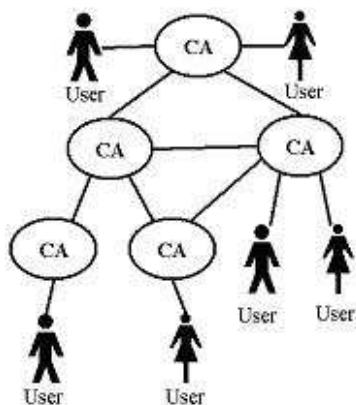
- Hierarchical architecture:



© 2004 Eliana Stavrou

A hierarchical architecture is constructed with subordinate CA relationships. In this configuration, all users trust a single "root" CA. The root CA issues certificates to subordinate CAs only, whereas subordinate CAs may issue certificates to users or other CAs. The trust relationship is specified in only one direction. In this PKI architecture, every certification path begins with the root CA's public key.

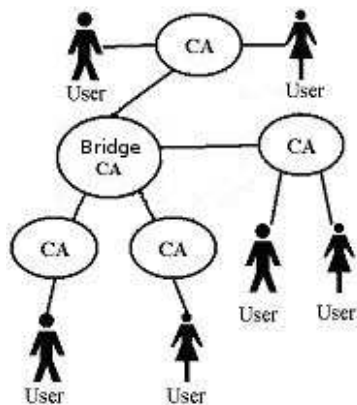
- Mesh architecture:



© 2004 Eliana Stavrou

A mesh architecture does not include only one CA that is trusted by all entities in the PKI system. CAs can be connected with cross certification creating a "web of trust" where end entities may choose to trust any CA in the PKI. If a CA wishes to impose constraints on certain trust relationships, it must specify appropriate limitations in the certificates issued to its peers.

- Bridge architecture



Bridge CA: roughly speaking a CA that cross-certifies other CA's with a similar trust level. To make full use of such a cross-certification you need access to a directory and to the revocation information of the other CA's. While a Bridge CA by itself cares for the trust relationship, the problem of certificate distribution and certificate validation remains unsolved. Thus one also needs a central directory and a central OCSP-Responder to allow for a seamless interoperability - even with a Bridge-CA.

3. Ten risks of PKI

- Risk #1: "Who do we trust, and for what?"
- Risk #2: "Who is using my key?"
- Risk #3: "How secure is the verifying computer?"
- Risk #4: "Which John Robinson is he?"
- Risk #5: "Is the CA an authority?"
- Risk #6: "Is the user part of the security design?"
- Risk #7: "Was it one CA or a CA plus a Registration Authority?"
- Risk #8: "How did the CA identify the certificate holder?"
- Risk #9: "How secure are the certificate practices?"
- Risk #10: "Why are we using the CA process, anyway?"

© 2000 Computer Security Journal • Volume XVI, Number 1, Bruce Schneier

4. Legal aspects

- 1997: COM(97) 503 ensuring security & trust in e-communications
- 1999: Electronic signature directive (1999/93/EC)
- 1999 - 2000: eEurope 2002 Action Plan - smart card & secure access
 1. A cheaper, faster, secure Internet
 - Cheaper and faster Internet access
 - Faster Internet for researchers and students
 - **Secure networks and smart cards**
 2. Investing in people and skills
 - European youth into the digital age
 - Working in the knowledge-based economy
 - Participation for all in the knowledge-based economy
 3. Stimulate the use of the Internet
 - Accelerating e-commerce
 - Government online: electronic access to public services
 - Health online
 - European digital content for global networks
 - Intelligent transport systems
- 2002: eEurope 2005 Action Plan - a task force is proposed
 - modern online public services & dynamic e-business environment
 - **e-government, e-learning and e-health services**
 - and, as an enabler for these
 - widespread availability of broadband access at competitive prices
 - **a secure information infrastructure**

4.1. Electronic signature directive (1999/93/EC)

The electronic signature directive (1999/93/EC) establishes a harmonized *electronic* signature similar to the handwritten signature.

