Some Cryptographic Implementations

October 10 – 14, 2016 Guinee Conakry

By

Marcus K. G. Adomey

Chief Operations Manager
AfricaCERT
Email: marcus.adomey@africacert.org

OVERVIEW

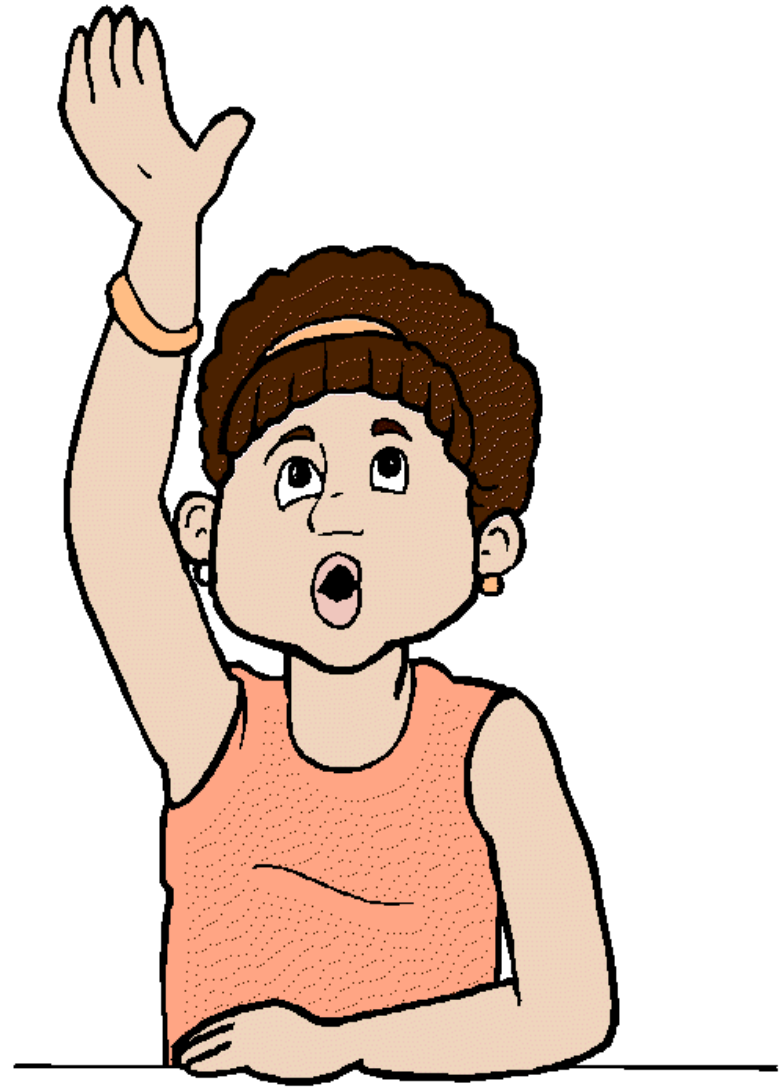
- Fingerprint
- Digital Signature
- Certificate Authority
- Digital Certificate
- Key management
- Public Key Infrastructure (PKI)
- Web of Trust
- Secure Socket Layer (SSL)

Public Key Fingerprint

Public Key Fingerprint

- Public key fingerprint is a short sequence of bytes used to identify a longer public key.
- Fingerprints are created by applying a cryptographic hash function to a public key.
- Since fingerprints are shorter than the keys they refer to, they can be used to simplify certain key management tasks.
- In Microsoft software, "thumbprint" is used instead of "fingerprint."

User-ID:	Heinrich Heine (test) <heinrich@gpg4win.de>
Validity:	from 2010-03-05 05:06 until forever
Certificate type:	2,048-bit RSA (secret certificate available)
Certificate usage:	Signing EMails and Files, Encrypting EMails and Files, Certifying other Certificates
Key-ID:	C93D94BA
Fingerprint:	7EDC0D141A82250847448E91FE7EEC85C93D94BA
Stored:	on this computer

