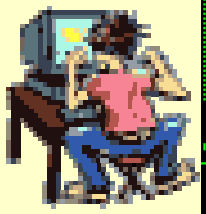
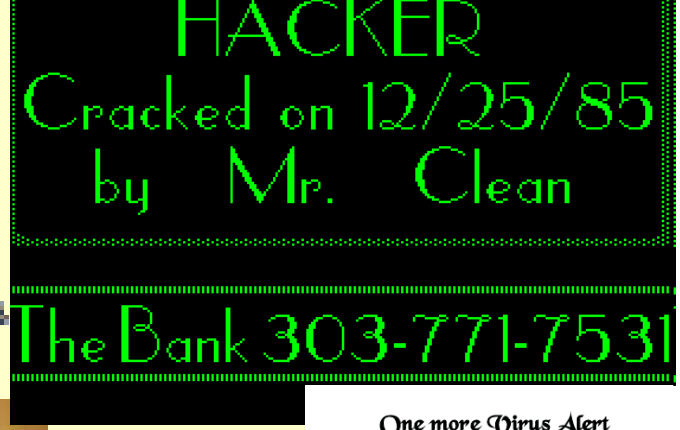




Sicurezza e Internet 04

sommario

- Crittografia
  - Simmetrica (privata)
  - Asimmetrica (pubblica)
  - Una combinazione delle due
- Hashing e Firma Digitale
- La crittografia applicata ai servizi di sicurezza
- La PKI (organizzazione della distribuzione delle chiavi)
  - Certification authority CA
  - Registration Authority RA
  - Certificate Server

La Sicurezza logica

Certificato digitale
Username e password
Controllo degli accessi e autenticazione
Crittografia
SSL - Secure Socket Layer
Firma digitale
Firewall
Servizi di Intrusion Detection (IDS)
Antivirus
Email scanning
Virtual POS
SET - Secure Electronic Transaction
Disaster Recovery

La Sicurezza logica **e la Crittografia**

La maggior parte dei servizi di sicurezza è basata sull'utilizzo della crittografia (cifratura) in varie forme

Crittografia … fin da tempi più antichi ...

… un po’ di storia 1/3

I primi esempi di crittografia trovano riscontro già nel 400 a.c. presso gli spartani che usavano scrivere il messaggio in verticale su di un pezzo di cuoio arrotolato attorno ad un bastone di un certo diametro. Solo chi riavvolgeva il cuoio attorno ad un bastone dello stesso diametro poteva leggere il messaggio originale.

Giulio Cesare, durante le sue campagne introduce il cifrario monoalfabetico che consiste nel sostituire ogni lettera con quella successiva di *n* posizioni:

s e m i n a r i o

v h p n q d u n r

in questo caso la chiave di cifratura è il modulo n delle posizioni da traslare (3).

Crittografia … fin dai tempi più antichi ...

… un po’ di storia 2/3

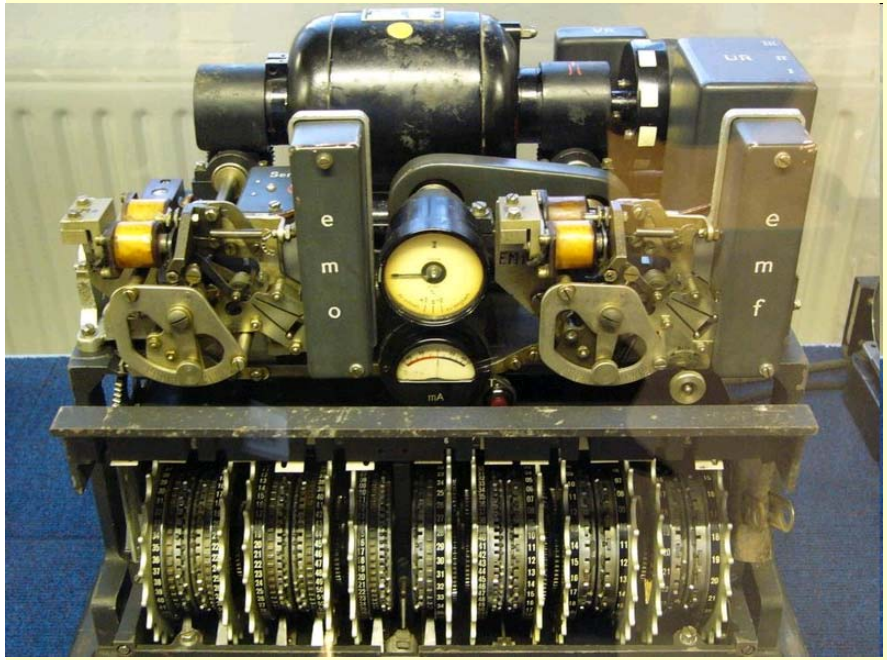
Cesare Augusto introduce il cifrario polialfabetico che consiste nel far corrispondere alla n-esima lettera del messaggio la n-esima lettera del testo di un libro noto agli interlocutori. In questo caso la **chiave di cifratura** è il libro utilizzato per effettuare la sostituzione delle lettere.

Sistemi sempre più complessi furono utilizzati, ma una svolta significativa in termini di sicurezza si ebbe con l'avvento della seconda guerra mondiale. I tedeschi idearono una macchina chiamata *Enigma*, gli inglesi riuscirono a costruire *Colossus* che permetteva di decifrarne i messaggi.

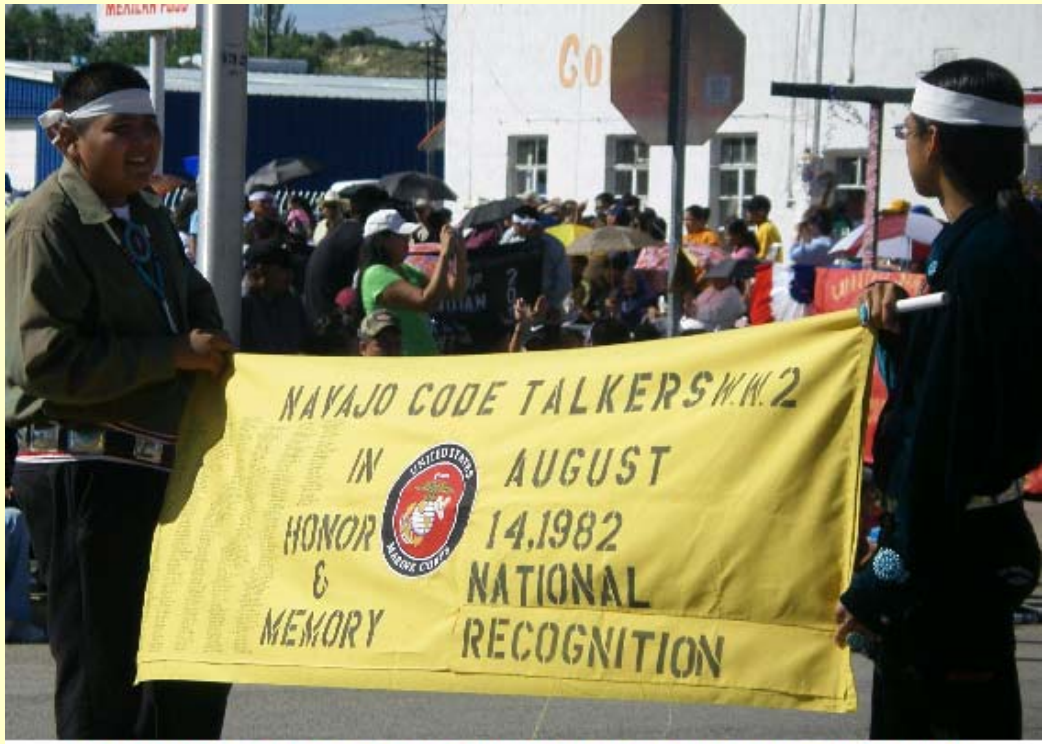
L'avvento dei calcolatori e l'applicazione di algoritmi matematici complessi hanno oggi reso molto più affidabili i sistemi di cifratura.

Crittografia … 60 anni fa ...

… un po’ di storia 3/3



The German Lorenz cipher machine, used in World War II for encryption of very high-level general staff messages



The Navajo "Codetalkers" in II World War Marine Corp

L’uso di “chiavi”

- La moderna crittografia è basata su algoritmi che trasformano il testo in modo reversibile.
- La variante, che rende difficile la interpretazione è un parametro chiamato “chiave”

❖L’algoritmo è pubblico, standard e conosciuto da tutti mentre la chiave è segreta.

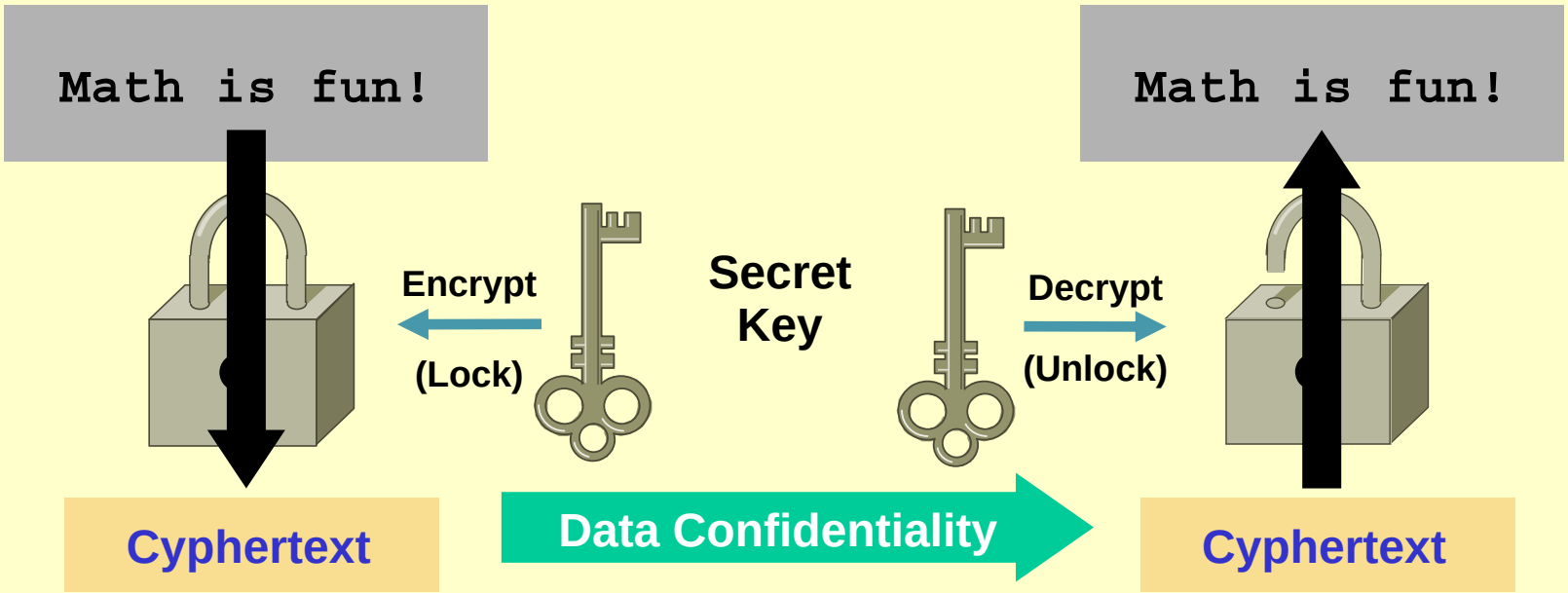
Encryption Fundamentals

Data Encryption Basics

What Is Encryption?

A method of protecting the confidentiality of data

Uses keys to encrypt the data, and decrypt it at



Due tipi di chiavi (e di crittografia)

Simmetriche e asimmetriche












Le tipologie di crittografia 1/3

Simmetrica o a chiave privata:

Si utilizza una chiave nota solo al mittente e al destinatario.

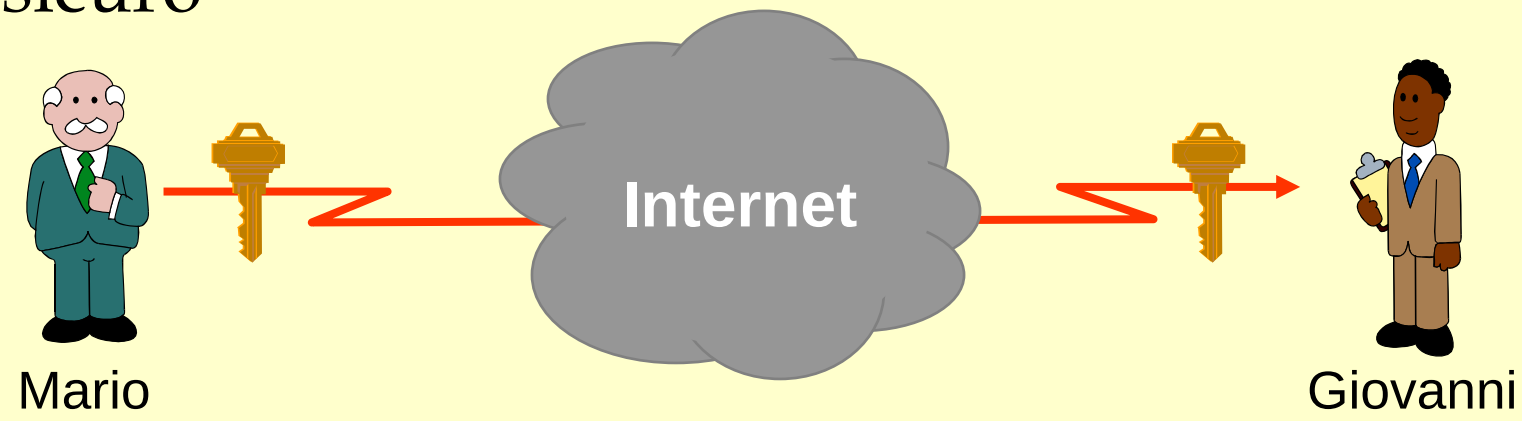
E' molto veloce ma ha l'inconveniente di dover inviare la chiave privata di cifratura al destinatario.

Altra criticità è che a volte la chiave di cifratura viene …*dimenticata* da chi la deve usare.

L'algoritmo più diffuso è il Data Encryption Standard - DES che nasce dai laboratori della IBM e che nel 1997 diventa standard del Governo americano.

Un segreto comune: la chiave

- Mario e Giovanni hanno un segreto comune (che non è a conoscenza di nessun altro)
- Infatti entrambi conoscono la chiave di cifratura della crittografia simmetrica
- Devono entrambi custodire la chiave e, se vogliono includere qualcuno nel "*club*" hanno il problema di comunicare la chiave in modo sicuro



Le tipologie di crittografia 2/3

Asimmetrica o a chiave pubblica:

Ideata da Diffie-Hellman, prevede l'utilizzo di una coppia di chiavi:

-una privata, nota solo all'autore del messaggio,

-una pubblica, nota a tutti (esiste una sorta di elenco telefonico delle chiavi pubbliche).

Il processo di **crittografia asimmetrica** si basa su due capisaldi:

1) il messaggio cifrato con la chiave privata può essere messo in chiaro soltanto attraverso l'utilizzo della chiave pubblica (e viceversa),

2) da una tipologia di chiave (per es.quella pubblica) non si può risalire in alcun modo all'altra chiave (per es.quella privata).

L'algoritmo più diffuso è l'RSA (da Rivest Shamir e Adleman) ….Altri algoritmi: DSA, curve ellittiche, ECC, ...

Le tipologie di crittografia 3/3

RSA: dati due grandi numeri **p** e **q** :

- interi, dispari, positivi e numeri primi

Per i curiosi appassionati

$$Key_{pub} = \text{numero primo rispetto a } N=(p)x(q)$$

$$Key_{pri} = \text{numero tale che } Key_{pri} \times Key_{pub} \text{ modulo } N \text{ sia} = 1$$

Detto **M** il messaggio da cifrare e **X** il corrispondente messaggio cifrato, il processo di codifica risulta rappresentabile attraverso la relazione:

$$X = M^{key_{pub}} \text{ modulo } N$$

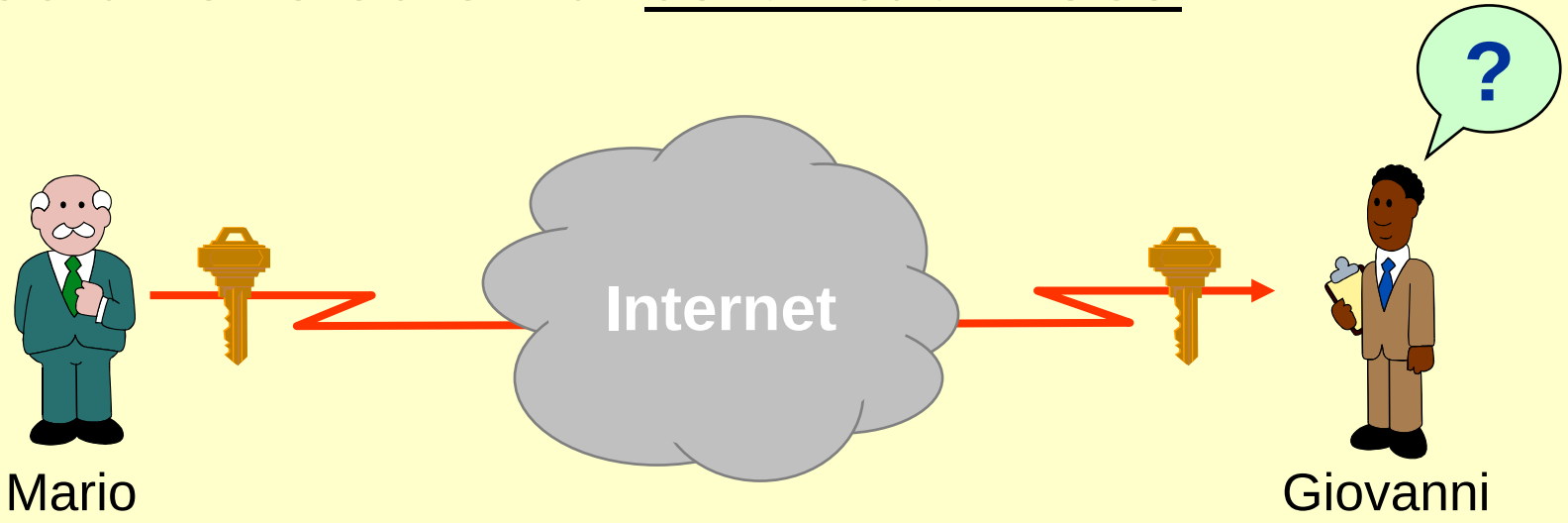
e quello di decodifica dalla relazione:

$$X^{key_{pri}} \text{ modulo } N = (M^{key_{pub}} \text{ modulo } N)^{key_{pri}} \text{ modulo } N$$
$$= M^{key_{pub} \times key_{pri}} \text{ modulo } N = M$$