The key definitions from the directive are:

- electronic signature

data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication;

- advanced electronic signature an electronic signature which meets the following requirements:
 1. it is uniquely linked to the signatory;
 2. it is capable of identifying the signatory;
 3. it is created using means that the signatory can maintain under his sole control; and
 4. it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable;
- signatory

a person who holds a signature-creation device and acts either on his own behalf or on behalf of the natural or legal person or entity he represents;

- signature-creation device

configured software or hardware used to implement the signature-creation data;

- signature-creation data

unique data, such as codes or private cryptographic keys, which are used by the signatory to create an electronic signature;

- signature-verification device

configured software or hardware used to implement the signature-verification data;

- signature-verification-data

data, such as codes or public cryptographic keys, which are used for the purpose of verifying an electronic signature.

During the signature-verification process it should be ensured with reasonable certainty that:

1. the data used for verifying the signature correspond to the data displayed to the verifier;
2. the signature is reliably verified and the result of that verification is correctly displayed;
3. the verifier can, as necessary, reliably establish the contents of the signed data;
4. the authenticity and validity of the certificate required at the time of signature verification are reliably verified;
5. the result of verification and the signatory's identity are correctly displayed;
6. the use of a pseudonym is clearly indicated; and
7. any security-relevant changes can be detected;

- secure-signature-creation device

1. Secure signature-creation devices must, by appropriate technical and procedural means, ensure at the least that:
 - the signature-creation-data used for signature generation can practically occur only once, and that their secrecy is reasonably assured;
 - the signature-creation-data used for signature generation cannot, with reasonable assurance, be derived and the signature is protected against forgery using currently available technology;
 - the signature-creation-data used for signature generation can be reliably protected by the legitimate signatory against the use of others.
2. Secure signature-creation devices must not alter the data to be signed or prevent such data from being presented to the signatory prior to the signature process;

- certification-service-provider

an entity or a legal or natural person who issues certificates or provides other services related to electronic signatures;

- electronic-signature product

hardware or software, or relevant components thereof, which are intended to be used by a certification-service-provider for the provision of electronic-signature services or are intended to be used for the creation or verification of electronic signatures;

- voluntary accreditation

any permission, setting out rights and obligations specific to the provision of certification services, to be granted upon request by the certification-service-provider concerned, by the public or private body charged with the elaboration of, and supervision of compliance with, such rights and obligations, where the certification-service-provider is not entitled to exercise the rights stemming from the permission until it has received the decision by the body.

- certificate

an electronic attestation which links signature-verification data to a person and confirms the identity of that person;

- qualified certificate

- a certificate which meets the following requirements:
 - an indication that the certificate is issued as a qualified certificate;
 - the identification of the certification-service-provider and the State in which it is established;
 - the name of the signatory or a pseudonym, which shall be identified as such;
 - provision for a specific attribute of the signatory to be included if relevant, depending on the purpose for which the certificate is intended;
 - signature-verification data which correspond to signature-creation data under the control of the signatory;
 - an indication of the beginning and end of the period of validity of the certificate;
 - the identity code of the certificate;
 - the advanced electronic signature of the certification-service-provider issuing it;
 - limitations on the scope of use of the certificate, if applicable; and
 - limits on the value of transactions for which the certificate can be used, if applicable.

- qualified certificate (cont'd)

- and is provided by a certification-service-provider who fulfils:
 - demonstrate the reliability necessary for providing certification services;
 - ensure the operation of a prompt and secure directory and a secure and immediate revocation service;
 - ensure that the date and time when a certificate is issued or revoked can be determined precisely;