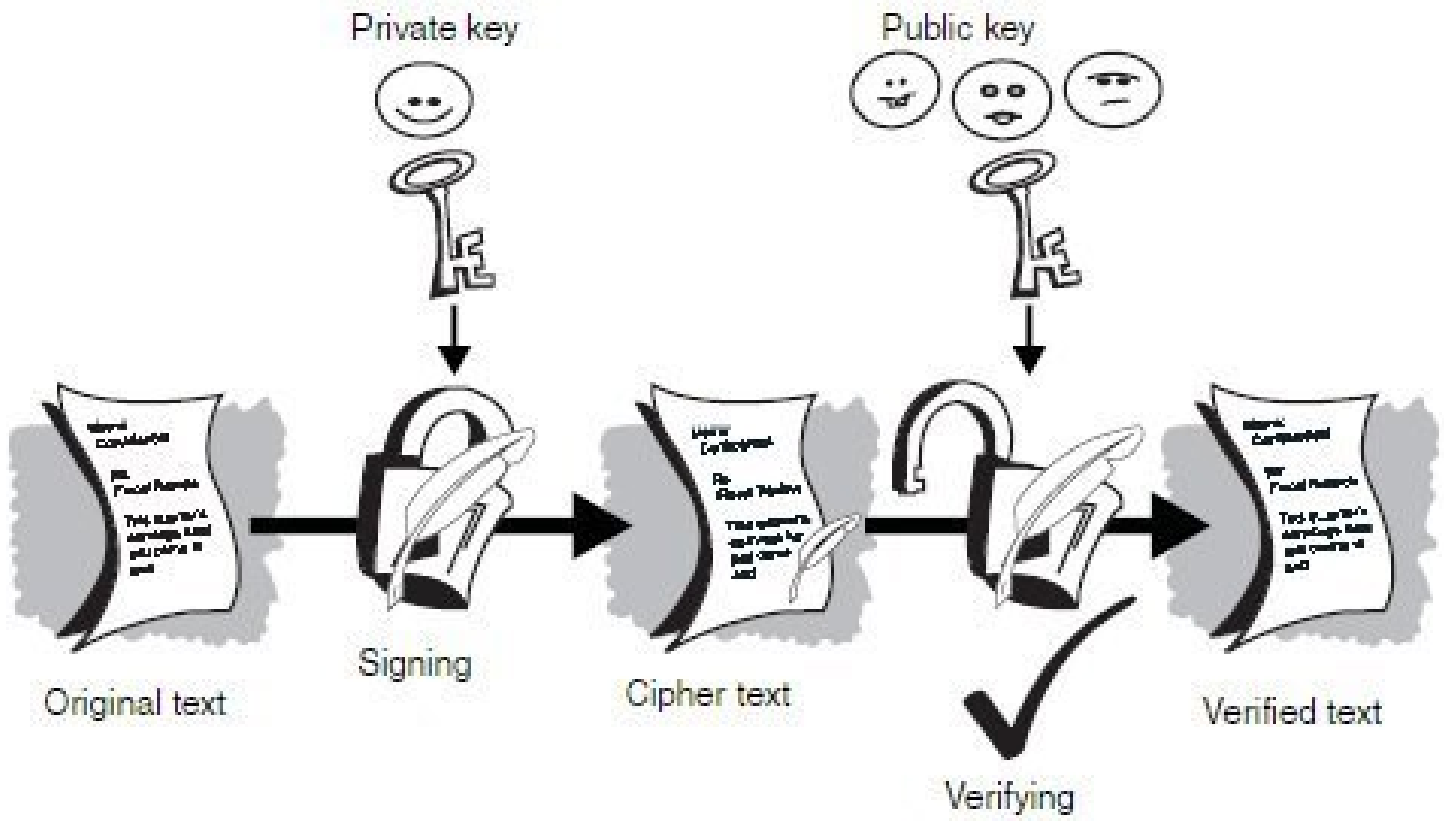


Digital Signature

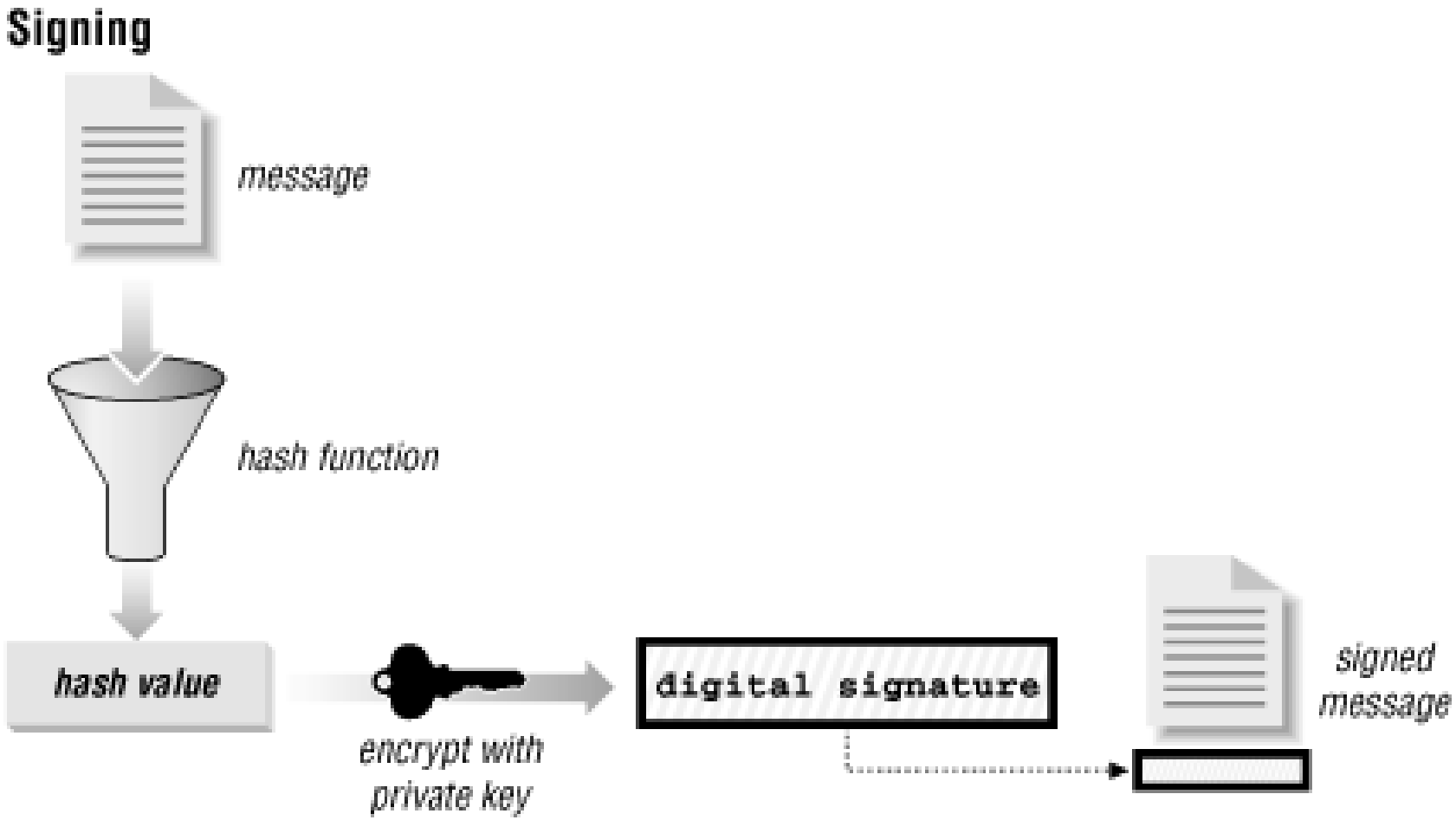
Digital Signature

- A digital signature is an electronic signature that can be used to authenticate the identity of the sender of a message or the signer of a document, and possibly to ensure that the original content of the message or document that has been sent is unchanged.
- Digital signatures are easily transportable, cannot be imitated by someone else, and can be automatically time-stamped. The ability to ensure that the original signed message arrived means that the sender cannot easily repudiate it later.
- A digital signature can be used with any kind of message, whether it is encrypted or not, simply so that the receiver can be sure of the sender's identity and that the message arrived intact.
- A valid digital signature gives a recipient reason to believe that the message was created by a known sender, that the sender cannot deny having sent the message (authentication and non-repudiation), and that the message was not altered in transit (integrity).