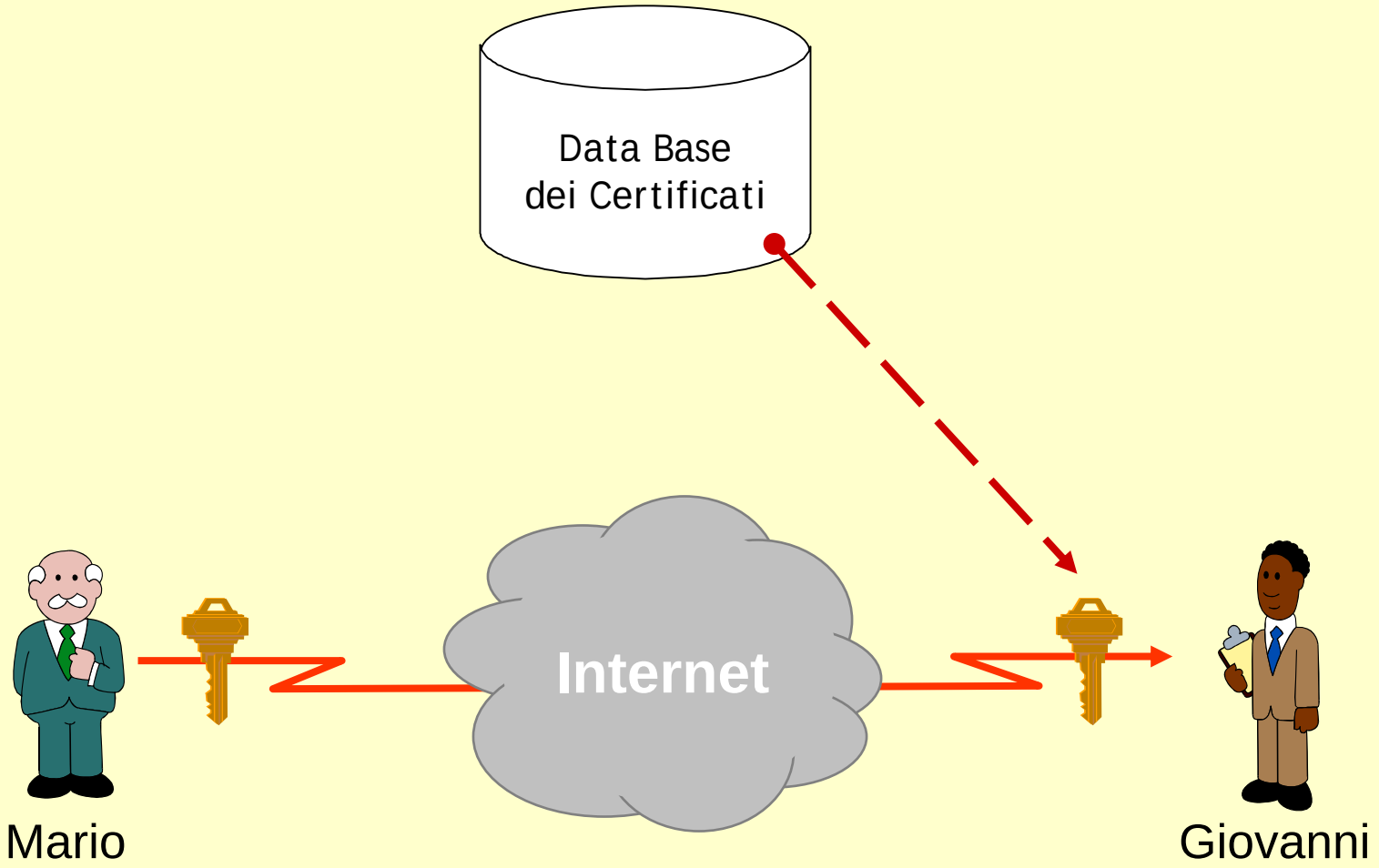
Una chiave di crittografia a 128 bit, stante le attuali potenze di elaborazione, garantisce un costo agli attacchi di 1016 anni.

La distribuzione delle chiavi pubbliche

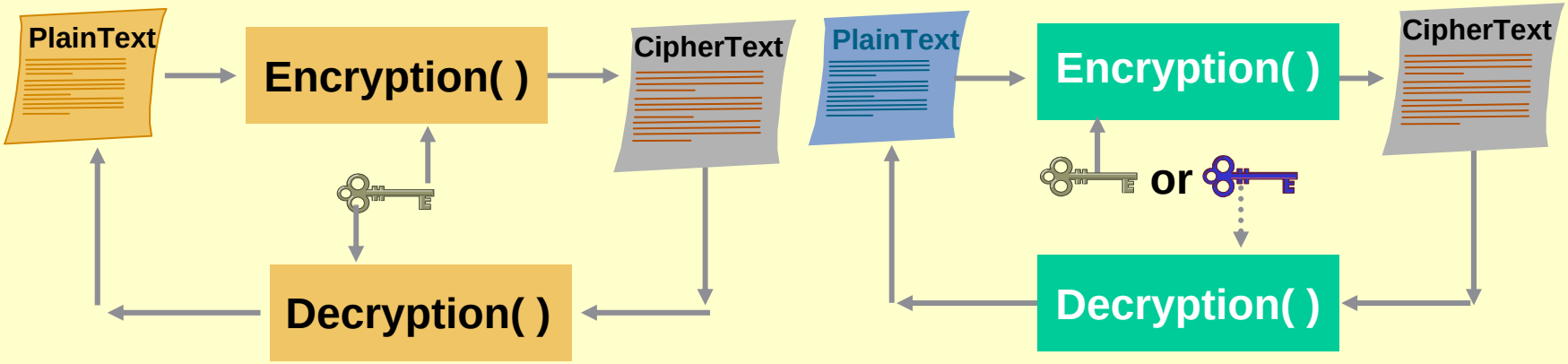
- La chiave pubblica di Mario è *davvero* quella di Mario?
- Dove posso reperire la vera chiave di Mario?
- Soluzione odierna: certificati X.509



La Certification Authority



Symmetric vs. Asymmetric Encryption Algorithms



- Secret-key cryptography
- Encryption and decryption use the same key
- Typically used to encrypt the content of a message
- Examples: DES

- Public-key cryptography
- Encryption and decryption use different keys
- Typically used in digital certification and key management
- Examples: Diffie-Hellman, RSA

Security Level of Crypto Algorithms

Security Level	Work Factor	Algorithms
Weak	$O(2^{40})$	DES, MD5
Legacy	$O(2^{64})$	RC4, SHA1
Minimum	$O(2^{80})$	3DES, SEAL, SKIPJACK
Standard	$O(2^{128})$	AES-128, SHA-256
High	$O(2^{192})$	AES-192, SHA-384
Ultra	$O(2^{256})$	AES-256, SHA-512

Misura della sicurezza per le chiavi simmetriche

- chiave di 40 bit ha circa 1.099 miliardi di combinazioni ($1{,}09*10^{12}$)
- se il livello è minimo e serve solo una protezione a brevissimo periodo allora è sufficiente utilizzare una chiave di lunghezza inferiore ai 64 bit;
- se si devono proteggere dei dati per brevi periodi e solo contro l'attacco di singoli individui o piccole società allora si può adottare una chiave a 72 bit;
- per avere una protezione garantita per un paio di anni la lunghezza minima della chiave deve essere di 80 bit;
- una chiave a 96 bit è prevedibile che offra una protezione non superiore ai 10 anni;
- per una protezione di 20 anni si deve utilizzare una chiave di almeno 112 bit ;
- dati estremamente sensibili o che devono resistere per almeno 30 anni devono essere protetti con una chiave non inferiore ai 128 bit; la chiave di 128 bit ha circa $3*10^{38}$ combinazioni
- la protezione offerta dalle chiavi a 256 bit, che alcuni algoritmi permettono di utilizzare, si può definire, allo stato attuale della tecnica, "da qui all'eternità".

Efficiency

The Table Below Shows the Comparable Key Lengths Required in DH/RSA as Compared to Secure a Symmetric Key of a Given Length

Symmetric Key Length		DH/RSA Key Length
80		1024
112		2048
128		3072
192		7680
256		15360

Reference: draft-ietf-ipsec-ike-ecc-groups-05.txt with Further Reference Contained Therein

Misura della sicurezza per le chiavi asimmetriche

- per offrire la protezione offerta da una chiave simmetrica ad 80 bit , la chiave RSA deve essere lunga 1248 bit;
- per avere la protezione offerta da una chiave simmetrica a 128 bit bisogna salire a 3248 bit;
- per avere invece la protezione offerta da una chiave a 256 bit dobbiamo addirittura utilizzare una chiave pubblica di ben 15424 bit!
- Molte chiavi pubbliche attuali sono di soli 512 bit, corrispondenti ad una chiave simmetrica di appena 50 bit e sono assolutamente inefficaci per proteggere i dati più sensibili!
- Anche le chiavi pubbliche a 1024 bit, le più diffuse, offrono la protezione di una chiave simmetrica da 73 bit, oggigiorno violabile in veramente pochi giorni di calcolo.
- Meglio utilizzare chiavi pubbliche di almeno 2048 bit (un taglio abbastanza diffuso) per avere una protezione paragonabile a quella offerta da una chiave simmetrica a 103 bit.
- Ma se volete dormire sonni tranquilli allora il consiglio è di utilizzare, dove possibile, una chiave pubblica da 4096 bit.

Cifrari a chiave pubblica

- La teoria dei sistemi a chiave pubblica è stata sviluppata da Whitfield Diffie, Martin Hellman e Merkle.
- Loro intuirono che il sistema a due chiavi avrebbe risolto il problema della distribuzione delle chiavi.
- In più, Diffie e Hellman svilupparono un algoritmo per la distribuzione delle chiavi e per la condivisione di segreti che deve il nome ai due ricercatori (Diffie-Hellman).

Il cifrario RSA

- Ron **R**ivest, Adi **S**hamir e Leonard **A**dleman, nel 1977 idearono l'algoritmo RSA sulla base della teoria Diffie-Hellman-Merkle
- RSA è stata la prima funzione matematica sottoposta a brevetto

  - Alice possiede 2 chiavi, una pubblica e l'altra privata. Lei distribuisce la pubblica su internet.
  - Chiunque può inviarle un messaggio cifrandolo con la chiave pubblica, e solo Alice potrà decifrarlo poiché è l'unica a possedere la chiave privata.

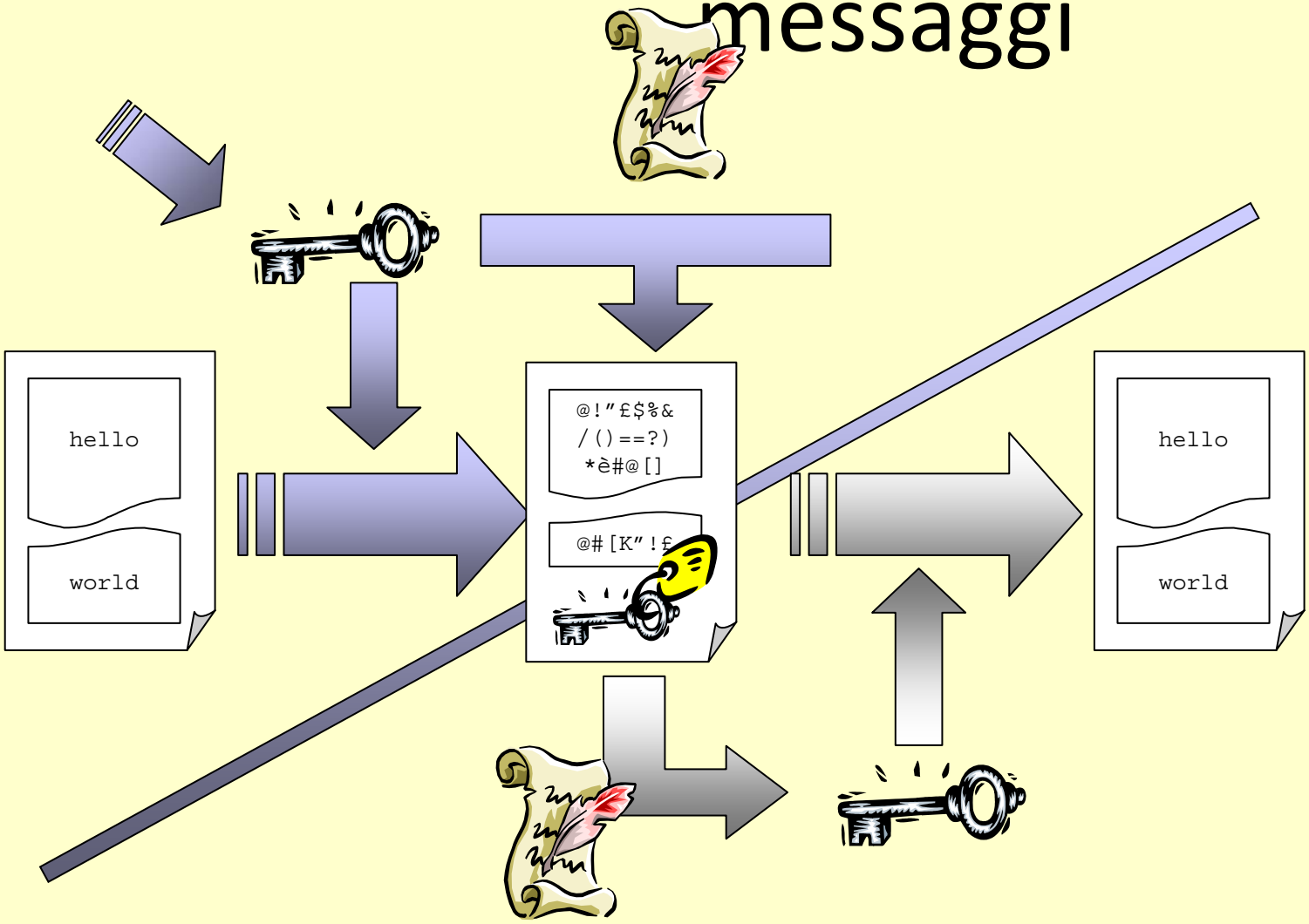
Una combinazione dei due metodi

- In verità il contenuto dei messaggi non è cifrato usando direttamente le chiavi asimmetriche
- Infatti la cifratura asimmetrica è molto inefficiente
- Viene usato un metodo ibrido

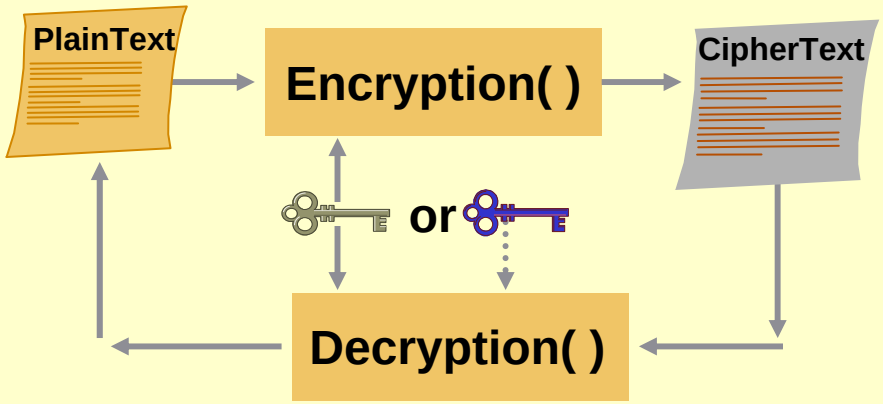
RSA e la comunicazione sicura

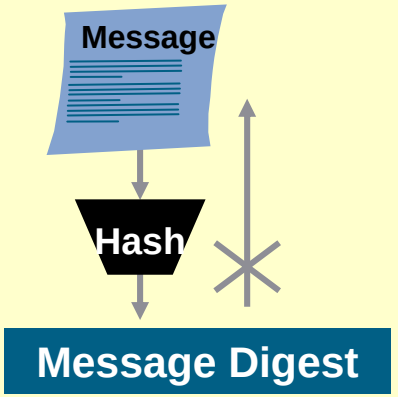
- Alice vuole spedire a Bob un messaggio cifrato:
  - Alice ricava da un elenco pubblico la chiave pubblica di Bob
  - Genera una chiave DES casuale e con quella cifra il messaggio
  - Alice cifra la chiave DES con la chiave pubblica di Bob e gli invia :
    - Testo cifrato + chiave DES cifrata con Kpub
  - Bob decifra con la chiave privata la chiave DES e con questa decifra e legge il messaggio
  - Con il medesimo sistema Bob può rispondere ad Alice
  - **NB: la chiave DES è generata casualmente ogni volta e mai più riutilizzata!!!!**

Cifratura – decifratura messaggi



Encryption vs. Hashing





- Encryption keeps communications private
- Encryption and decryption can use same or different keys
- Achieved by various algorithms, e.g. DES, CAST
- Need key management

- Hash transforms message into fixed-size string
- One-way hash function
- Strongly collision-free hash
- Message digest can be viewed as “digital fingerprint”
- Used for message integrity check and digital certificates
- Hash is generally faster than encryption

Hash

- L'algoritmo di hash elabora qualunque mole di bit (in informatica si dice "digerisce tutto ciò che gli viene dato in pasto"). Si tratta di una famiglia di algoritmi che soddisfa questi requisiti:

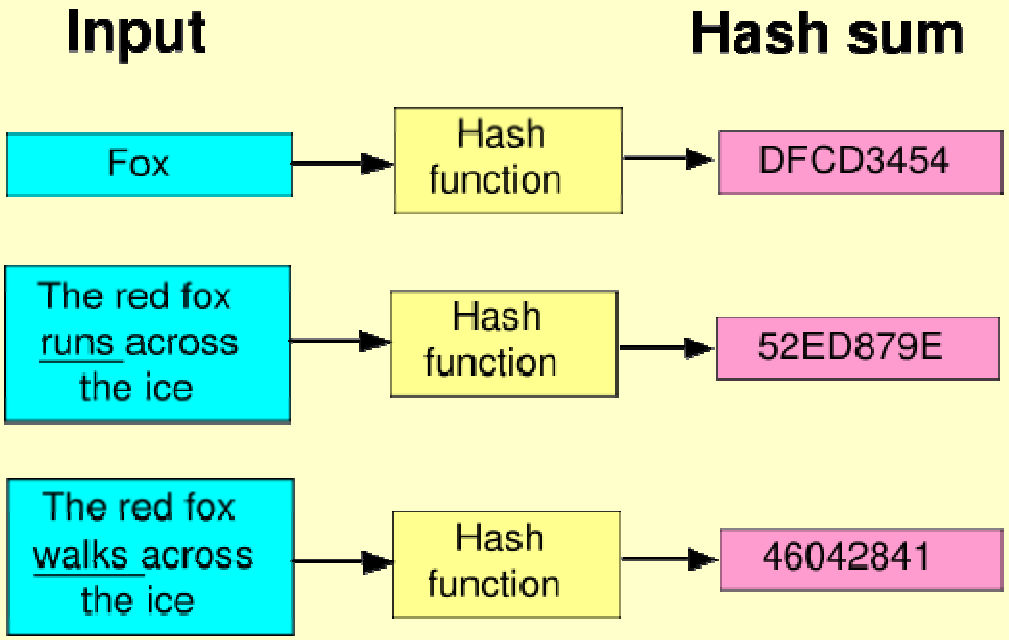
  1) L'algoritmo restituisce una stringa di numeri e lettere a partire da un qualsiasi flusso di bit di qualsiasi dimensione (può essere un file ma anche una stringa). L'output è detto **digest**.