- verify, by appropriate means in accordance with national law, the identity and, if applicable, any specific attributes of the person to which a qualified certificate is issued;
 - employ personnel who possess the expert knowledge, experience, and qualifications necessary for the services provided, in particular competence at managerial level, expertise in electronic signature technology and familiarity with proper security procedures; they must also apply administrative and management procedures which are adequate and correspond to recognised standards;
 - use trustworthy systems and products which are protected against modification and ensure the technical and cryptographic security of the process supported by them;
 - take measures against forgery of certificates, and, in cases where the certification-service-provider generates signature-creation data, guarantee confidentiality during the process of generating such data;
- qualified certificate (cont'd)
 - and is provided by a certification-service-provider who fulfils (cont'd):
 - maintain sufficient financial resources to operate in conformity with the requirements laid down in the Directive, in particular to bear the risk of liability for damages, for example, by obtaining appropriate insurance;
 - record all relevant information concerning a qualified certificate for an appropriate period of time, in particular for the purpose of providing evidence of certification for the purposes of legal proceedings. Such recording may be done electronically;
 - not store or copy signature-creation data of the person to whom the certification-service-provider provided key management services;
 - before entering into a contractual relationship with a person seeking a certificate to support his electronic signature inform that person by a durable means of communication of the precise terms and conditions regarding the use of the certificate, including any limitations on its use, the existence of a voluntary accreditation scheme and procedures for complaints and dispute settlement. Such information, which may be transmitted electronically, must be in writing and in readily understandable language. Relevant parts of this information must also be made available on request to third-parties relying on the certificate;
- qualified certificate (cont'd)
 - and is provided by a certification-service-provider who fulfils (cont'd):
 - use trustworthy systems to store certificates in a verifiable form so that:
 - only authorised persons can make entries and changes,
 - information can be checked for authenticity,
 - certificates are publicly available for retrieval in only those cases for which the certificate-holder's consent has been obtained, and
 - any technical changes compromising these security requirements are apparent to the operator;
- *Article 5 - Legal effects of electronic signatures*
 1. Member States shall ensure that advanced electronic signatures which are based on a qualified certificate and which are created by a secure-signature-creation device:
 - satisfy the legal requirements of a signature in relation to data in electronic form in the same manner as a hand-written signature satisfies those requirements in relation to paper-based data; and
 - are admissible as evidence in legal proceedings.
 2. Member States shall ensure that an electronic signature is not denied legal effectiveness and admissibility as evidence in legal proceedings solely on the grounds that it is:
 - in electronic form, or
 - not based upon a qualified certificate, or
 - not based upon a qualified certificate issued by an accredited certification-service-provider, or
 - not created by a secure signature-creation device.

4.2. LU legal framework

- *Code civil - Art. 1322-1.*
 - La signature nécessaire à la perfection d'un acte sous seing privé identifie celui qui l'appose et manifeste son adhésion au contenu de l'acte.
 - Elle peut être manuscrite ou électronique.
 - La signature électronique consiste en un ensemble de données, liées de façon indissociable à l'acte, qui en garantit l'intégrité et satisfait aux conditions posées à l'alinéa premier du présent article.
- *Loi du 14 août 2000 relative au commerce électronique*
 - Art. 18. Des effets juridiques de la signature électronique
 1. Sans préjudice des articles 1323 et suivants du Code civil, une signature électronique créée par un dispositif sécurisé de création de signature que le signataire puisse garder sous son contrôle exclusif et qui repose sur un certificat qualifié, constitue une signature au sens de l'article 1322-1 du Code civil.
 2. Une signature électronique ne peut être rejetée par le juge au seul motif qu'elle se présente sous forme électronique, qu'elle ne repose pas sur un certificat qualifié, qu'elle ne repose pas sur un certificat qualifié délivré par un prestataire accrédité de certification, ou qu'elle n'est pas créée par un dispositif sécurisé de création de signature.
 3. Nul ne peut être contraint de signer électroniquement.
- *Loi du 14 août 2000 relative au commerce électronique (cont'd)*
 - Art. 2. Champ d'application
 1. La présente loi ne s'applique pas:
 - à la fiscalité, sans préjudice des dispositions de l'article 16 de la présente loi;
 - aux accords ou pratiques régis par la législation relative aux ententes;
 - aux activités de jeux d'argent impliquant des mises ayant une valeur monétaire dans les jeux de hasard, y compris les loteries et les transactions sur les paris.
 2. Les dispositions de la présente loi ne s'appliquent pas à la représentation d'un client et la défense de ses intérêts devant les tribunaux.
 3. Les dispositions de la présente loi s'appliquent sans préjudice des dispositions relatives à la protection des données personnelles.
 4. La loi du lieu d'établissement du prestataire de services de la société de l'information s'applique aux prestataires et aux services qu'ils présentent, sans préjudice de la liberté des parties de choisir le droit applicable à leur contrat.