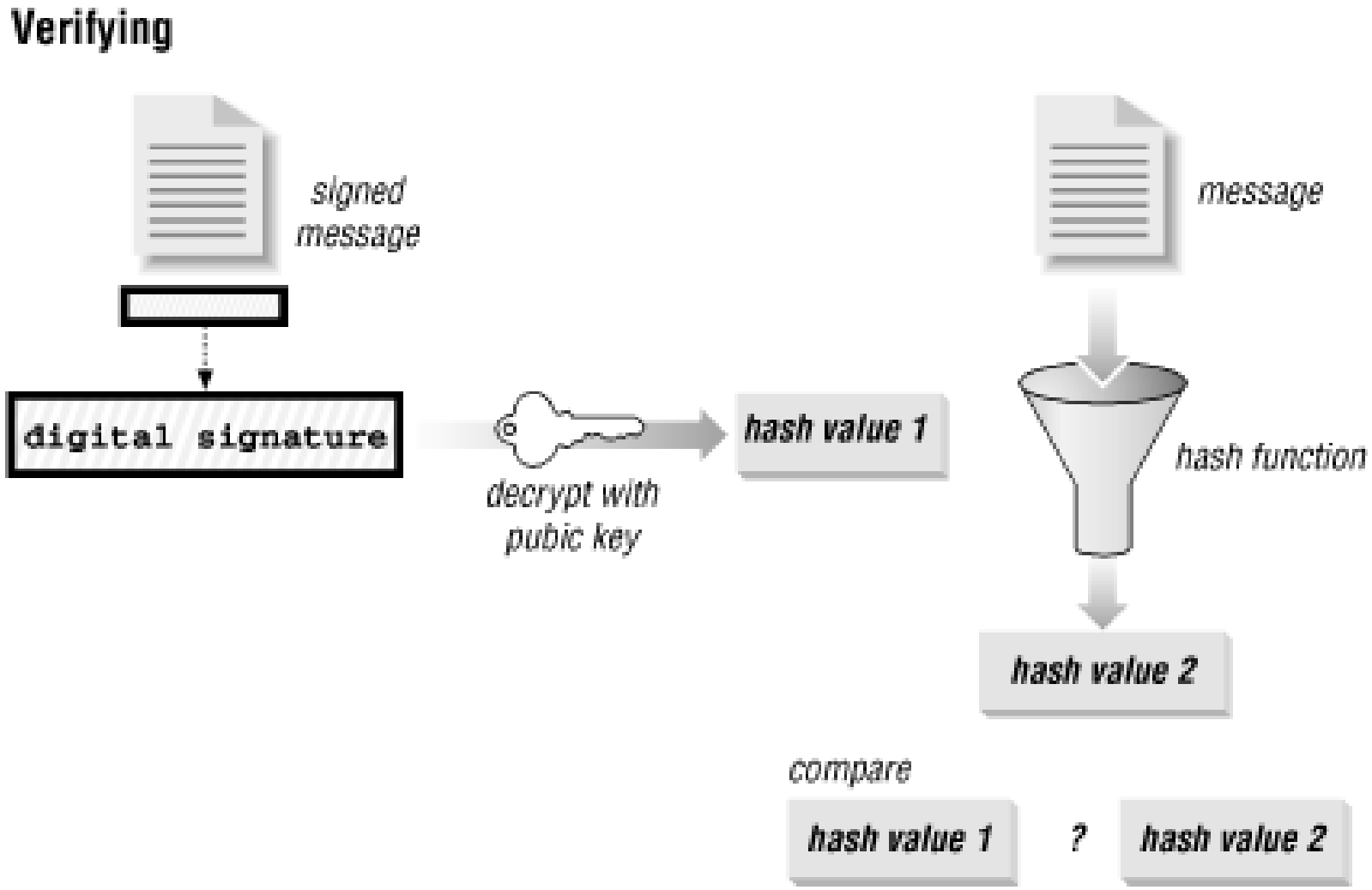
Digital Signature



Digital Signature



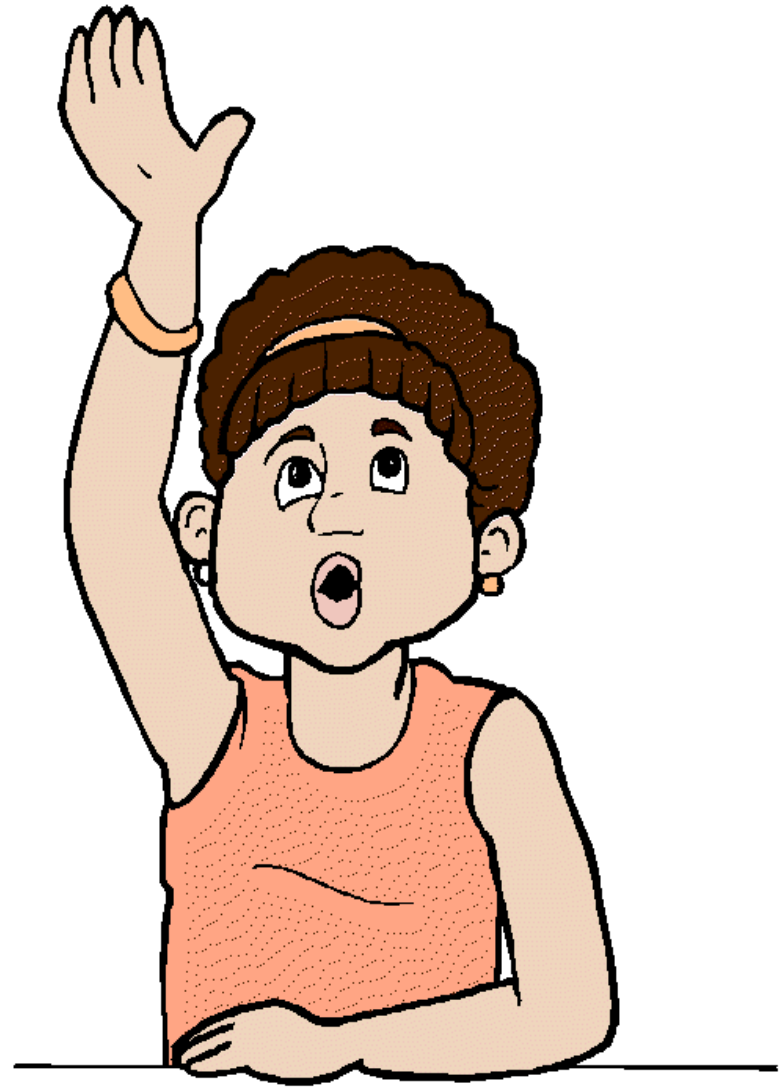
Digital Signature



Digital Signature

Physical Signature vs. Digital Signature

Physical Signature	Digital Signature
Physical Signature is just a writing on paper	Digital Signature encompasses crucial parameters of identification
Physical Signature can be copied	It is IMPOSSIBLE to copy a Digital signature
Physical Signature does not give privacy to content	Digital Signature also enables encryption and thus privacy
Physical Signature cannot protect the content	Digital Signature protects the content



Digital Certificate

Digital Certificate

- A digital certificate is an electronic “ID card" that establishes your credentials when doing business or other transactions on the Web.
- It is issued by a ***certification authority*** (CA)
- A digital certificate is also an electronic "passport" that allows a person, computer or organization to exchange information securely over the Internet using the public key infrastructure (PKI)
- A certificate authority (CA) is an authority in a network that issues and manages security credentials and public keys for message encryption
- A CA checks with a registration authority (RA) to verify information provided by the requestor of a digital certificate
- If the RA verifies the requestor's information, the CA can then issue a certificate

Digital Certificate

Types of Certificates

There are different types of certificates, each with different functions

Root or Authority Certificates

- create the base (or root) of a certification authority hierarchy.
- are self signed by the CA that created them
- not signed by another CA
- When a certificate is self-signed, it means that the name in the Issuer field is the same as the name in the Subject Field.

Digital Certificate

Types of Certificates

Institutional authority certificates

These certificates are also called campus certificates. These certificates are signed by a third party verifying the authenticity of a campus certification authority. Campuses then use their “authority” to issue client certificates for faculty, staff, and students.