  2) La stringa di output è univoca per ogni documento e ne è un identificatore. Perciò, l'algoritmo è utilizzabile per la firma digitale.

  3) L'algoritmo non è invertibile, ossia non è possibile ricostruire il documento originale a partire dalla stringa che viene restituita in output.

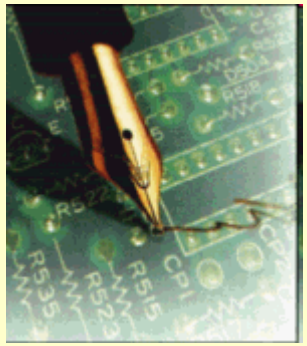
Hash (esempio)

- Un esempio eseguito con l'algoritmo SHA-1 (uno dei tanti disponibili)
- I risultati dell'Hash sono sempre di< lunghezza uguale indipendentemente dalla lunghezza del testo.
- Si noti che il risultato dell'Hash è molto differente anche per piccole variazioni del testo

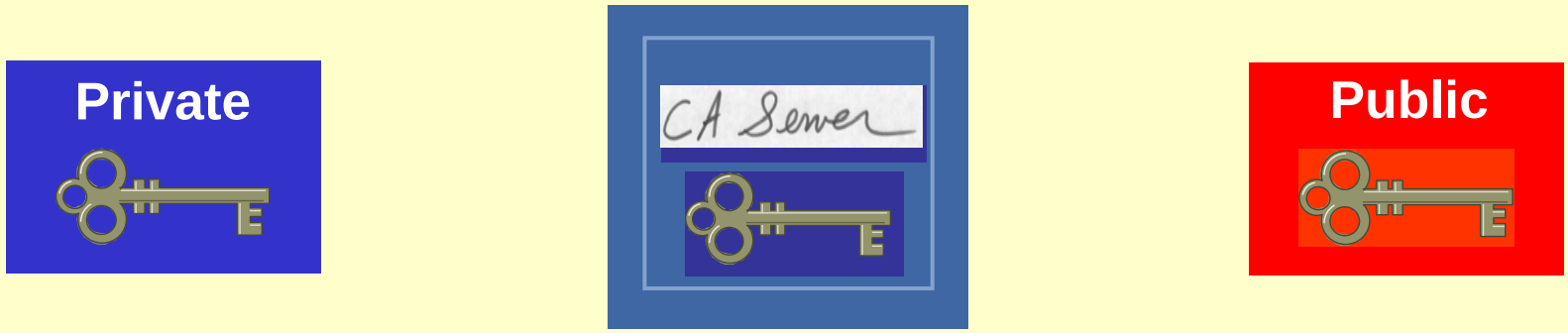


- La figura mostra solamente I primi 4 bytes in forma esadecimale per il risultato delle frasi di esempio (algoritmo SHA-1)

Hashing e Firma digitale



Digital Signatures (Firma digitale)



Entity authentication

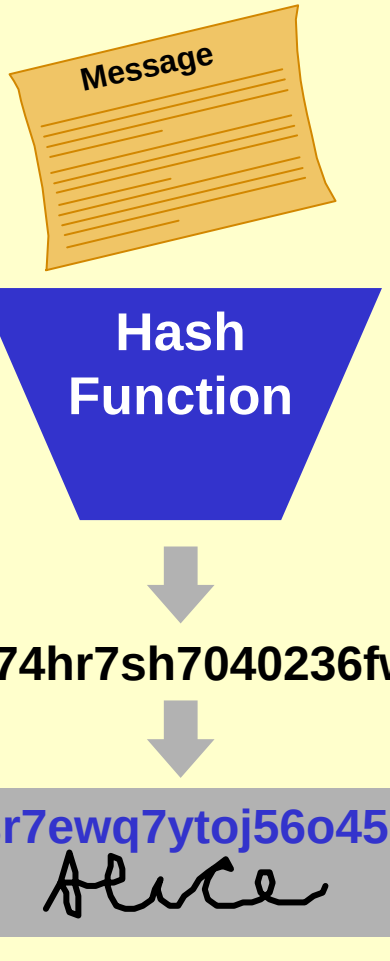
Data origin authentication

Integrity

Non-repudiation

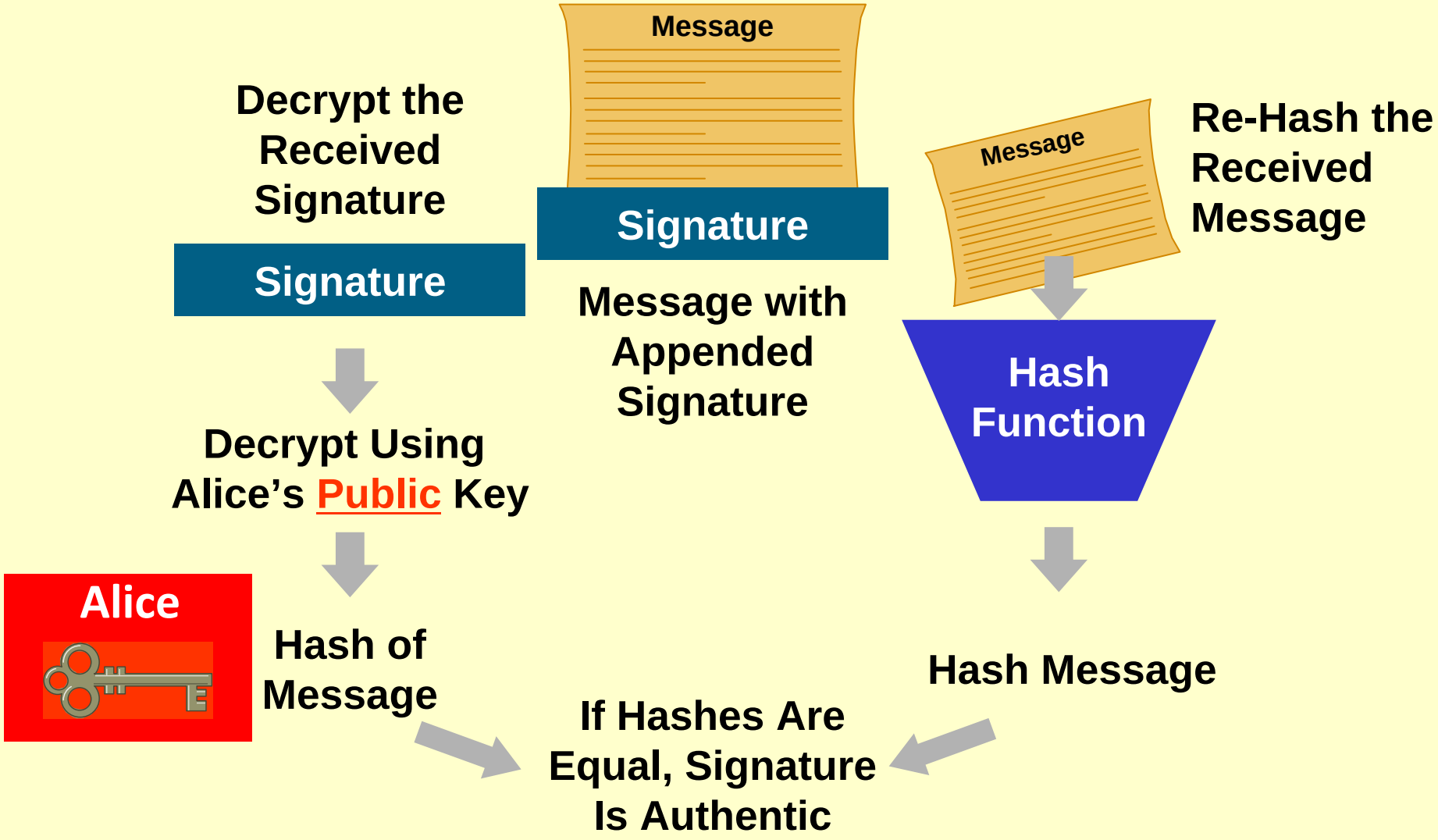
Digital Signatures

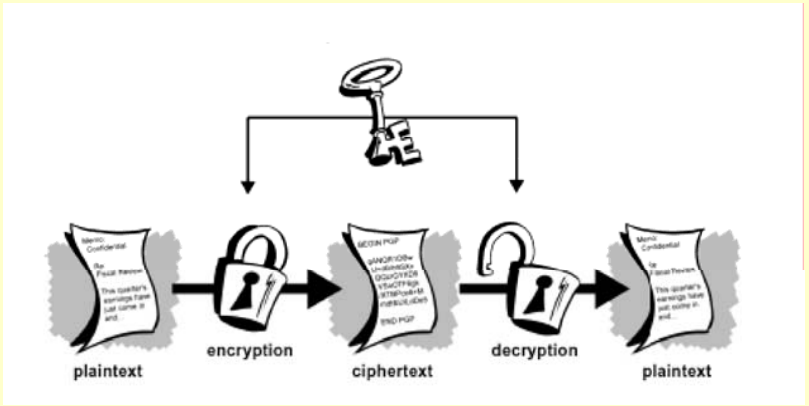
- **One-Way Function;**
- **Easy to Produce Hash from Message,**
- **"Impossible" to Produce Message from Hash**

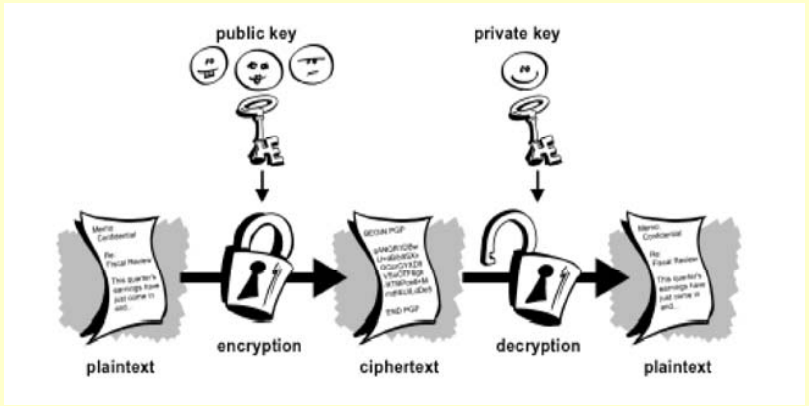


Signature = "Encrypted" Hash of Message

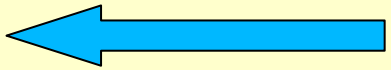
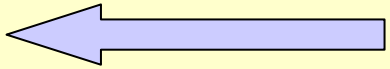
Signature Verification




plaintext
encryption
ciphertext
decryption
plaintext


public key
private key
plaintext
encryption
ciphertext
decryption
plaintext

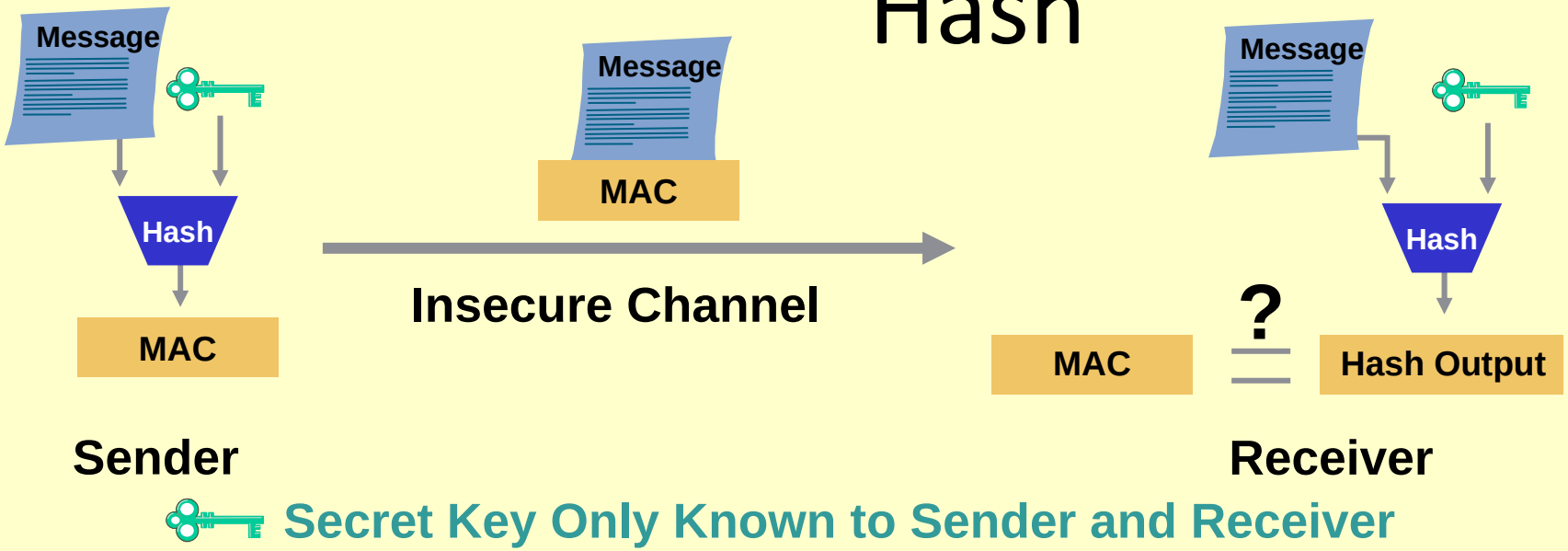
Come la crittografia rende possibili i servizi di sicurezza

- Autenticazione (reciproca) 
- Controllo accessi 
- Confidenzialità (riservatezza)
- Integrità
- Non ripudio

Crittografia asimmetrica e autenticazione

- Per sapere se un documento è stato spedito effettivamente da Alice, lei lo può cifrare con la sua chiave privata:
- tutti coloro che conoscono (o ricavano da un elenco pubblico) la sua chiave pubblica possono decifrare il documento.
- Poiché la chiave privata è in possesso solo di Alice, tutti possono essere sicuri che soltanto Alice può aver spedito il documento.

Message Authentication and Integrity Check Using Hash

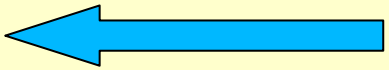


Secret Key Only Known to Sender and Receiver

MAC (Message Authentication Code): cryptographic checksum generated by passing data thru a message authentication algorithm

MAC is often used for message authentication and integrity check

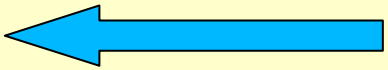
Come la crittografia rende possibili i servizi di sicurezza

- Autenticazione (reciproca)
- Controllo accessi
- Confidenzialità (riservatezza) 
- Integrità
- Non ripudio

Crittografia asimmetrica e Confidenzialità

- Alice deve spedire un documento a Bob in modo che solo lui possa interpretarlo:
- Alice cifra il documento con la chiave pubblica di Bob
- In linea viene spedito il messaggio cifrato che è inintelligibile per chiunque eccetto Bob
- Poiché la chiave privata è in possesso solo di Bob, il messaggio può essere messo in chiaro e interpretato.

Come la crittografia rende possibili i servizi di sicurezza

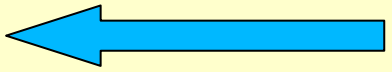
- Autenticazione (reciproca)
- Controllo accessi
- Confidenzialità (riservatezza)
- Integrità 
- Non ripudio

Crittografia asimmetrica e Integrità

- Alice deve rendere pubblico un documento ma vuole che nessuno possa modificarlo
- Alice non cifra il documento poiché questo deve essere letto da chiunque
- Alice produce invece un digest (riassunto) del testo e lo cifra con la sua chiave privata (firma digitale)
- Viene spedito il messaggio in chiaro e il digest cifrato
- Chi riceve il messaggio può produrre lo stesso digest, e lo confronta con quello ricevuto che è messo in chiaro con la chiave pubblica di Alice
- Se i digest sono identici non c'è stata modifica

Come la crittografia rende possibili i servizi di sicurezza

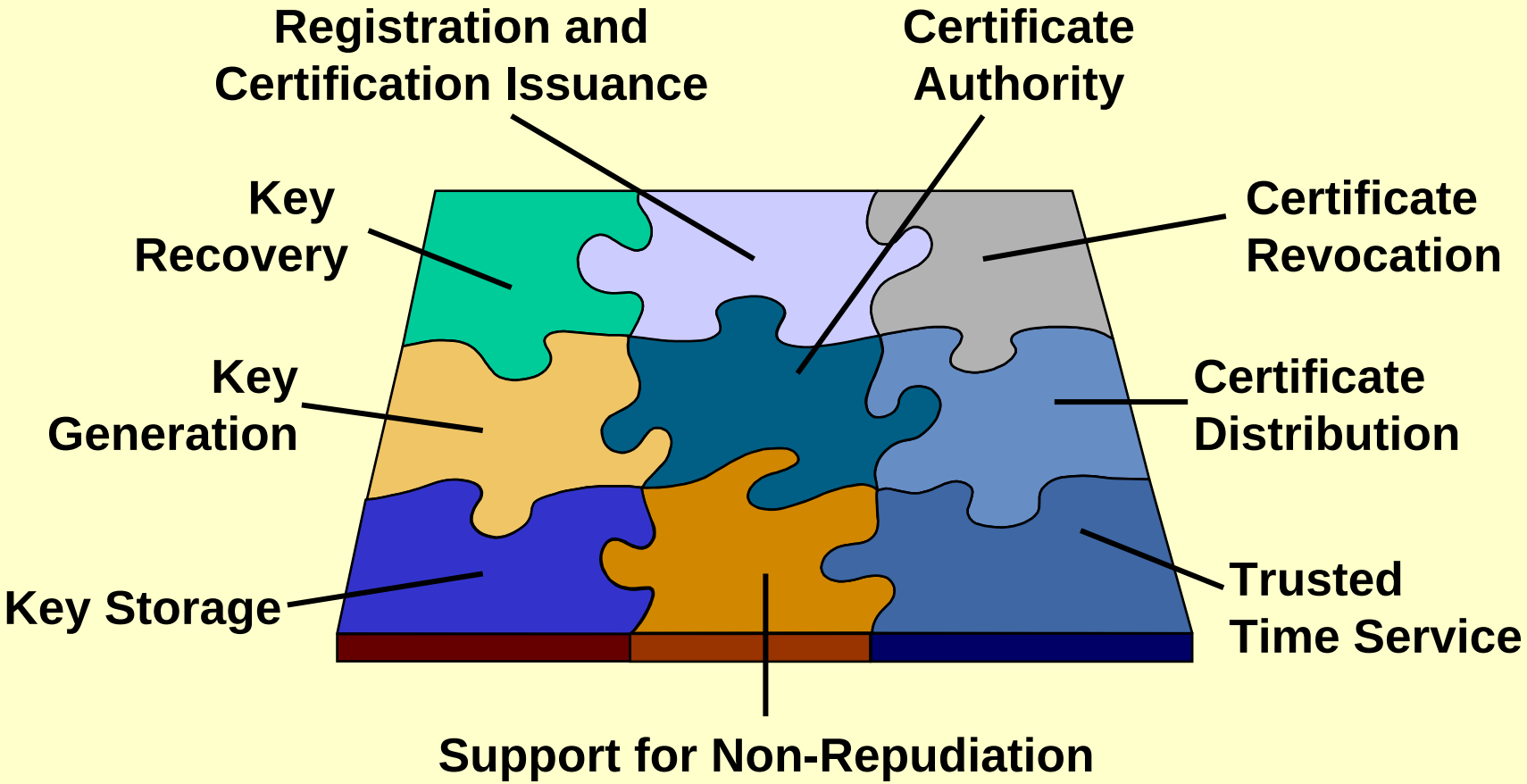
- Autenticazione (reciproca)
- Controllo accessi
- Confidenzialità (riservatezza)
- Integrità
- Non ripudio