5. La libre circulation des services de la société de l'information en provenance d'un autre Etat membre ne peut être restreinte.
1. Le ministre ayant le commerce électronique dans ses attributions peut, par dérogation aux dispositions du paragraphe (5), restreindre la libre circulation d'un service donné de la société de l'information en provenance d'un autre Etat membre lorsque ledit service porte atteinte, ou représente un risque sérieux et grave d'atteinte à l'ordre public, la sécurité publique, la santé publique ou la protection des consommateurs, en observant par ailleurs les exigences posées par le droit communautaire à l'exercice de cette faculté, et notamment le principe de proportionnalité.
2. Sans préjudice d'éventuelles procédures judiciaires, y compris les procédures pénales, les mesures de restriction ne peuvent être prises que si le ministre ayant le commerce électronique dans ses attributions a au préalable:
 - demandé à l'Etat membre d'origine de prendre des mesures;
 - notifié à la Commission européenne et à l'Etat membre d'origine son intention de prendre des mesures appropriées, si l'Etat membre d'origine ne prend pas de mesures ou si les mesures prises ne sont pas suffisantes.

Il peut être dérogé aux conditions prévues ci-dessus en cas d'urgence. En pareil cas, le ministre ayant le commerce électronique dans ses attributions notifie, dans les plus brefs délais, à la Commission européenne et à l'Etat membre d'origine les mesures prises et les raisons pour lesquelles il estime qu'il y a urgence.»
- Art. 3. De l'usage de la cryptographie
 - L'usage des techniques de cryptographie est libre.
- *Loi du 14 août 2000 relative au commerce électronique (cont'd)*
 - Art. 27. De la responsabilité des prestataires de «services de certification délivrant des certificats qualifiés»
 - Tout prestataire de services de certification délivrant des certificats qualifiés est tenu de notifier à l'Autorité Nationale d'Accréditation et de Surveillance la conformité de ses activités aux exigences de la présente loi et des règlements pris en son exécution.

A moins qu'il ne prouve n'avoir commis aucune négligence, le prestataire de service de certification qui délivre à l'intention du public un certificat qualifié ou qui garantit publiquement un tel certificat est responsable du préjudice causé à toute personne qui se fie raisonnablement:

- à l'exactitude des informations contenues dans le certificat qualifié à dater de sa délivrance;
 - à l'assurance que, au moment de la délivrance du certificat, le signataire identifié dans le certificat qualifié détenait les données afférentes à la création de signature correspondant aux données afférentes à la vérification de signature fournies ou identifiées dans le certificat;
 - à l'assurance que le dispositif de création de signature et le dispositif de vérification de signature fonctionnent ensemble de façon complémentaire, au cas où le prestataire a généré les deux dispositifs.
 - A moins qu'il ne prouve n'avoir commis aucune négligence, le prestataire de service de certification qui délivre à l'intention du public un certificat qualifié ou qui garantit publiquement un tel certificat est responsable du préjudice causé à toute personne qui se prévaut raisonnablement du certificat, pour avoir omis de faire enregistrer la révocation du certificat.
- *Loi du 14 août 2000 relative au commerce électronique (cont'd)*
 - Art. 27. De la responsabilité des prestataires de «services de certification délivrant des certificats qualifiés» (cont'd)
 - Le prestataire de service de certification n'est pas responsable du préjudice résultant de l'usage abusif d'un certificat qualifié qui dépasse les limites fixées à son utilisation ou la valeur limite des transactions pour lesquelles le certificat peut être utilisé, pour autant que ces limites soient inscrites dans le certificat et discernables par les tiers.
 - Les dispositions des paragraphes 1 à 3 sont sans préjudice de la loi modifiée du 25 août 1983 relative à la protection juridique du consommateur.