Client certificates

These are also known as end-entity certificates, identity certificates, or personal certificates. The Issuer is typically the campus CA.

Web server certificates

These certificates are used to secure communications to and from Web servers, for example when you buy something on the Web. They are called server-side certificates. The Subject name in a server certificate is the DNS name of the server.

Digital Certificate

Types of Certificates

Object signing certificates

An object signing certificate is a certificate that you use to digitally "sign" an object. By signing the object, you provide a means by which you can verify both the object's integrity and the origination or ownership of the object.

User certificates

A user certificate is a digital credential that validates the identity of the client or user that owns the certificate.

Digital Certificate

Certificate Standards

X.509

- is an important standard for a public key infrastructure (PKI) to manage digital certificates and public-key encryption
- An ITU-T standard,
- uses to verify that a public key belongs to the user, computer or service identity contained within the certificate
- widely accepted international PKI standard
- specifies formats for public key certificates, certificate revocation lists, attribute certificates, and a certification path validation algorithm
- used as a key part of the Transport Layer Security protocol used to secure web and email communication.

Certificate Authority

Certificate Standards

Structure of X.509 certificate

Serial Number: Used to uniquely identify the certificate.

Subject: The person, or entity identified.

Signature Algorithm: The algorithm used to create the signature.

Signature: The actual signature to verify that it came from the issuer.

Issuer: The entity that verified the information and issued the certificate.

Valid-From: The date the certificate is first valid from.

Valid-To: The expiration date.

Public Key: The public key.

Thumbprint Algorithm: The algorithm used to hash the public key certificate.