Crittografia asimmetrica e Non ripudio

- Alice deve spedire un documento in modo formale e vuole essere sicura che siano certificate la avvenuta spedizione e l'ora di spedizione
- Alice invia il documento ad una entità riconosciuta che esegue il servizio di "notary"
- Il notary firma il documento apponendo il time-stamp della ricezione
- Il notary inoltra il messaggio al destinatario conservandone una copia el proprio archivio pubblico
- Chi riceve il messaggio non può ripudiarne il contenuto e la avvenuta spedizione

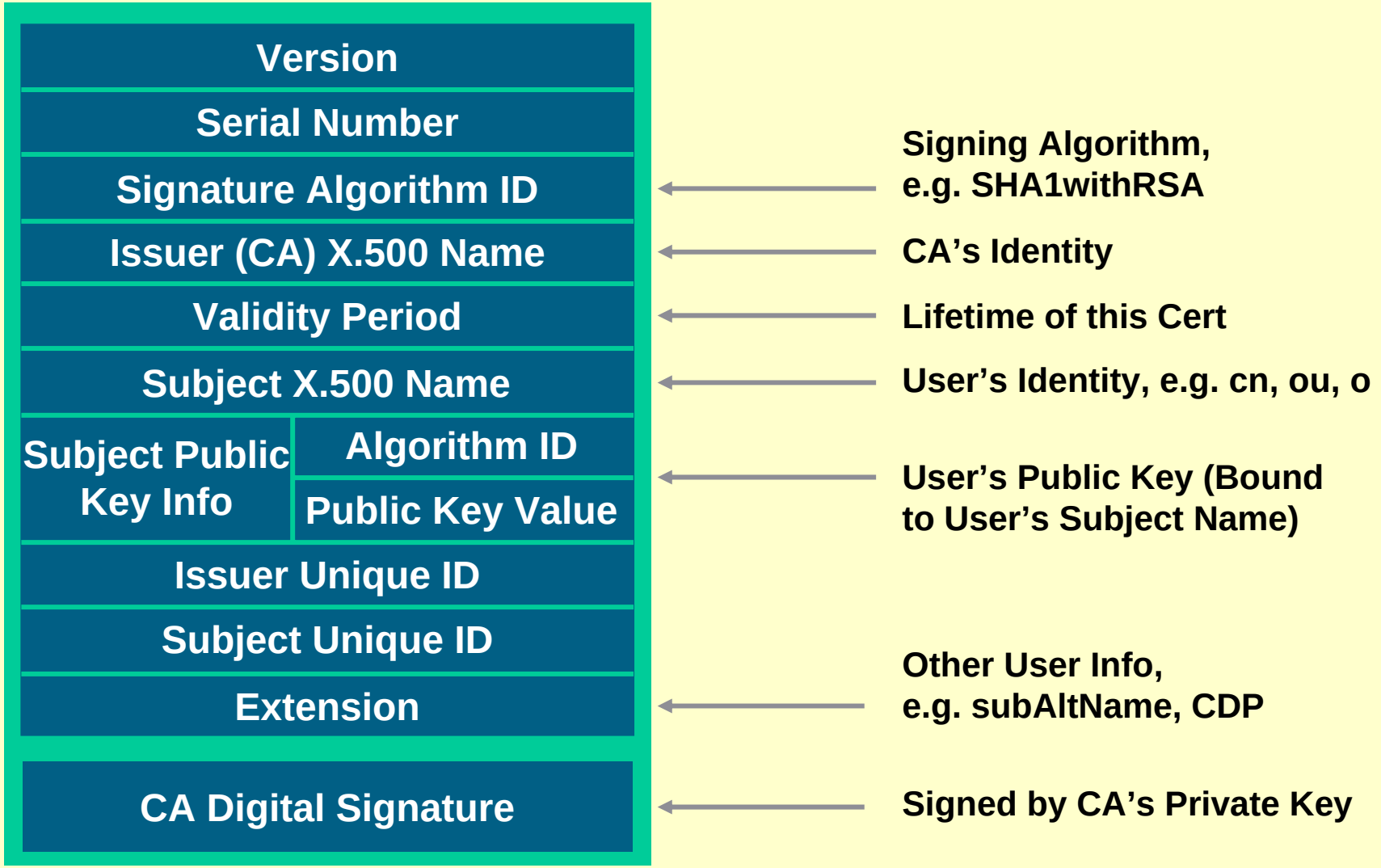
PKI: Authentication Architecture



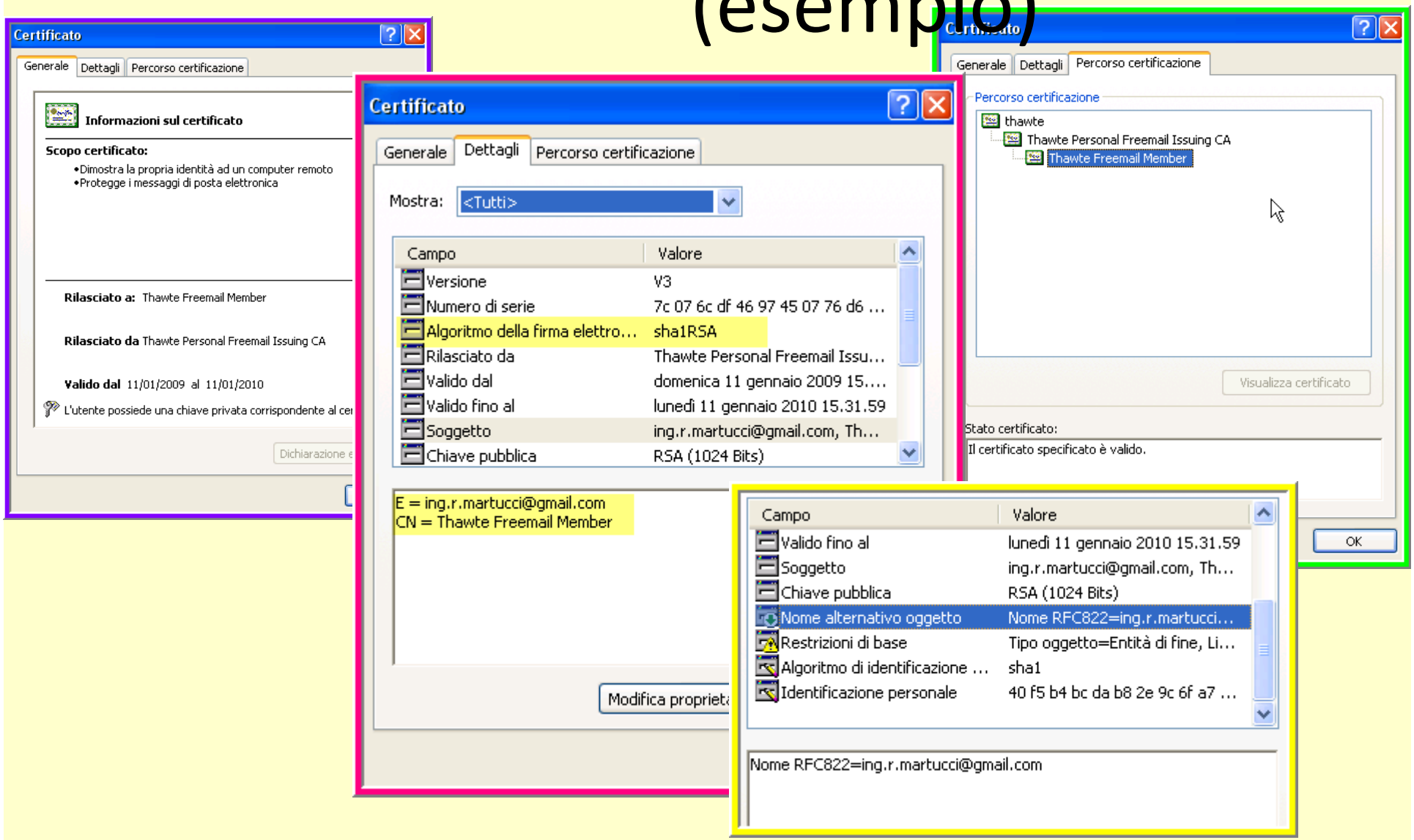
Certification Authority

- È una “terza parte” che garantisce per l’identità dell’utente
- Deve essere riconosciuta come “fidata” da tutte le entità coinvolte nella comunicazione
- La garanzia dell’identità è comprovata da un “CERTIFICATO DIGITALE” associato alla chiave, che contiene i dati identificativi dell’utente e della chiave pubblica, più una serie di campi opzionali
- Il certificato è fornito dalla CA tramite una “procedura di certificazione”
- La CA firma il certificato utente con il proprio certificato
- E’ possibile costruire gerarchie di CA: in tal caso una CA “root” genera e firma il certificato delle sub-CA. Il processo può essere ripetuto per un numero infinito di livelli.

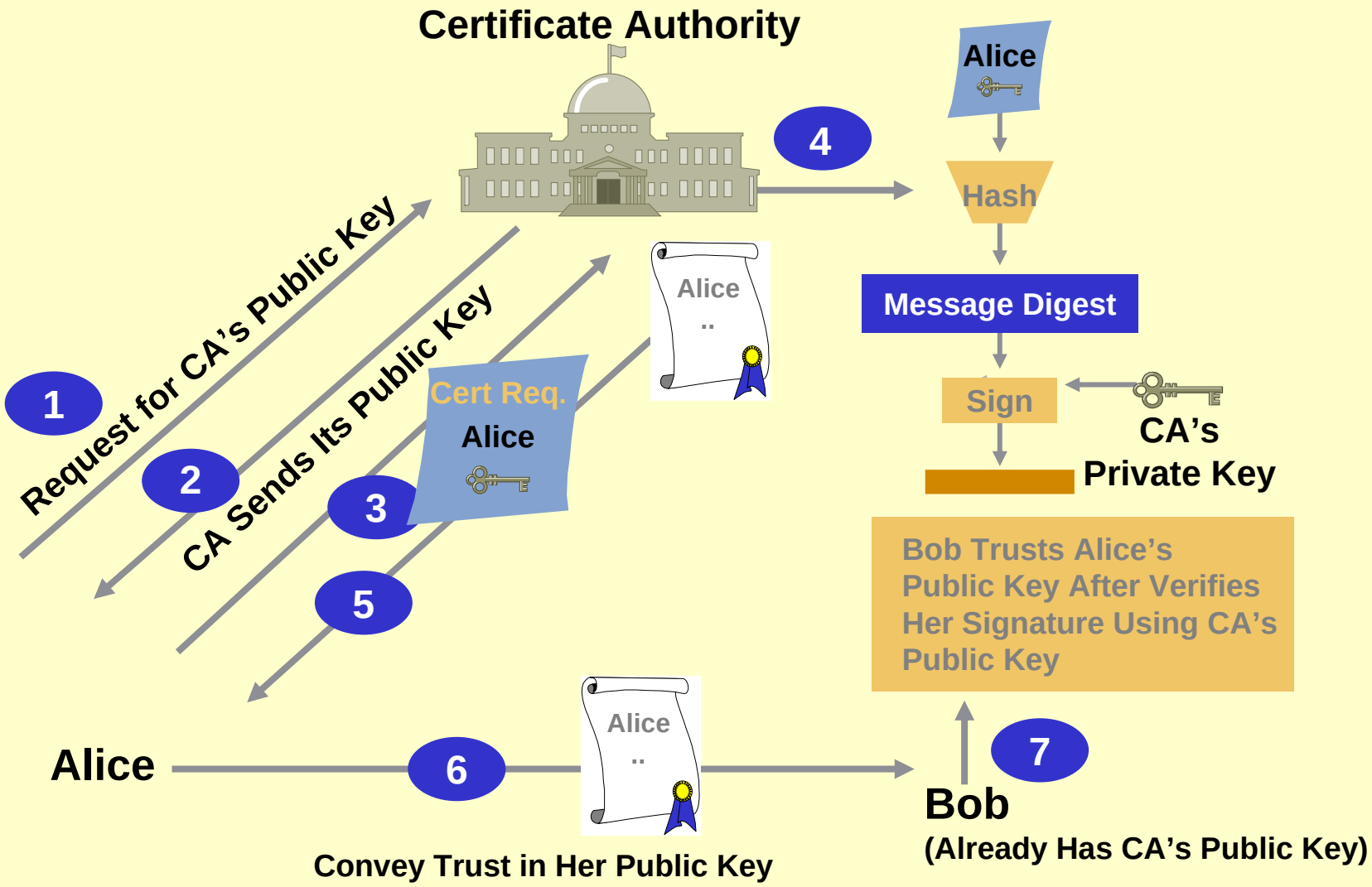
X.509 v3 Certificate



X.509 v3 Certificate (esempio)



Digital Certification



Procedura di Certificazione

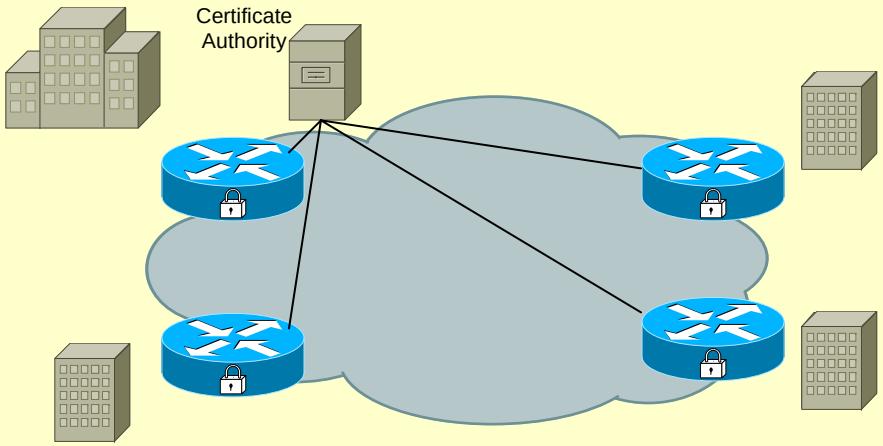
- Alice genera la sua coppia di chiavi
- Raggiunge l'ufficio registrazione (Registration Authority) della CA, si identifica e fornisce la sua chiave pubblica perché sia certificata
- La RA approva la richiesta di certificazione dopo opportune verifiche, dopodiché chiede alla CA di generare un certificato per Alice
- La CA ho un proprio certificato (root CA) *self-signed* con il quale firma il certificato generato per Alice
- Alice riceve per e-mail il proprio certificato firmato dalla CA, ed il certificato root della CA.
- Ogni volta che firmerà un documento, Alice allegherà il proprio certificato digitale oppure il numero seriale dello stesso.
- Il certificato di Alice è pubblicato dalla CA sul proprio "Certificate Server" accessibile tramite protocollo LDAP.