4.3. CSP supervision/accreditation legal framework

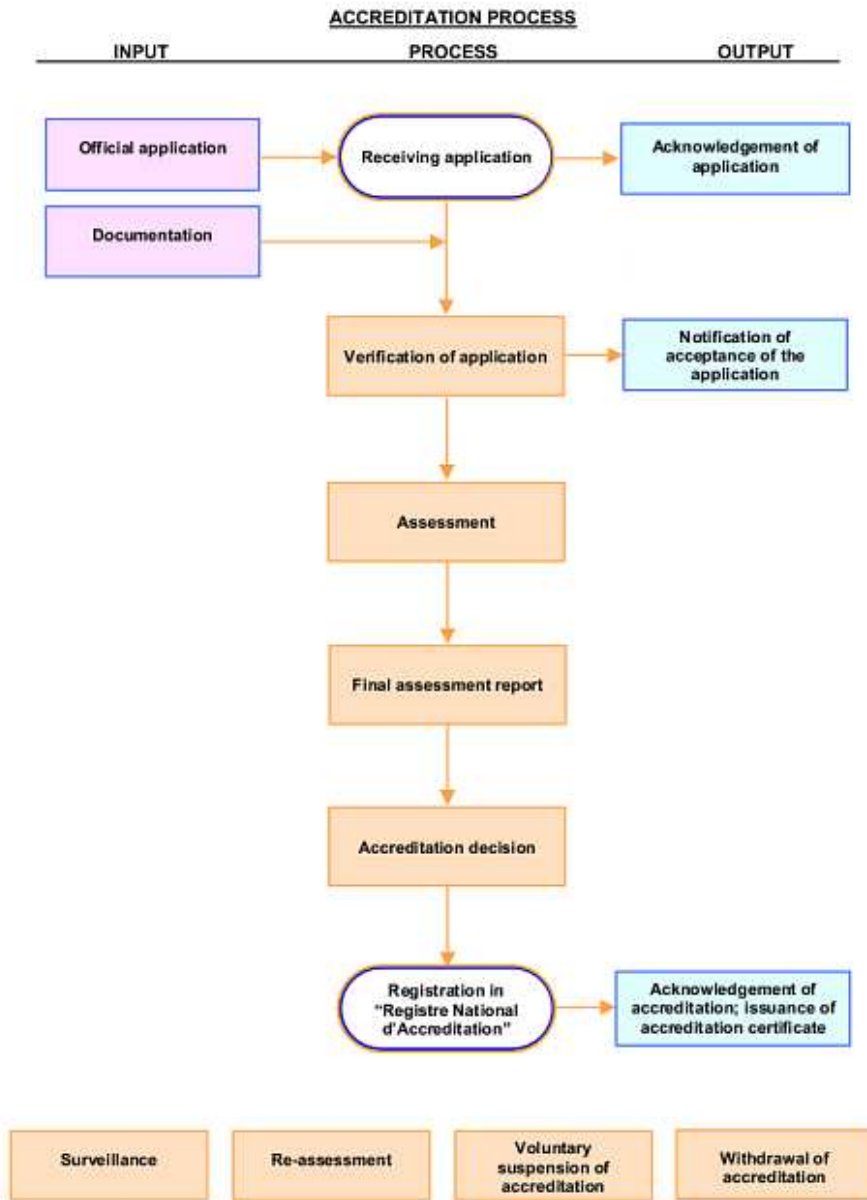
- *Loi du 14 août 2000 relative au commerce électronique (cont'd)*
 - Art. 29. La surveillance (cont'd)
 - L'Autorité Nationale d'Accréditation et de Surveillance tient un registre des notifications, qui fait l'objet, à la fin de chaque année de calendrier, d'une publication au Mémorial, Recueil administratif et économique, sans préjudice de la possibilité, pour l'Autorité Nationale d'Accréditation et de Surveillance, de publier à tout moment, soit au Mémorial, soit dans un ou plusieurs journaux, luxembourgeois ou étrangers, une radiation du registre, si une telle mesure de publicité est commandée par l'intérêt public.
 - L'Autorité Nationale d'Accréditation et de Surveillance veille au respect par les prestataires de services de certification délivrant des certificats qualifiés des exigences contenues dans les articles 19 à 27 de la présente loi et dans les règlements grand-ducaux pris en application.
 - L'Autorité Nationale d'Accréditation et de Surveillance peut, soit d'office, soit à la demande de toute personne intéressée, vérifier ou faire vérifier la conformité des activités d'un prestataire de service de certification délivrant des certificats qualifiés aux dispositions de la présente loi ou des règlements pris en son exécution.
- *Loi du 14 août 2000 relative au commerce électronique (cont'd)*
 - Art. 29. La surveillance (cont'd)
 - L'Autorité Nationale d'Accréditation et de Surveillance peut avoir recours à des auditeurs externes agréés pour de telles vérifications. Un règlement grand-ducal détermine la procédure d'agrément, à délivrer par le ministre ayant le commerce électronique dans ses attributions. Pourront faire l'objet d'un agrément les personnes qui justifient d'une qualification professionnelle adéquate ainsi que de connaissances et d'une expérience spécialisées dans le domaine des technologies des signatures électroniques, et qui présentent des garanties d'honorabilité professionnelle et d'indépendance par rapport aux prestataires de service de certification délivrant des certificats qualifiés dont elles sont appelées à vérifier les activités.
 - Dans l'accomplissement de leur mission de vérification, les agents de l'Autorité Nationale d'Accréditation et de Surveillance, ainsi que les auditeurs externes agréés ont, sur justification de leurs qualités, le droit