Fingerprint/Thumbprint : The hash itself, used as an abbreviated form of the public key certificate.

```
$ openssl x509 -in freesoft-certificate.pem -noout -text
Certificate:
   Data:
       Version: 1 (0x0)
       Serial Number: 7829 (0x1e95)
       Signature Algorithm: md5WithRSAEncryption
       Issuer: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting cc,
               OU=Certification Services Division,
               CN=Thawte Server CA/emailAddress=server-certs@thawte.com
       Validity
           Not Before: Jul  9 16:04:02 1998 GMT
           Not After : Jul  9 16:04:02 1999 GMT
       Subject: C=US, ST=Maryland, L=Pasadena, O=Brent Baccala,
                OU=FreeSoft, CN=www.freesoft.org/emailAddress=baccala@freesoft.org
       Subject Public Key Info:
           Public Key Algorithm: rsaEncryption
           RSA Public Key: (1024 bit)
               Modulus (1024 bit):
                   00:b4:31:98:0a:c4:bc:62:c1:88:aa:dc:b0:c8:bb:
                   33:35:19:d5:0c:64:b9:3d:41:b2:96:fc:f3:31:e1:
                   66:36:d0:8e:56:12:44:ba:75:eb:e8:1c:9c:5b:66:
                   70:33:52:14:c9:ec:4f:91:51:70:39:de:53:85:17:
                   16:94:6e:ee:f4:d5:6f:d5:ca:b3:47:5e:1b:0c:7b:
                   c5:cc:2b:6b:c1:90:c3:16:31:0d:bf:7a:c7:47:77:
                   8f:a0:21:c7:4c:d0:16:65:00:c1:0f:d7:b8:80:e3:
                   d2:75:6b:c1:ea:9e:5c:5c:ea:7d:c1:a1:10:bc:b8:
                   e8:35:1c:9e:27:52:7e:41:8f
               Exponent: 65537 (0x10001)
   Signature Algorithm: md5WithRSAEncryption
       93:5f:8f:5f:c5:af:bf:0a:ab:a5:6d:fb:24:5f:b6:59:5d:9d:
       92:2e:4a:1b:8b:ac:7d:99:17:5d:cd:19:f6:ad:ef:63:2f:92:
       ab:2f:4b:cf:0a:13:90:ee:2c:0e:43:03:be:f6:ea:8e:9c:67:
       d0:a2:40:03:f7:ef:6a:15:09:79:a9:46:ed:b7:16:1b:41:72:
       0d:19:aa:ad:dd:9a:df:ab:97:50:65:f5:5e:85:a6:ef:19:d1:
       5a:de:9d:ea:63:cd:cb:cc:6d:5d:01:85:b5:6d:c8:f3:d9:f7:
       8f:0e:fc:ba:1f:34:e9:96:6e:6c:cf:f2:ef:9b:bf:de:b5:22:
       68:9f
```

```
$ openssl x509 -in thawte-ca-certificate.pem -noout -text
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 1 (0x1)
        Signature Algorithm: md5WithRSAEncryption
        Issuer: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting cc,
                OU=Certification Services Division,
                CN=Thawte Server CA/emailAddress=server-certs@thawte.com
        Validity
            Not Before: Aug  1 00:00:00 1996 GMT
            Not After : Dec 31 23:59:59 2020 GMT
        Subject: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting cc,
                 OU=Certification Services Division,
                 CN=Thawte Server CA/emailAddress=server-certs@thawte.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
                    00:d3:a4:50:6e:c8:ff:56:6b:e6:cf:5d:b6:ea:0c:
                    68:75:47:a2:aa:c2:da:84:25:fc:a8:f4:47:51:da:
                    85:b5:20:74:94:86:1e:0f:75:c9:e9:08:61:f5:06:
                    6d:30:6e:15:19:02:e9:52:c0:62:db:4d:99:9e:e2:
                    6a:0c:44:38:cd:fe:be:e3:64:09:70:c5:fe:b1:6b:
                    29:b6:2f:49:c8:3b:d4:27:04:25:10:97:2f:e7:90:
                    6d:c0:28:42:99:d7:4c:43:de:c3:f5:21:6d:54:9f:
                    5d:c3:58:e1:c0:e4:d9:5b:b0:b8:dc:b4:7b:df:36:
                    3a:c2:b5:66:22:12:d6:87:0d
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints: critical
                CA:TRUE
    Signature Algorithm: md5WithRSAEncryption
        07:fa:4c:69:5c:fb:95:cc:46:ee:85:83:4d:21:30:8e:ca:d9:
        a8:6f:49:1a:e6:da:51:e3:60:70:6c:84:61:11:a1:1a:c8:48:
        3e:59:43:7d:4f:95:3d:a1:8b:b7:0b:62:98:7a:75:8a:dd:88:
        4e:4e:9e:40:db:a8:cc:32:74:b9:6f:0d:c6:e3:b3:44:0b:d9:
        8a:6f:9a:29:9b:99:18:28:3b:d1:e3:40:28:9a:5a:3c:d5:b5:
        e7:20:1b:8b:ca:a4:ab:8d:e9:51:d9:e2:4c:2c:59:a9:da:b9:
        b2:75:1b:f6:42:f2:ef:c7:f2:18:f9:89:bc:a3:ff:8a:23:2e:
        70:47
```

Public Key Infrastructure (PKI)

Public Key Infrastructure (PKI)

- is a set of roles, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates and manage public-key encryption.
- is responsible for issuing certificates, ensuring the distribution of these certificates through a directory, and validating certificates.