Struttura della PKI

- Certification Authority : è l'Autorità che emette i certificati e le liste di sospensione e revoca. Dispone di un certificato con il quale sono firmati tutti i certificati emessi agli utenti, e quindi deve essere installata su di una macchina sicura (off-line?)
- Registration Authority:presso questa autorità, gli utenti si rivolgono per richiedere la certificazione delle chiavi, identificandosi, e fornendo almeno la chiave pubblica e l'indirizzo e-mail
- Certificate Server : servizio di directory accessibile mediante un "operational protocol", tipicamente LDAP, è essenzialmente una lista di pubblicazione dei certificati e delle liste di certificati revocati e sospesi

PKI Concepts

Overview



- Public Key Infrastructure (PKI) è uno schema di autenticazione che fa capo ad una “ROOT CA” che è ritenuta TRUSTED dagli utenti
- La root CA fornisce I certificati ai suoi utenti, I certificati forniscono la prova di identità dei clienti

PKI Concepts
X.509 Certificates

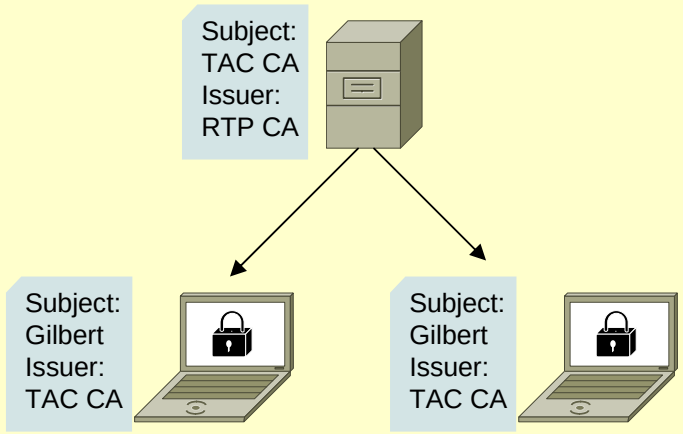
- The passport for network access
- Certificates are issued by the CA server to a person/device and used as a proof of identity
- The certificate is signed by the CA using an encrypted hash
- Can be viewed in Windows by naming the file <name>.cer.
- More details on the certificate format can be found in RFC 2459

PKI Concepts

CA Hierarchy

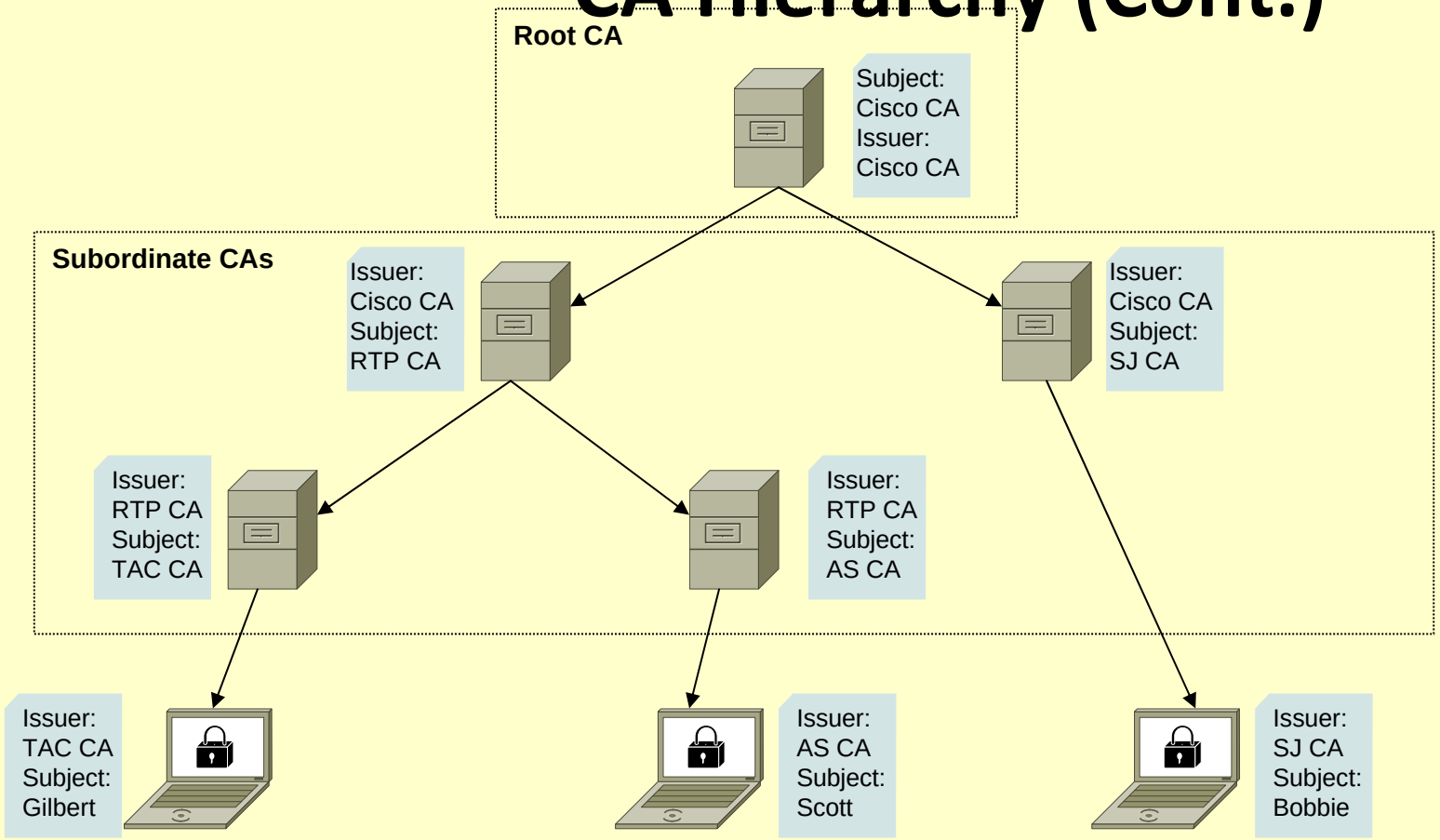
Central vs. Hierarchical Infrastructure

- Central
  - One CA server which issues all of the identity certificates
  - Most common deployment for PKI in a small to medium sized network



PKI Concepts

CA Hierarchy (Cont.)



Hierarchical

A given identity certificate is issued from a CA chain as opposed to a single CA server.

PKI Concepts

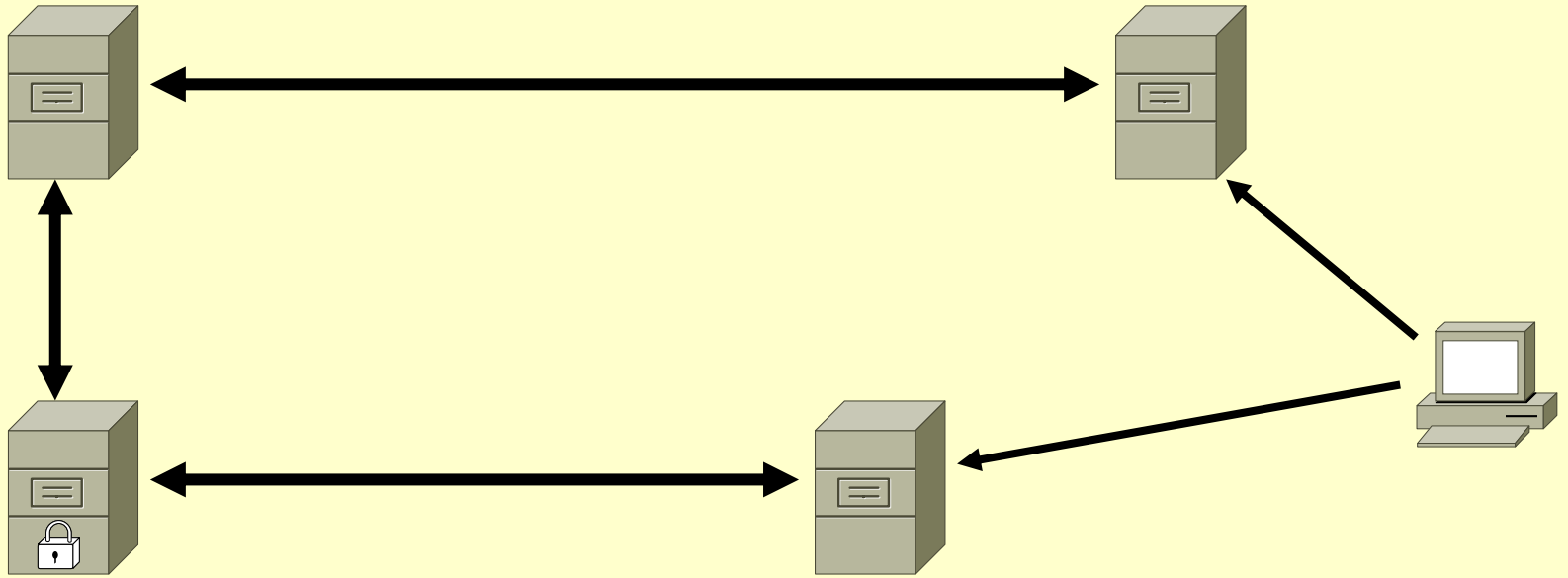
Components

Certificate Authority (CA)

Responsible for signing, issuing and maintaining the certificates

Registration Authority (RA)

Responsible for communicating with clients requesting certificates. Offloads the enrollment process overhead.



Central Repository

Provides a secure storage location for the certificates and CRLs.

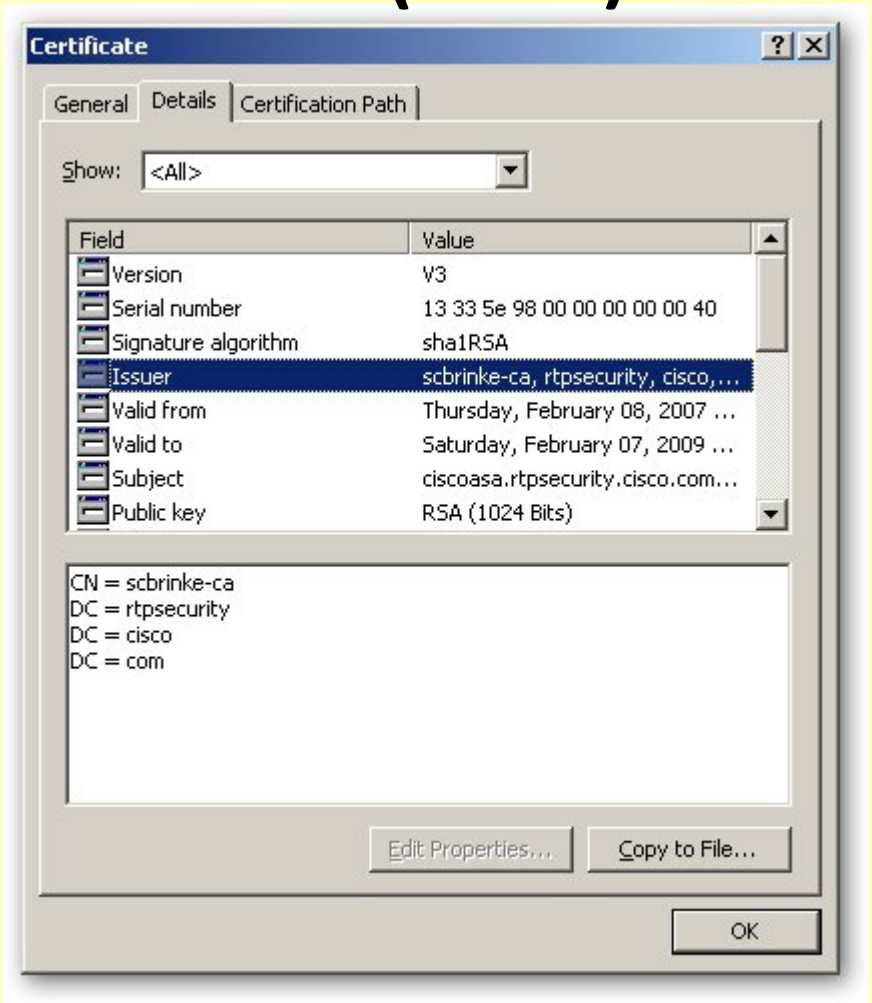
CRL Issuer

OCSP Responder

Note: In many cases these components will be combined into a single server.

PKI Concepts

X.509 Certificates (Cont.)

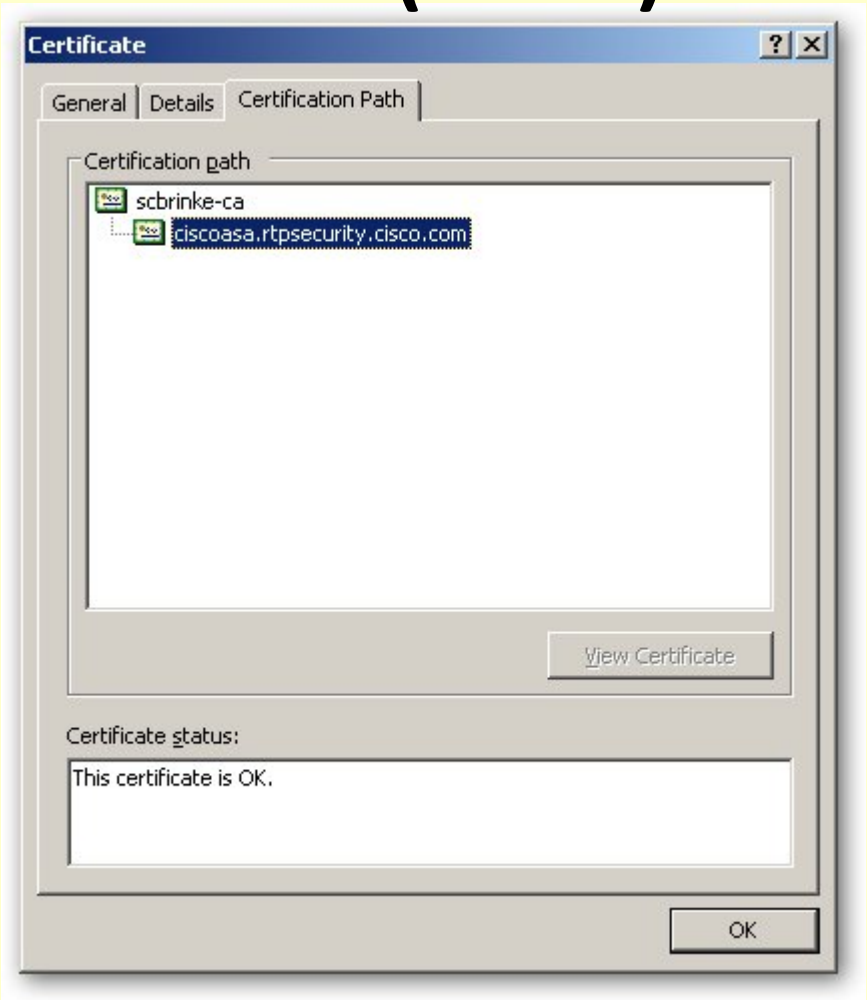


A x.509 identity certificate as viewed from Windows

PKI Concepts

X.509 Certificates (Cont.)

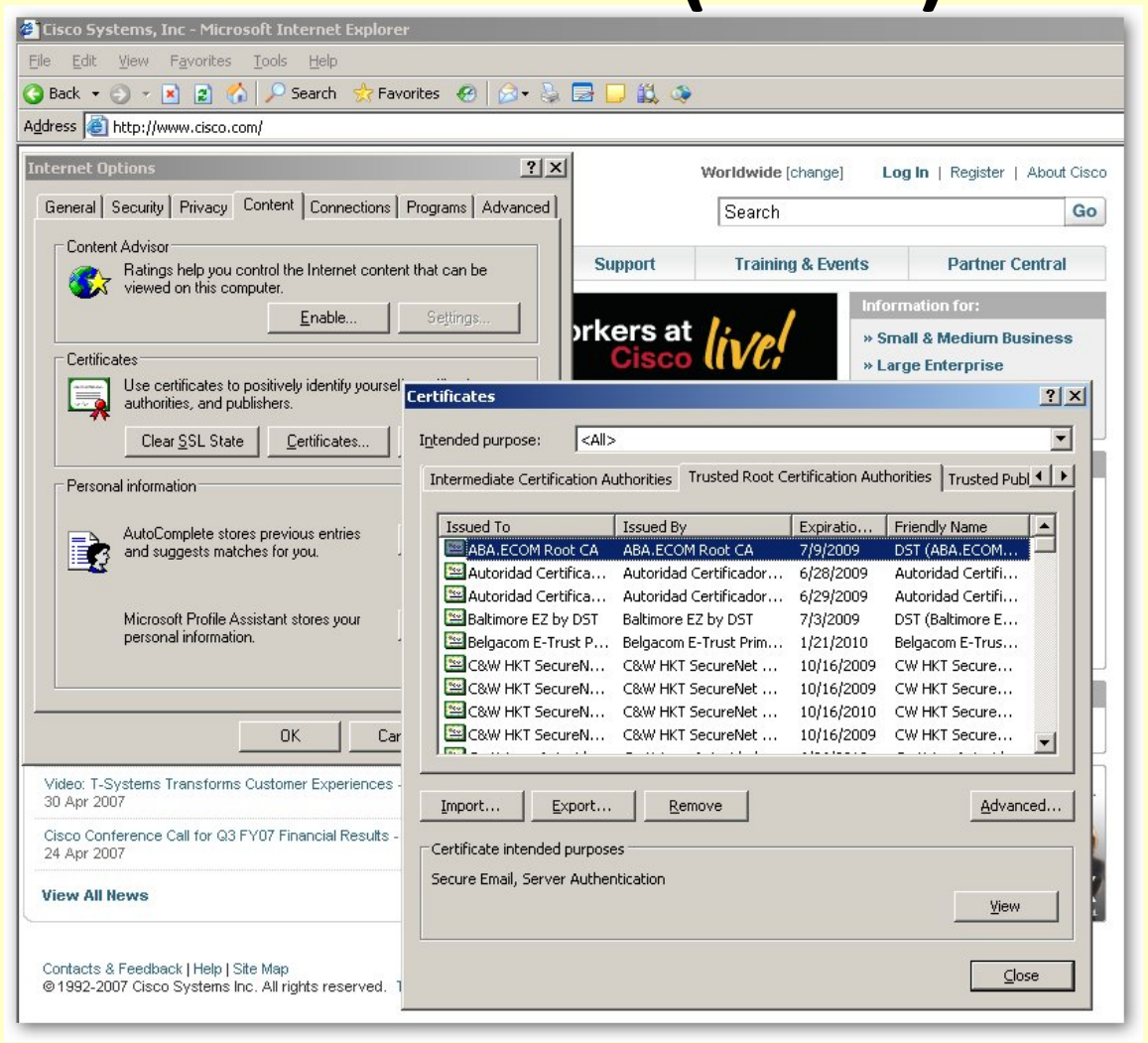
- Windows will try to build the entire certificate chain from the certificates in the local Windows certificate store
- This can be a useful tool when trying to determine which CA certificates are required to install an identity certificate onto a device



PKI Concepts

X.509 Certificates (Cont.)

- Windows by default has a number of trusted CA certificates pre-installed in the local certificate store
- They can be view by going to Tools -> Internet Options -> Content (tab) -> Certificates



PKI Concepts
X.509 Certificate Fields

- **Version:** Current version is 3
- **Serial Number:** Unique number assigned by the issuing CA server
- **Signature Algorithm:** The hash and encryption algorithm used in generating the certificate. (i.e., sha1RSA)
- **Issuer:** DN (Distinguished name) of the CA server which issued the certificate (x.500 format)
- **Validity:** Start and end date for the certificate's lifetime
- **Subject:** DN of the client/host the certificate is being issued to (x.500 format)
- **Subject Public Key Info:** The subject's public key and algorithm used
- **Issuer Unique Identifier** (optional)**:** Used to uniquely identify the issuer if multiple CAs exist with the same issuer DN

PKI Concepts
X.509 Certificate Fields (Cont.)

Subject Unique Identifier (optional)**:** Used to uniquely identify the subject if multiple certificates exist with the same subject DN

Extensions (optional):

- **Key Usage:** States if the certificate's public key is for signing and/or encryption
- **Subject Key Identifier:** Used to identify the certificate owner's key if they hold multiple keys
- **Authority Key Identifier:** Used to identify the issuer's key should it hold multiple keys. This happens when the CA renews its certificate and generates new keys
- **CRL Distribution Point (CDP):** URL to the location of the CRL
- **Authority Information Access (AIA):** URL to the OCSP server
- **Subject Alternative Name (SAN):** Contains a list of additional identities for the subject (ie. E-mail, FQDN, IP address etc.)
- **Enhanced Key Usage (EKU):** Defines the intended purpose of this certificate

PKI Concepts

Reference Slide

X.509 Certificate Fields (Cont.)