d'accéder à tout établissement et de se voir communiquer toutes informations et tous documents qu'ils estimeront utiles ou nécessaires à l'accomplissement de leur mission.

Tout refus de la part d'un prestataire de service de certification de collaborer activement est puni d'une amende de 251 à 20.000 euros. L'Autorité Nationale d'Accréditation et de Surveillance peut, en pareil cas, également procéder à la radiation des prestataires du registre des notifications.

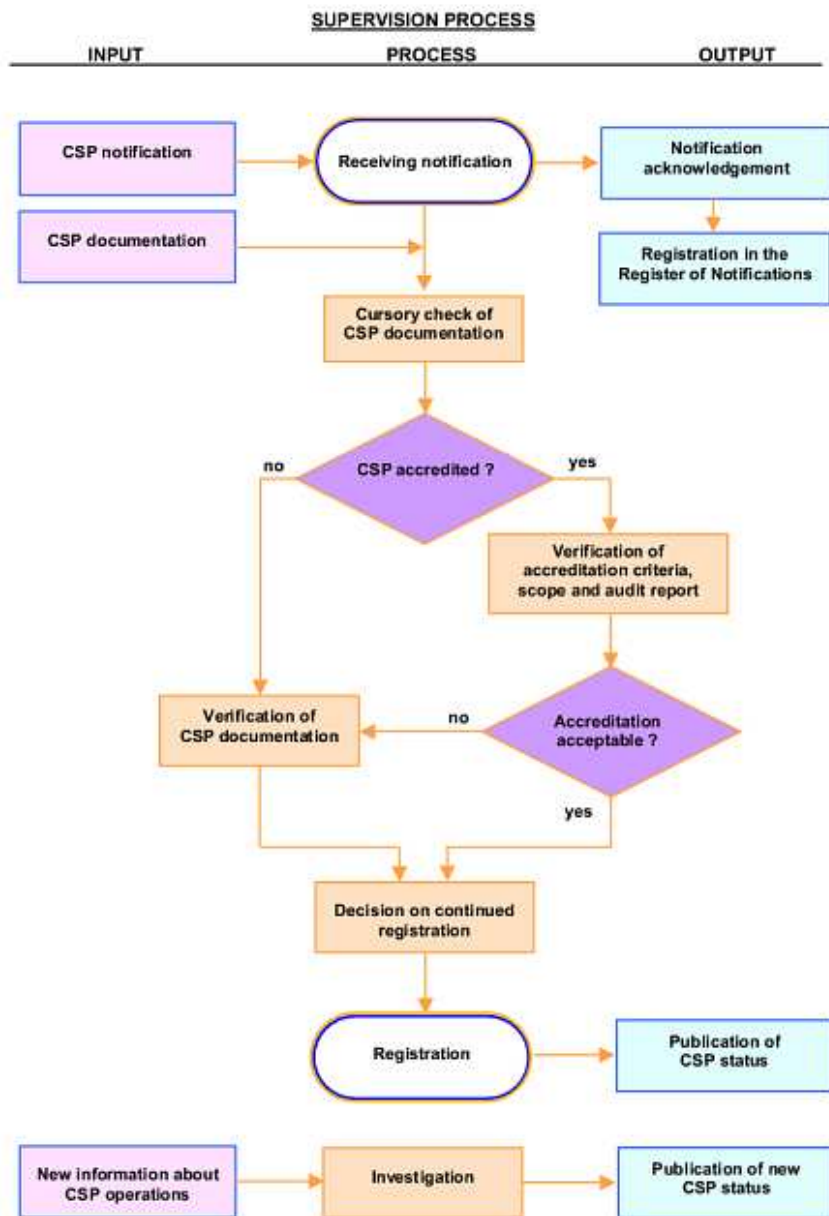
- *Loi du 14 août 2000 relative au commerce électronique (cont'd)*
 - Art. 29. La surveillance (cont'd)
 - Si, sur le rapport de ses agents ou de l'auditeur externe agréé, l'Autorité Nationale d'Accréditation et de Surveillance constate que les activités du prestataire de services de certification délivrant des certificats qualifiés ne sont pas conformes aux dispositions de la présente loi ou des règlements pris en son exécution, elle invite le prestataire à se conformer, dans le délai qu'elle détermine, auxdites dispositions. Si, passé ce délai, le prestataire ne s'est pas conformé, l'Autorité Nationale d'Accréditation et de Surveillance procède à la radiation du prestataire du registre des notifications.
 - En cas de constatation d'une violation grave par un prestataire de services de certification délivrant des certificats qualifiés des dispositions de la présente loi ou des règlements pris en son exécution, l'Autorité Nationale d'Accréditation et de Surveillance peut en informer à telles fins que de droit les autorités administratives compétentes en matière de droit d'établissement. Les rapports établis à l'attention de l'autorité nationale peuvent être communiqués à ces autorités, dans la mesure où le prestataire de service de certification en a reçu communication dans ses relations avec l'Autorité Nationale d'Accréditation et de Surveillance.
- *Loi du 14 août 2000 relative au commerce électronique (cont'd)*
 - Art. 30. De l'accréditation
 1. Les prestataires de service de certification sont libres de demander ou non une accréditation.
 2. L'accréditation couvre la délivrance de certificats relatifs à l'identité, éventuellement à la profession ou tout autre attribut durable du titulaire du certificat, ainsi qu'à toute autre mention pouvant être certifiée.