The purpose of a PKI is to facilitate the secure electronic transfer of information for a range of network activities such as e-commerce, internet banking and confidential email.

PKI provides assurance of public key. It provides the identification of public keys and their distribution. An anatomy of PKI comprises of the following components.

Public Key Infrastructure (PKI)

An anatomy of PKI comprises of the following components.

- A certificate authority (CA) that stores, issues and signs the digital certificates
- A registration authority which verifies the identity of entities requesting their digital certificates to be stored at the CA
- A central directory—i.e., a secure location in which to store and index keys
- A certificate management system managing things like the access to stored certificates or the delivery of the certificates to be issued.
- A certificate policy
- Certificate Management System
- Public Key Certificate, commonly referred to as ‘digital certificate’.
- Private Key tokens.

Key Management

There are two specific requirements of key management for public key cryptography.

- **Secrecy of private keys**. Throughout the key lifecycle, secret keys must remain secret from all parties except those who are owner and are authorized to use them.
- **Assurance of public keys**. In public key cryptography, the public keys are in open domain and seen as public pieces of data. By default there are no assurances of whether a public key is correct, with whom it can be associated, or what it can be used for. Thus key management of public keys needs to focus much more explicitly on assurance of purpose of public keys.
    - The distribution of public keys.
    - The use of public-key encryption to distribute secret keys.

The most crucial requirement of 'assurance of public key' can be achieved through the public-key infrastructure (PKI), a key management systems for supporting public-key cryptography.

Certificate Authority

Certificate Standards

Some Certificate Authorities

Addtrust	Certum Trusted Network
Entrust	Equifax
GeoTrust Global CA	GlogalSign
Go Daddy	GTE CyberTrust
Secure Trust CA	Starfield Root CA
Thwate	Verisign

Digital Certificate

Certificate Standards

OpenPGP

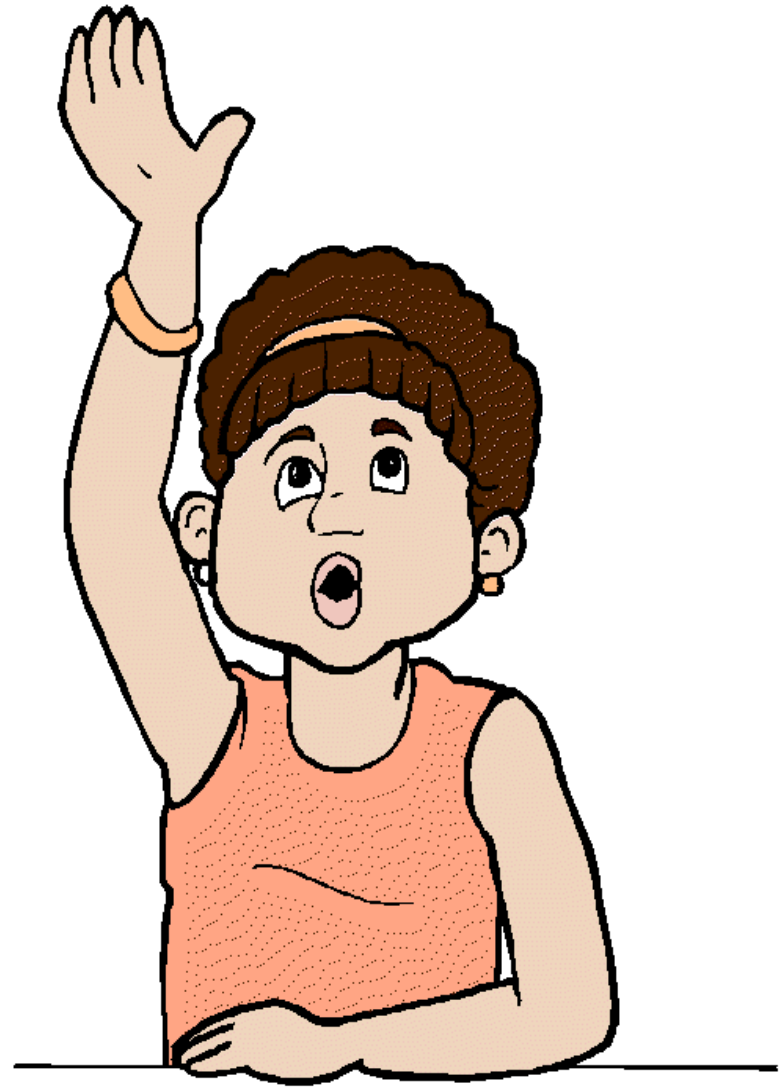
- OpenPGP is on the Internet Standards Track and is under active development
- Many e-mail clients provide OpenPGP-compliant email security as described in RFC 3156.
- The current specification is RFC 4880 (November 2007), the successor to RFC 2440
- RFC 4880 specifies a suite of required algorithms consisting of ElGamal encryption, DSA, Triple DES and SHA-1.