Digital Signature: Digitally signed hash of the certificate contents

- Allows an end client holding the Issuer's certificate to verify the contents of a peer's identity certificate and hence validate the peer they are talking too
- The hash, either MD5 or SHA, is computed across all the above mentioned fields and then encrypted with the Issuing CA's private key

PKI Concepts

Exporting/Transporting Certificates

- Certificates are safe to be transported because the private key is not included with the certificate
  - **It is not possible to impersonate a device or person without the private key**
- DER Encoded certificates
  - Binary format
  - Not typically used because they cannot be copied via command line interfaces

PKI Concepts

Exporting/Transporting Certificates (Cont.)

- **PEM Encoded Certificates**
  - Also known as Base64
  - Stored in ASCII format
  - Note: The Begin/End headers are optional, but some devices may require them


```
-----BEGIN CERTIFICATE-----
MIIFBzCCA++gAwIBAgIQV0wRzAlBGqBHLgZ9U8ikC
DANBgkqhkiG9w0BAQUFADBfMRMwEQYKCZImiZPy
LGQBGRYDY29tMRUwEwYKCZImiZPyLGQBGRYFY2l
zY28xGzAZBgoJkiaJk/IsZAEZFgtydHBzZWN1cml0eT
EUMBIGA1UEAxMLc2Nicmlua2UtY2EwHhcNMDYxMj
EyMTk0MDA1WhcNMTExMjEyMTk0ODM2WjBfMRMw
EQYKCZImiZPyLGQBGRYDY29tMRUwEwYKCZImiZP
yLGQBGRYFY2lzY28xGzAZBgoJkiaJk/IsZAEZFgtydH
BzZWN1cml0eTEUMBIGA1UEAxMLc2Nicmlua2UtY2E
wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKA
oIBAQDfNDhN/K873Gd8AKZMozZD3Kl6GDhFD04H80
UcBrdMJ0jcrUzKHvQ/S0dDESZCmMou/IJnnYylE6p8Q
733oMMoUYma4O23VrbA60dpr2I718HqQHyS5YToCZ
Wbc8slbKlJNHBv2mb7+P/lpRJhOILVrzKZBQYaEqS72
+Tb5y53EcttNbhZtv8d0+QUl0oWZoP6OpHk5shBOnN
43Qhxon3j4Q27j+c0A17hCAmLiCKg+hghNb3JXyigyq
7Dh1SCXvbj/UQk3c+y6jnuEvWsCvfUrqZrnRsD7ed8Mj
oB5Mx1iB/CyeQ7qzmwdWdKytjUebZxLSIdAxPXg9dN
X6fxvdd4BEcomIuLKE7qhWpLc2sDrn2hOl/JqDcmu8
R4JDtUpWi5OZtMG77RjkY955QJJzghd4XGPIN0SPHy
hn73wIKv8Q7ro+pypIRWxDycm9qvoaOSfOeq3cwUuJ
vJmBMBcFoMxAAcFlqyJ9io7tjcqet9In6Blo5HuUKY3G
/brQm++/7x2zGoTZaHFkOBWl8DEz0Z+rEBTZ0n6lQGJ
lY9GRqRr1g==
-----END CERTIFICATE-----
```

PKI Concepts
Exporting/Transporting Certificates (Cont.)

PKCS 7

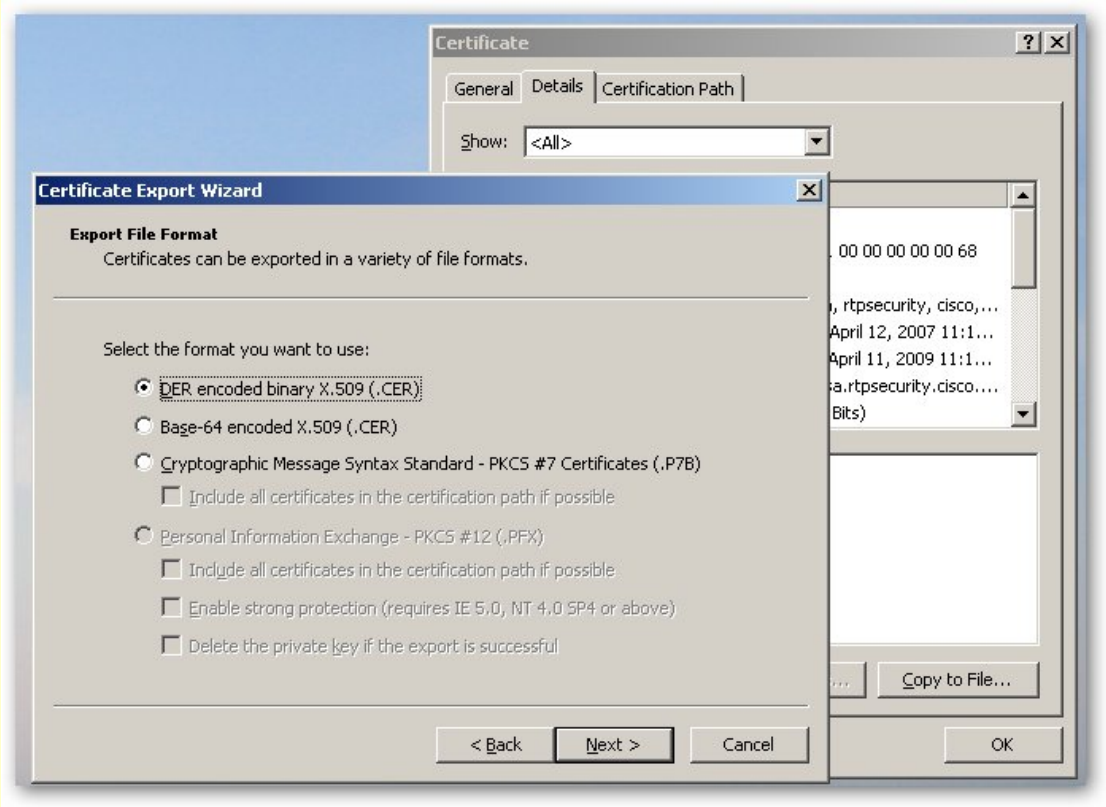
- Provides a means for bundling multiple certificates into a single packet
- Useful for transporting the entire certificate chain

PKCS 12 (.pfx)

- This packages all the certificates in the CA chain including the identity certificate along with the private key
- Encrypted with a password making it safe to transport the private key
- Used for exported and importing trustpoints on both the firewalls and routers

PKI Concepts

Manipulating Certificate



- Certificate conversion can also be accomplished within Windows by opening the certificate and using the copy to file option on the Details tab

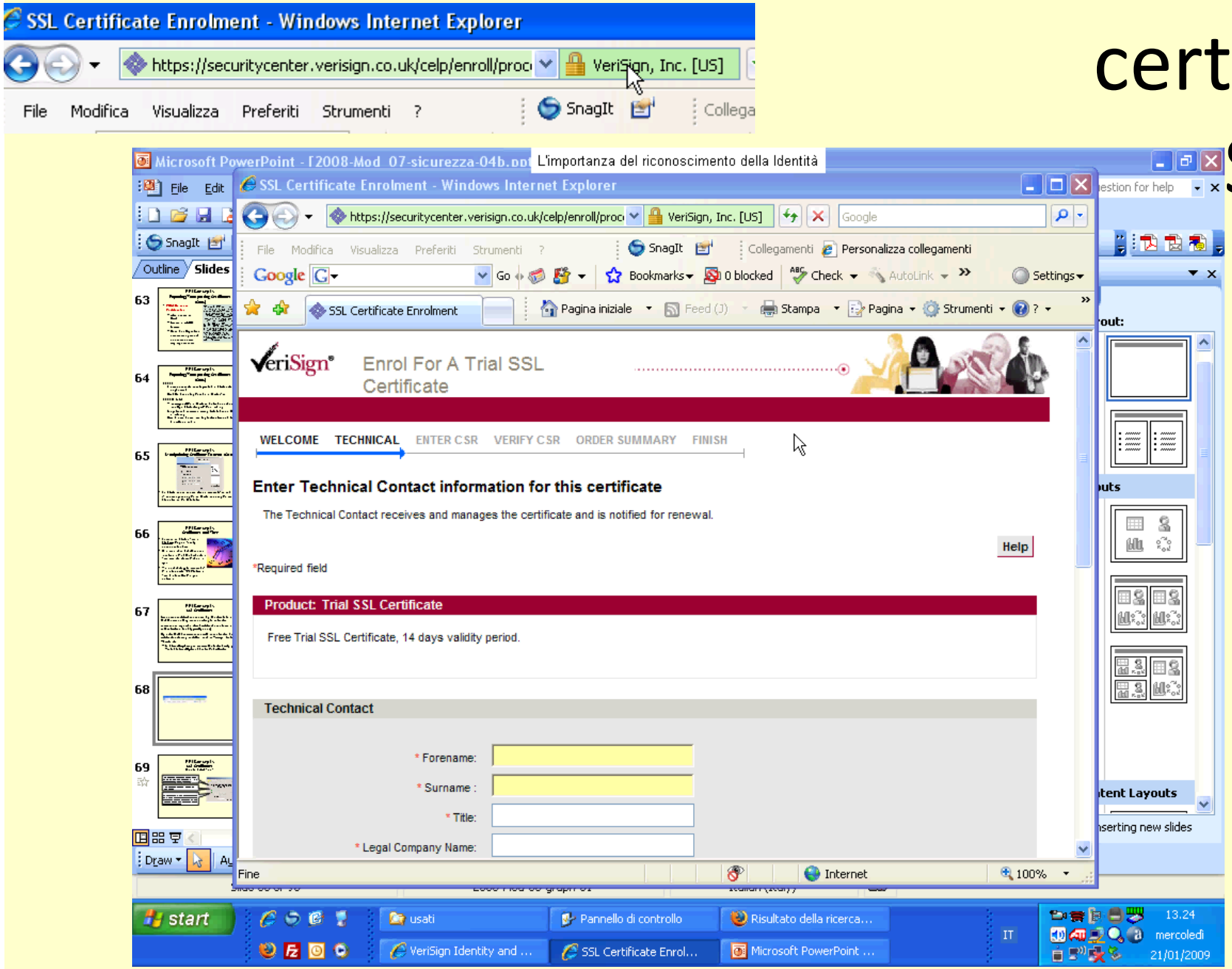
PKI Concepts
Certificates and Time

- Because certificates have a lifetime, they are heavily dependant on time
- It is imperative that all devices involved in the PKI infrastructure have accurate clocks that are in sync
- The best strategy to accomplish this is to enable NTP (Network Time Protocol) within your network

PKI Concepts
SSL Certificates

- Server side certificates are used by the clients to verify that the server they are connecting to is trusted
- A server can request a client certificate as a form of user authentication (not typically done)
- By default all browsers come with some trusted CA certificates already installed, such as Verisign, Entrust, Thawte, etc.
  - In Internet Explorer, you can view the trusted CAs by going to Tools -> Internet Options -> Content -> Certificates

Un certificat SSL



PKI Concepts

SSL Certificates

Should I click Yes?

The certificate was signed by a CA which we do not have a CA certificate for. This is typical with self signed certificates.

The certificate has either expired or is not yet valid.

The hostname or IP address typed into the web browser does not match the certificate. Most browsers will look at the SAN field first. If the SAN doesn't exist, the browser will look at the certificate subject.

Certificate Revocation

Certificate Revocation Checking

What happens if an end users leaves the company, but still has their certificate?

What if a remote router is lost and still has a valid certificate installed?

Certificate Revocation Checking

- Used to invalidate certificates that should no longer be used for authentication
- This is an optional check that can be performed by the authenticator
- A method of revocation checking
  - CRL (Certificate Revocation List)

Certificate Revocation Checking

CRLs (Certificate Revocation Lists)

CRLs are defined in the X.509 RFC and are very similar in format to X.509 certificates

Can be PEM (base-64) or DER encoded

Signed list of revoked serial numbers

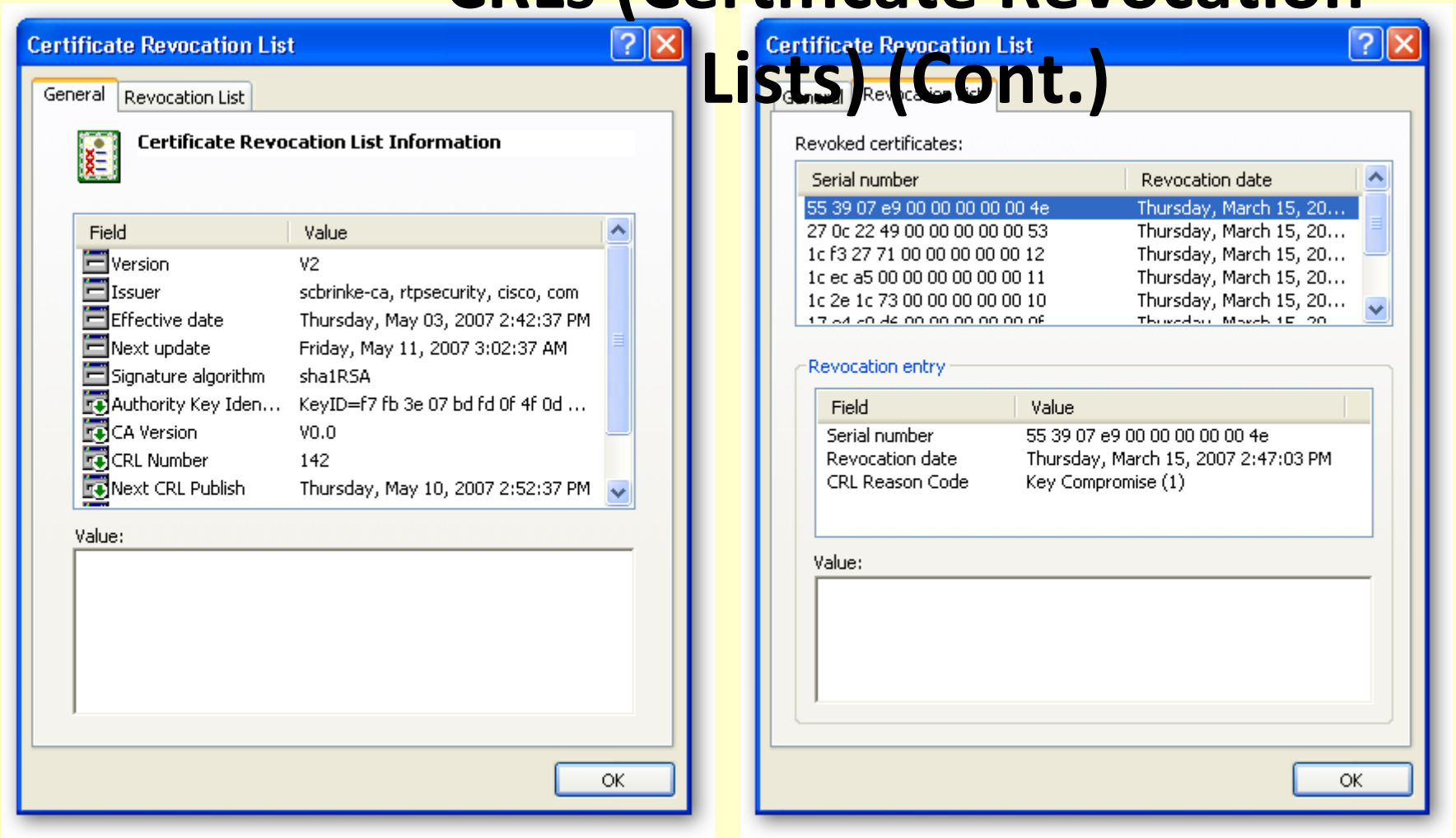
CRLs are published one of three ways

- LDAP
- HTTP
- SCEP

The authenticator determines the CRL location by looking at the CDP (CRL Distribution Point) field of the CA certificate

Certificate Revocation Checking

CRLs (Certificate Revocation Lists) (Cont.)



Certificati sospesi e revocati

La CA si occupa di pubblicare periodicamente due liste sul Certificate Server:

- Certificate Revocation List (CRL)
- Certificate Suspension List (CSL)

CRL: Certificati definitivamente revocati (compromissione chiave privata, smarrimento ecc…) e non più riattivabili

CSL: Certificati sospesi per un certo periodo di tempo. Al termine della sospensione possono essere riattivati, sospesi nuovamente o revocati

Le CRL aderiscono al formato internazionale ITU-T X.509 secondo quanto descritto dallo standard PKIX “Certificate and CRL Profile” (www.ietf.org)

Un riassunto

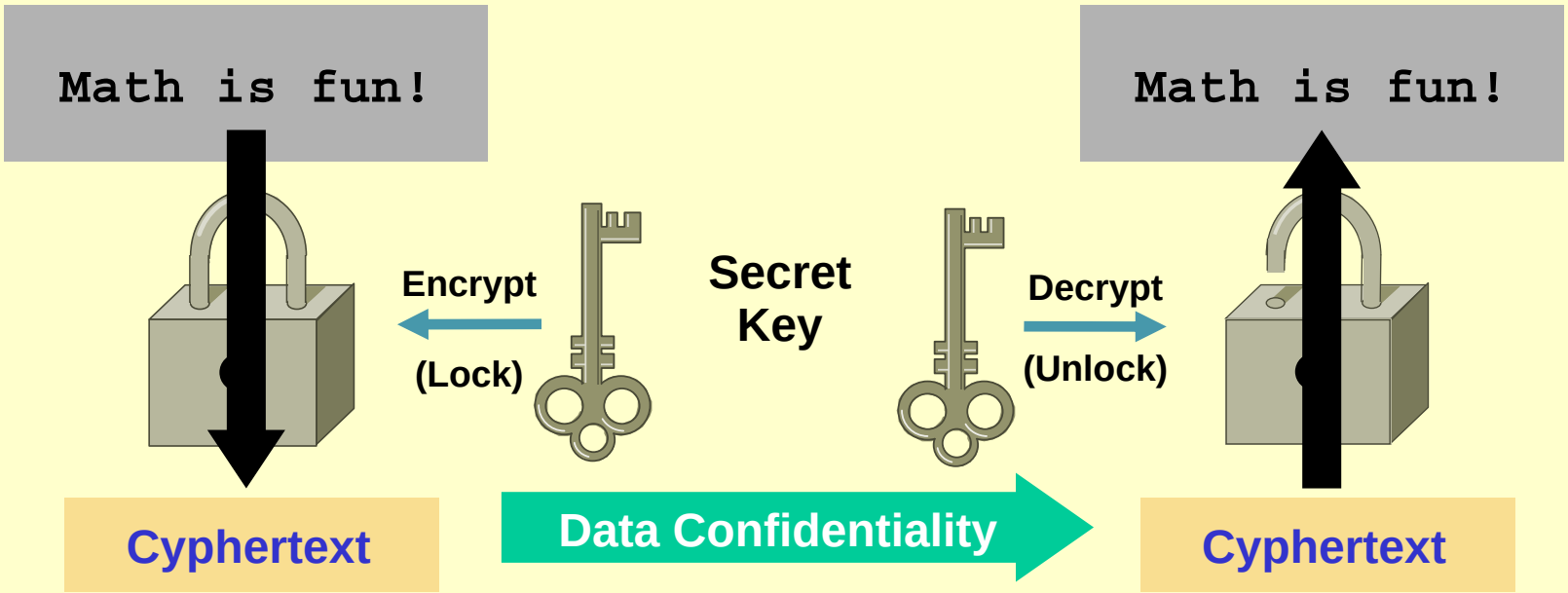
Encryption Fundamentals

Data Encryption Basics

What Is Encryption?