 3. Le prestataire de service de certification peut demander l'accréditation pour un ou plusieurs de ces éléments et pour une ou plusieurs catégories de titulaires.
- *Loi du 14 août 2000 relative au commerce électronique (cont'd)*
 - Art. 31. Des conditions d'obtention de l'accréditation
 1. Les conditions d'obtention et de conservation de l'accréditation sont fixées par un règlement grand-ducal.
 2. Un règlement grand-ducal détermine:
 1. la procédure de délivrance, d'extension, de suspension et de retrait des accréditations;
 2. les frais d'examen et de suivi des dossiers;
 3. les délais d'examen des demandes;
 4. le montant et les modalités de la garantie financière;
 5. les règles relatives à l'information que le prestataire de service de certification est tenu de conserver concernant ses services et les certificats délivrés par lui;
 6. les garanties d'indépendance que les prestataires de service de certification doivent offrir aux utilisateurs du service;
 7. la durée de conservation des données.
 3. Des conditions complémentaires peuvent être fixées par règlement grand-ducal pour qu'un prestataire de service de certification soit habilité à délivrer des certificats à des personnes qui souhaitent utiliser une signature électronique dans leurs échanges avec les autorités publiques.
 4. La décision sur la suspension ou le retrait de l'accréditation peut être déférée, dans le délai d'un mois, sous peine de forclusion, au tribunal administratif, qui statue comme juge de fond.

4.4. CSP accreditation scheme



© 2005 OLAS - Office Luxembourgeois d'Accréditation et de Surveillance

4.5. CSP supervision scheme



© 2005 OLAS - Office Luxembourgeois d'Accréditation et de Surveillance

5. Bibliographic references

- [Cryptographic introductory notes](#) (Department of Computer Science and Information Systems, The University of Hong Kong)
- [Public key cryptography](#) (Wikipedia)
- [CASES elearning portal](#)
- [Ten risks of PKI](#) (B. Schneier, C. Ellison)
- [Web of trust](#) (Wikipedia)
- [The PGP Trust Model](#) (A. Abdul-Rahman)
- [Why OpenPGP's PKI is better than an X.509](#) (P. Zimmermann) PKI
- [Usability of Security: A Case Study](#) (A. Whitten, J.D. Tygar)
- [The Keysigning party HOWTO](#) (V. Alex Brennen)
- [PKI architectures how to choose one](#) (E. Stavrou)
- [Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures](#)
- [Recueils de Législation: Commerce Electronique](#)