Certificate Authority

Certificate Standards

OpenPGP

Field	Description
version	The field that indicates the version of the OpenPGP structure.
user ID	An RFC 2822 string that identifies the owner of the key. There may be multiple user identifiers in a key.
public key	The main public key of the certificate.
expiration	The expiration time of the main public key.
public subkey	An additional public key of the certificate. There may be multiple subkeys in a certificate.
public subkey expiration	The expiration time of the subkey.



Web of Trust

Web of Trust

A web of trust is a concept used in PGP, GnuPG, and other OpenPGP-compatible systems to establish the authenticity of the binding between a public key and its owner.

Its decentralized trust model is an alternative to the centralized trust model of a public key infrastructure (PKI), which relies exclusively on a certificate authority (or a hierarchy of such).

The web of trust concept was first put forth by PGP creator Phil Zimmermann in 1992 in the manual for PGP version 2.0:

Key Signing Party

A key signing party is a get-together with PGP users for the purpose of meeting other PGP users and signing each other's keys. This helps to extend the "web of trust" to a great degree. Also, it sometimes serves as a forum to discuss strong cryptography and related issues.

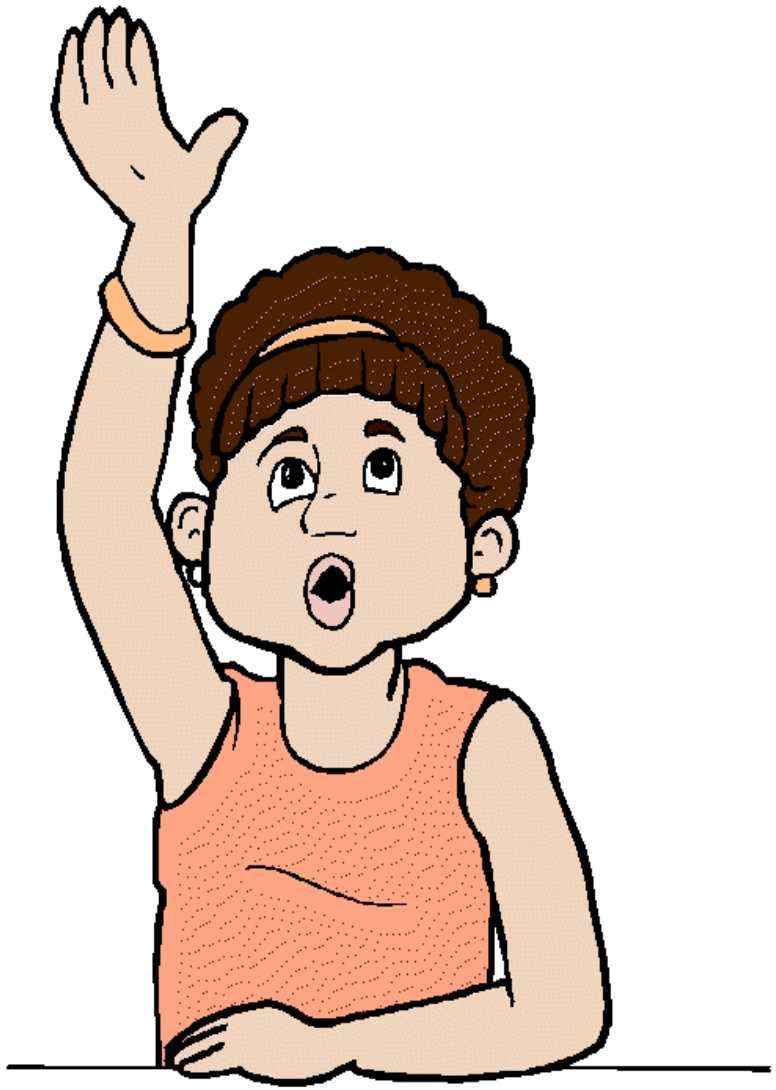
Items required

Physical attendance.

Positive picture ID.

Your key ID, key type, fingerprint, and key size. (Key size and fingerprint together are important since it is possible for two RSA keys of different sizes to have the same fingerprint.)

Secure Socket Layer



Thank you