A method of protecting the confidentiality of data

Uses keys to encrypt the data, and decrypt it at



Encryption Fundamentals

Data Encryption Basics

"Key" Issue: The Person You're Communicating With Needs to Have the Key to Decrypt Your Traffic. How Do You Securely Get the Key to the Other Side?

Shared secrets:

- Secret key is carried "out of band" to the remote side
- Easiest mechanism, but has inherent security concerns

Public Key Infrastructure (PKI):

- Uses "asymmetric cryptography" in which the encryption key is different than the decryption key
- Lets you publish the encryption key, while keeping the decryption key secret
- Widely used in e-commerce sites around the world

Encryption Fundamentals

Data Encryption Terminology

Symmetric encryption

Often called “shared key” encryption; the key used to encrypt is the same as the one used to decrypt

Asymmetric encryption

Also called Public/Private Key Cryptography; the key used to encrypt (public) is different than the key used to decrypt (private)

More computationally intensive than symmetric keying

Cryptographic algorithms

The specific algorithm used to transform the data; most common include 3DES and AES (128–256 bit keys); both are symmetric

Hash functions

A “one way only” mathematical function; identical data always produces the same hash output; hashes are often used to guarantee the integrity of data

Common hashes: MD5 and SHA1

Crittografia: un riassunto

Cosa succede se il mittente:

Tipo azione	*Obiettivo principale raggiunto*
Codifica il messaggio con la key_{pub} destinatario	La **riservatezza** del documento in quanto solo il destinatario, che possiede la sua chiave privata può rimetterlo in chiaro.
Codifica il messaggio con la propria key_{pri}	La **autenticità** del documento in quanto il destinatario, accedendo alla chiave pubblica del mittente può rimetterlo in chiaro.
Codifica il messaggio con la key_{pub} destinatario e poi lo firma utilizzando la propria key_{pri}	La **autenticità** e la **riservatezza** del documento in quanto chiunque, accedendo alla chiave pubblica del mittente, può sapere da chi proviene il documento, ma solo il destinatario, può rimetterlo in chiaro.

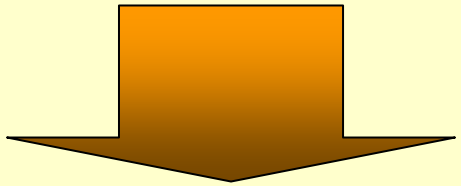
Crittografia: un riassunto

Un nuovo concetto: la funzione di hash o impronta

A partire da una qualsiasi stringa di caratteri (anche documenti molto estesi come libri, lettere o relazioni) restituisce una stringa di valori binari di lunghezza fissa (128 o 160 bit).

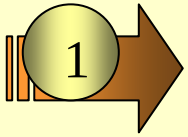
Permette di conseguire i seguenti obiettivi:

- semplicità e velocità dell'algoritmo utilizzato (in genere si basa su un principio di crittografia simmetrica),
- dall'impronta non si può risalire al documento originario,
- la potenziale impossibilità di avere impronte uguali per documenti diversi

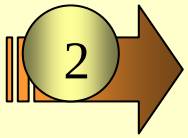


Integrità del messaggio

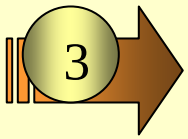
La firma - lato mittente



genera l'impronta ($hash_{mittente}$) del documento (una stringa binaria di lunghezza fissa ed univoca dello stesso. (La legge italiana prevede l'algoritmo SHA-1 a 160 bit che ha una resistenza alle collisioni=10^{48} tentativi),

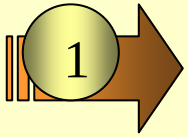


firma il documento, cioè crittografa con la sua chiave privata l'hash del documento,

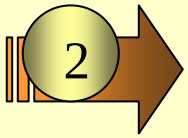


genera l'associazione documento-firma-certificato emesso dalla Certification Authoriry secondo lo standard PKCS#7 dando vita alla "busta elettronica".

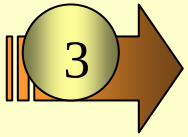
La firma - lato destinatario



apre la busta elettronica,separa il documento in chiaro dalla firma e calcola l'hash del documento (applicando lo stesso algoritmo mittente) ottenendo l'$hash_{destinatario}$



utilizza la chiave pubblica del mittente, estratta dal certificato per ottenere l'$hash_{mittente}$,



confronta $hash_{mittente}$ con $hash_{destinatario}$. Se l'esito è positivo, il messaggio si deve ritenere, integro.

La firma - la CA, le chiavi ed il certificato

La principale differenza tra firma autografa e firma digitale è che la prima è direttamente riconducibile all'identità di colui che firma

- Il DPR 513 introduce il ruolo di Certification Authority (CA) come la terza parte preposta a garantire l'associazione *identità firmatario / chiave pubblica firmatario*

- Le fasi previste per richiedere un certificato sono, in genere, quattro:
  - •prenotazione presso una CA,
  - •riconoscimento fisico del richiedente,
  - •richiesta del certificato,
  - •rilascio del certificato (e del sw di firma).

La firma - la tipologia di chiavi

- Le regole tecniche prevedono tre tipi di chiavi asimmetriche in relazione alle diverse funzioni da attivare od alle diverse responsabilità dell'utilizzatore:

  •**chiavi di sottoscrizione**: destinate alla generazione e verifica delle firme apposte e quindi utilizzate dal titolare privato per firmare i suoi documenti,

  •**chiavi di certificazione**: destinate alla generazione e verifica delle firme apposte ai certificati, alle liste di revoca e a quelle di sospensione e quindi utilizzate dall'ente certificatore,

  •**chiavi di marcatura temporale**: destinate alla generazione e verifiche delle marche temporali, e quindi utilizzate, ancora una volta, dall'ente certificatore che offer il servizio di marcatura temporale.

La firma - il certificato

- I certificati possono essere di quattro tipi:
  - **di sottoscrizione** - usati per la firma dei documenti,
  - **di autenticazione** - per essere riconosciuti su web o per sottoscrivere la posta elettronica,
  - **di crittografia** - utilizzati per la crittografia dei documenti riservati,
  - **di attributo** - per associare a chi firma un particolare ruolo ovvero mandato.

- Le informazioni contenute nel certificato sono:
  - Nome proprietario ed suoi dati anagrafici,
  - Nome CA e suoi dati identificativi,
  - Numero del certificato e sua validità temporale,
  - altri attributi aggiuntivi denominati *estensioni* del certificato.

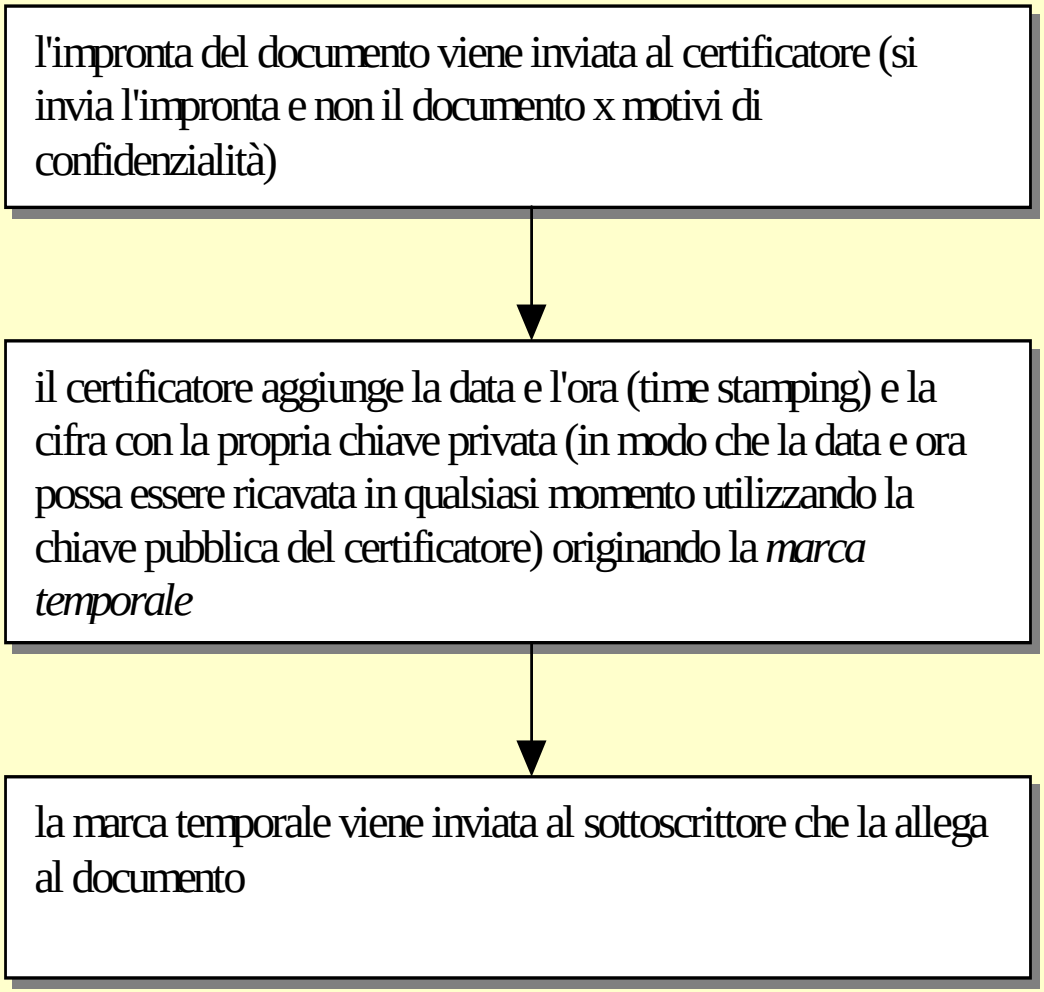
- Tutti i certificati devono essere conformi allo standard X.509 version 3

La firma - la marcatura temporale

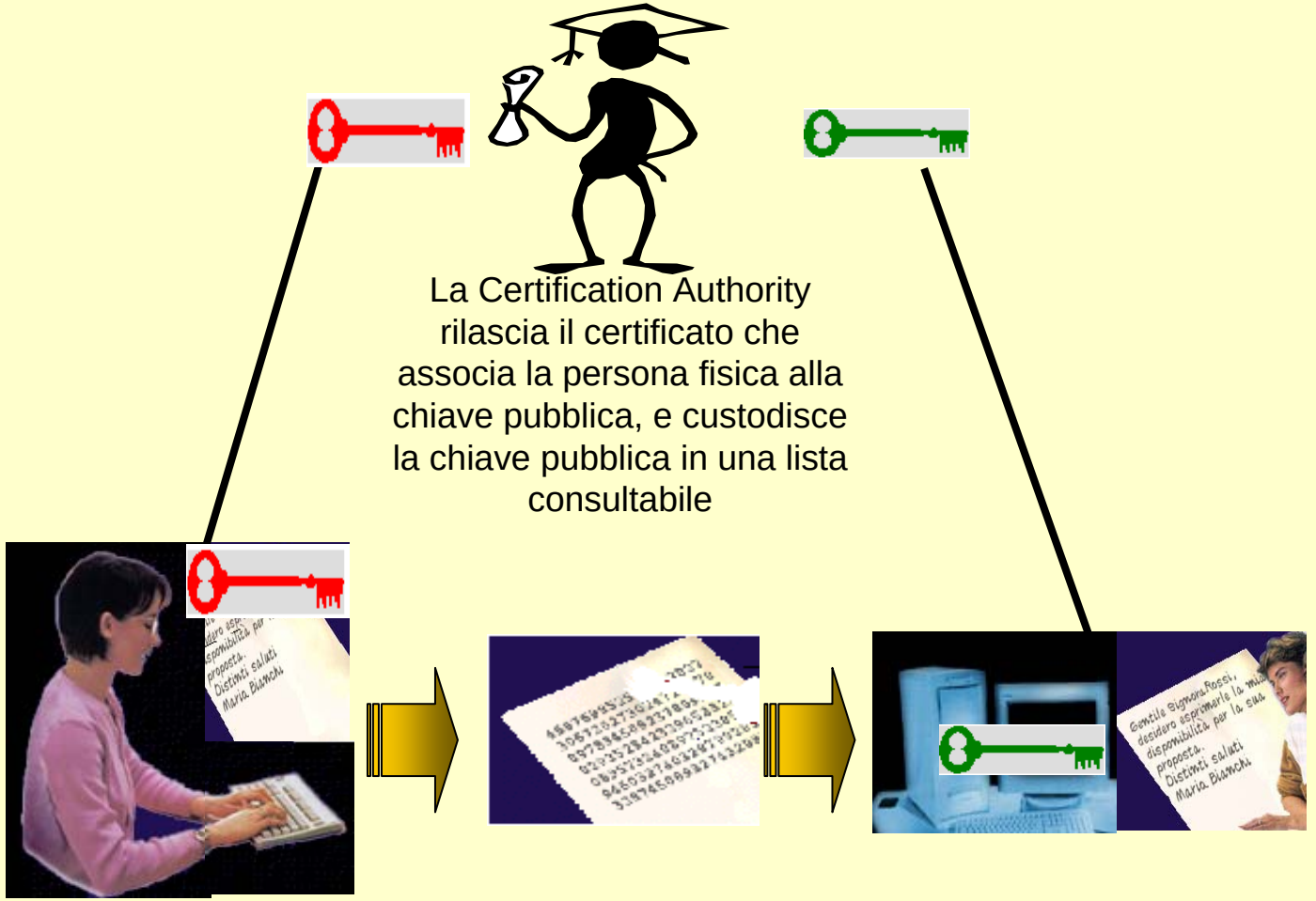
Serve per attribuire ad un documento certezza circa il momento in cui è stato redatto e sottoscritto digitalmente e quindi è divenuto valido e probatorio

- La CA offre il servizi di marcatura temporale
- Le fasi previste per la generazione della marca temporale sono:
  - •l'invio dell'impronta del documento al servizio di marcatura temporale,
  - •il servizio di marcatura temporale aggiunge il timestamp (data e ora), ottenendo l'impronta marcata,
  - •la CA cifra con la sua chiave privata l'impronta marcata ottenendo la marca temporale da cui è possibile recuperare l'informazione del timestamp attraverso l'utilizzo della chiave pubblica del servizio di marcatura,
  - •la marca temporale viene inviata al richiedente il servizio.
- La marca temporale presenta interessanti analogie con il processo di autenticazione e garantisce sia che il documento non venga sostituito da uno diverso da parte dell'autore stesso, sia la collocazione temporale del documento (*timbro postale*).

La firma - la marcatura temporale



Il processo - sintesi

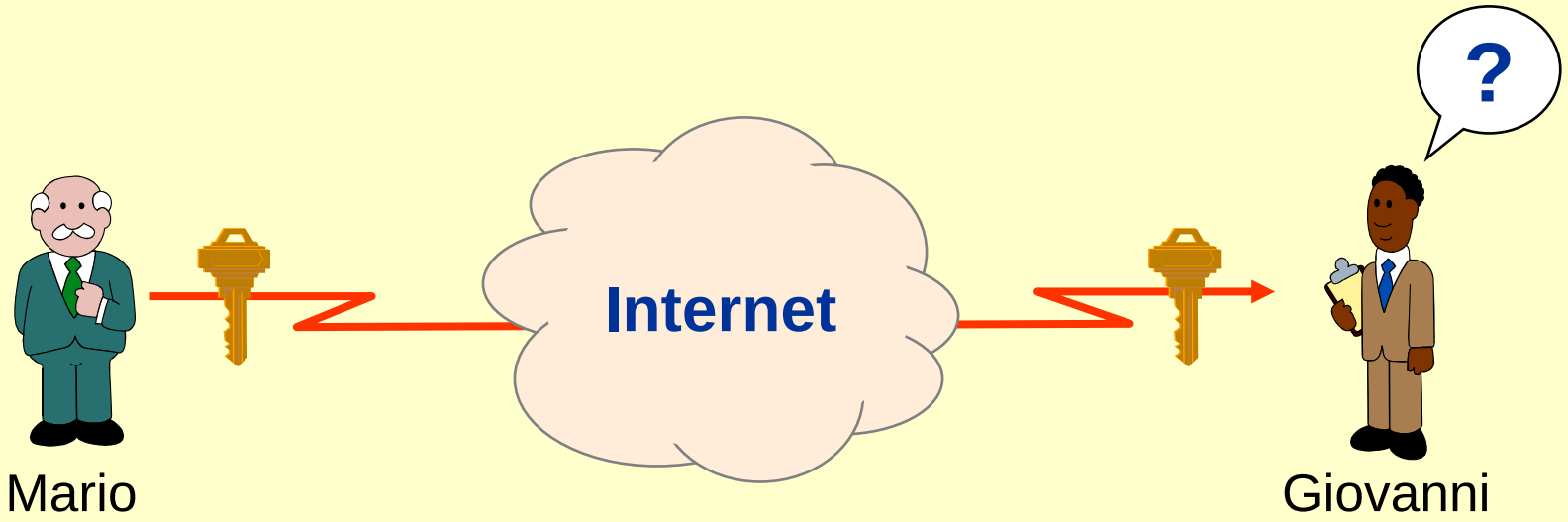


Il mittente firma con la sua chiave privata un documento

Il messaggio firmato, insieme al certificato del mittente rilasciato dalla CA, raggiunge il destinatario

Il destinatario, usando la chiave pubblica del mittente, riesce a determinare l'autenticità dello stesso e l'integrità del messaggio

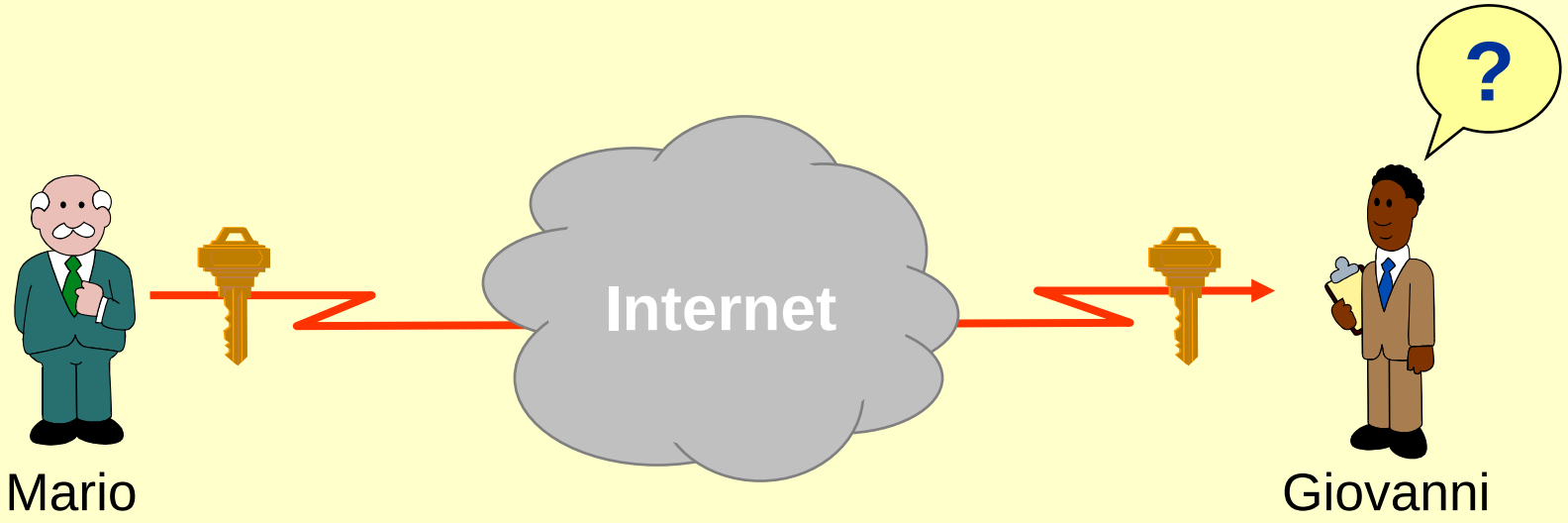
La distribuzione delle chiavi pubbliche



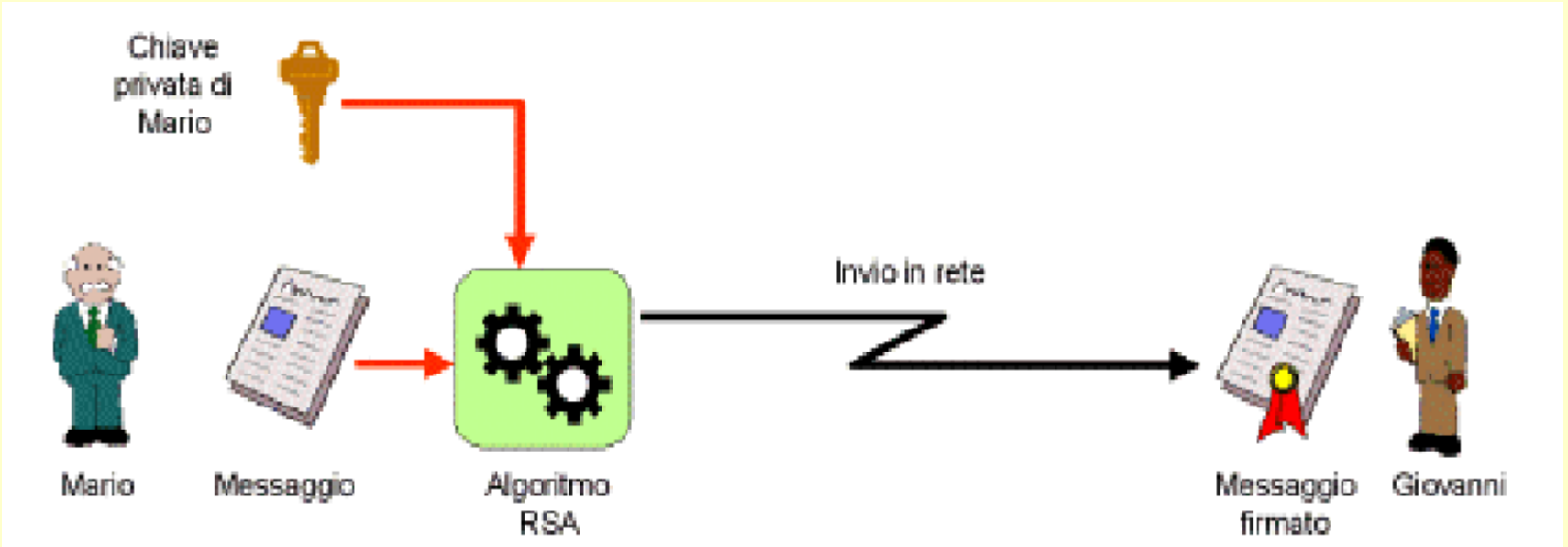
La distribuzione delle chiavi pubbliche

La chiave pubblica di Mario è *davvero* quella di Mario?

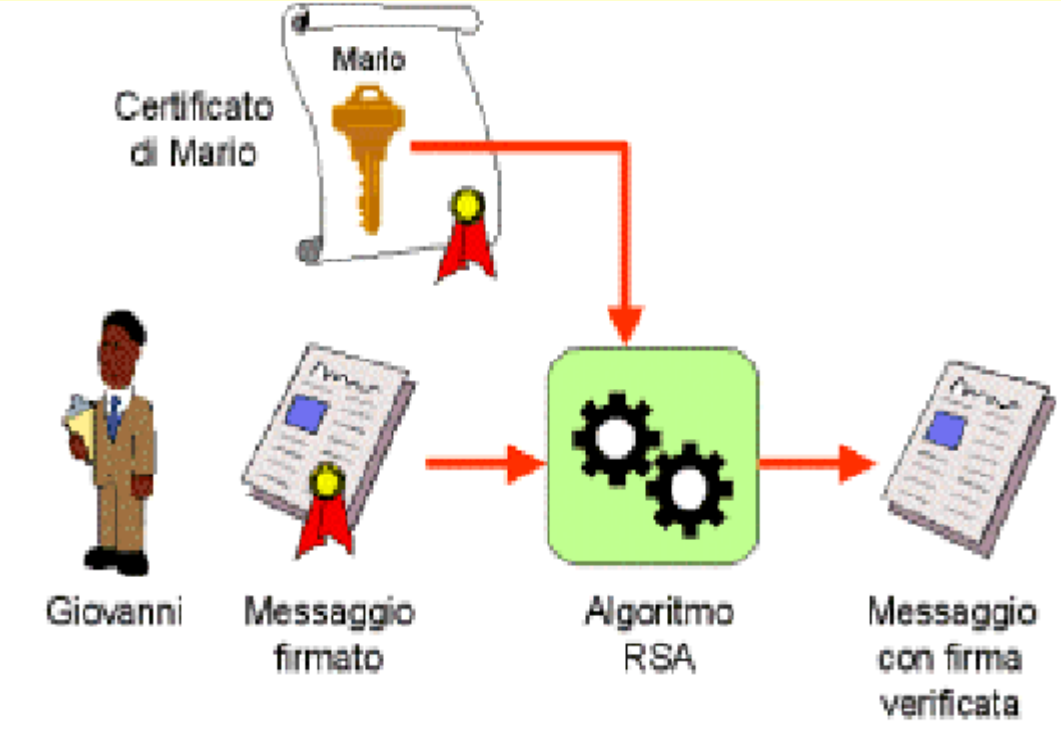
Soluzione odierna: certificati X.509



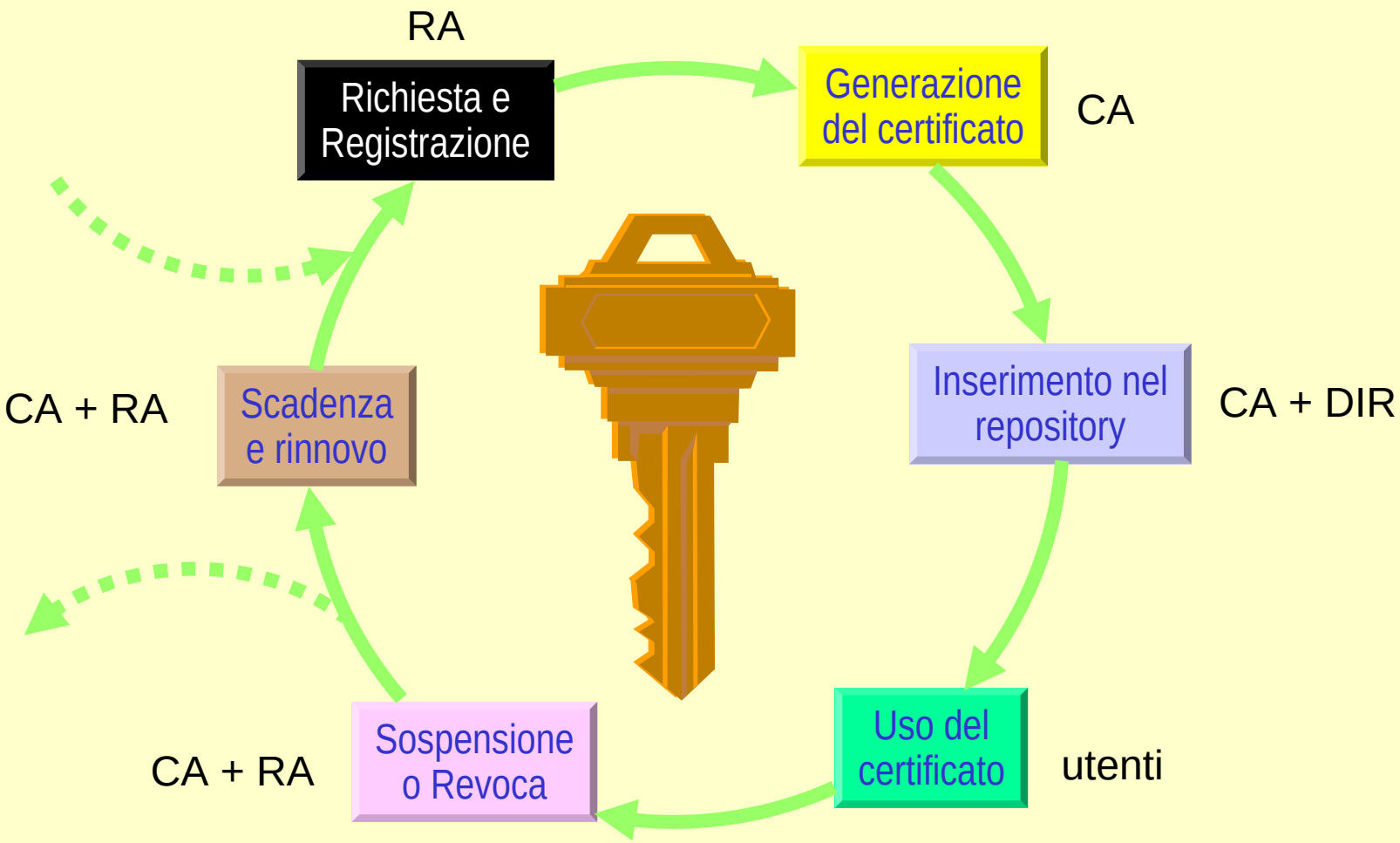
Firma digitale: apposizione



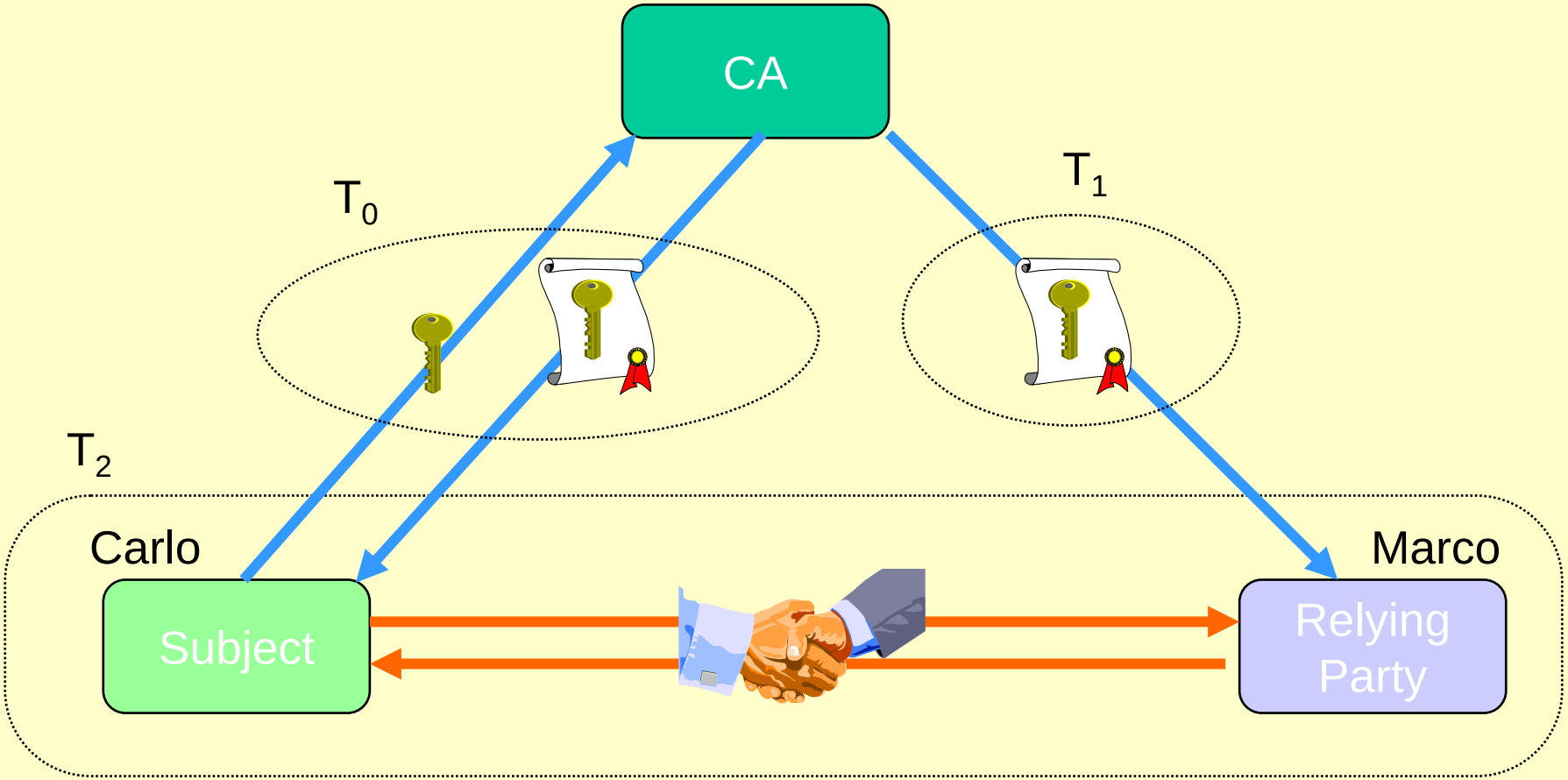
Firma digitale: verifica



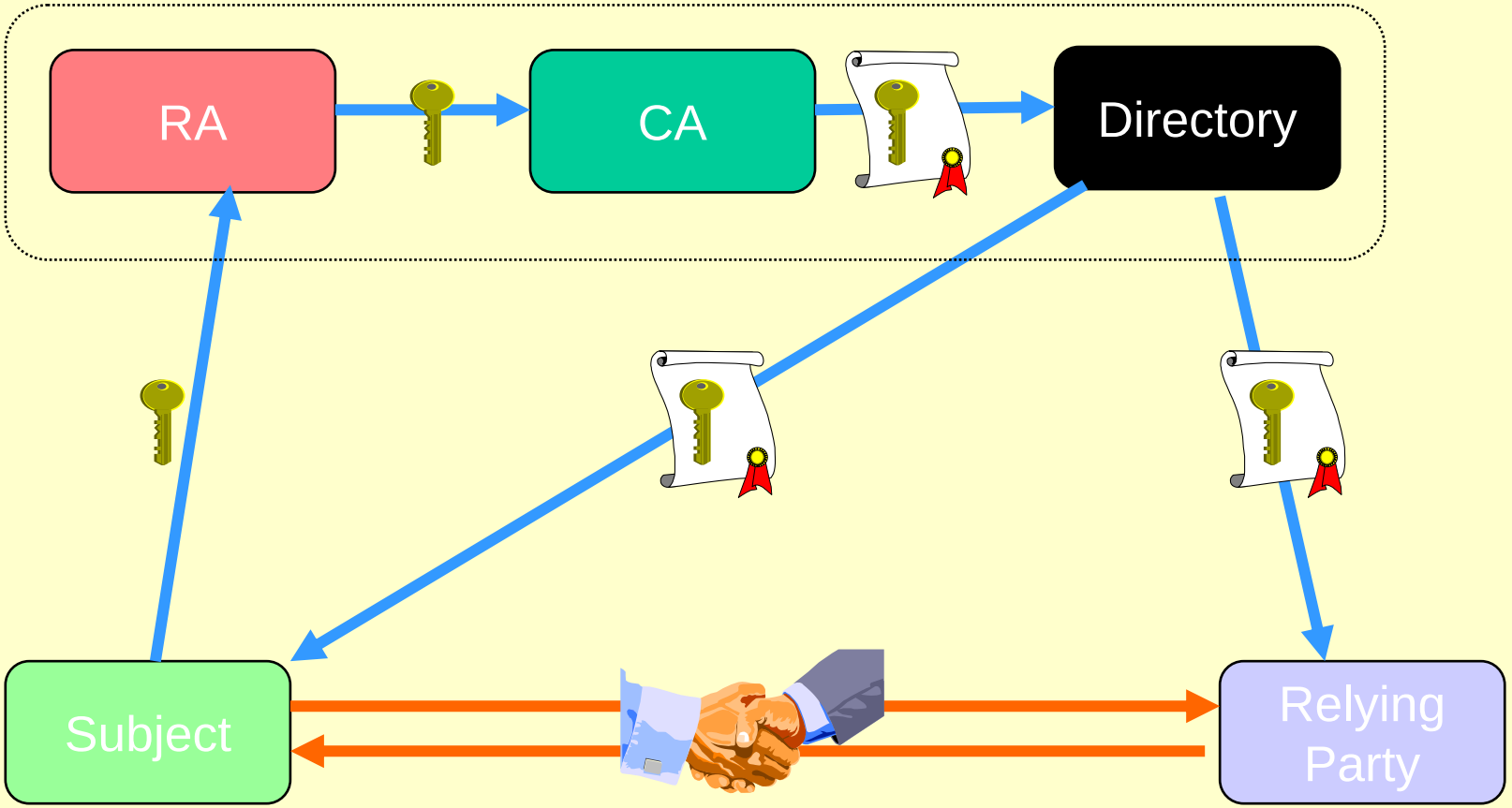
Il ciclo di vita dei certificati



La PKI elementare (una sola CA + utenti)



La PKI elementare (generalizzata)



La PKI gerarchica