I Firewall

Metodi e strumenti per la Sicurezza informatica

Claudio Telmon
claudio@di.unipi.it

Firma digitale e Public Key Infrastructures

Firma elettronica

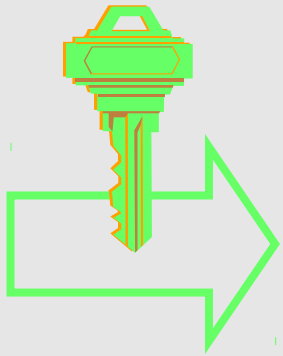
- Dato un messaggio M, se ne calcola il digest d mediante una funzione hash H
- Si sceglie una coppia di chiavi per un algoritmo di crittografia asimmetrico, k_d e k_e, e si rende pubblica k_d.
- $S = E\ k_e(d)$
- Si utilizza k_e per cifrare d. Il risultato è la firma elettronica

Signatures

SIGN A MESSAGE

This is cleartext

Secret key



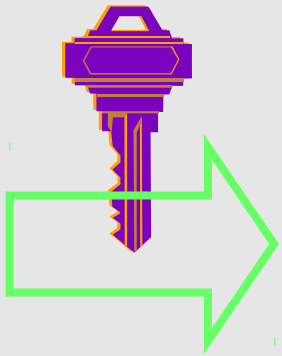
iaxjfhzz

signature

VERIFY A MESSAGE

This is cleartext

Public key



iaxjfhzz

Firma digitale ≠firma autografa

- La firma digitale è legata all'uso della chiave privata
- La firma autografa è legata all'uso della mano

Chiave pubblica?

- Problemi:
  - come distribuire la chiave pubblica?
  - come essere sicuri che una chiave pubblica sia effettivamente associata al mittente del messaggio?
  - Come accertarsi se una chiave pubblica è ancora valida?

Distribuzione delle chiavi

- Scambio di chiavi personale
- Repository
- Verifica in linea

Web of trust (1)

- A conosce B ed è disposto a garantire sulla sua identità; A firma la chiave pubblica di B
- C conosce A e la sua chiave pubblica; C “si fida” di A per quanto riguarda la firma delle chiavi
- C si fida dell’autenticità della chiave di B firmata da A

Web of trust (2)

- Vantaggi:
  - non serve alcun tipo di infrastruttura
  - gli utenti scelgono di chi fidarsi
- Svantaggi:
  - la transitività non è ragionevole oltre due-tre passaggi
  - non è utilizzabile per contatti con entità con le quali non si hanno “conoscenze comuni”
  - responsabilità? (non sono parte del meccanismo)

Legare la chiave alla persona

- Le Certification Authority sono delle “Terze parti fidate” che garantiscono l’associazione fra un’entità e una coppia di chiavi
- Generano un certificato, cioè un documento firmato contenente:
  - un’identificazione dell’entità certificata
  - la chiave pubblica dell’entità
  - un periodo di validità
- È un Web of trust a due soli livelli

Certification Authority (1)

- Viene scelta un'entità della quale "tutti si fidano": la Certification Authority (CA)
- La CA ha il compito di assicurarsi dell'identità degli utenti e di firmarne le chiavi pubbliche (certificati)
- Per gli utenti è necessario conoscere solo la chiave pubblica della CA

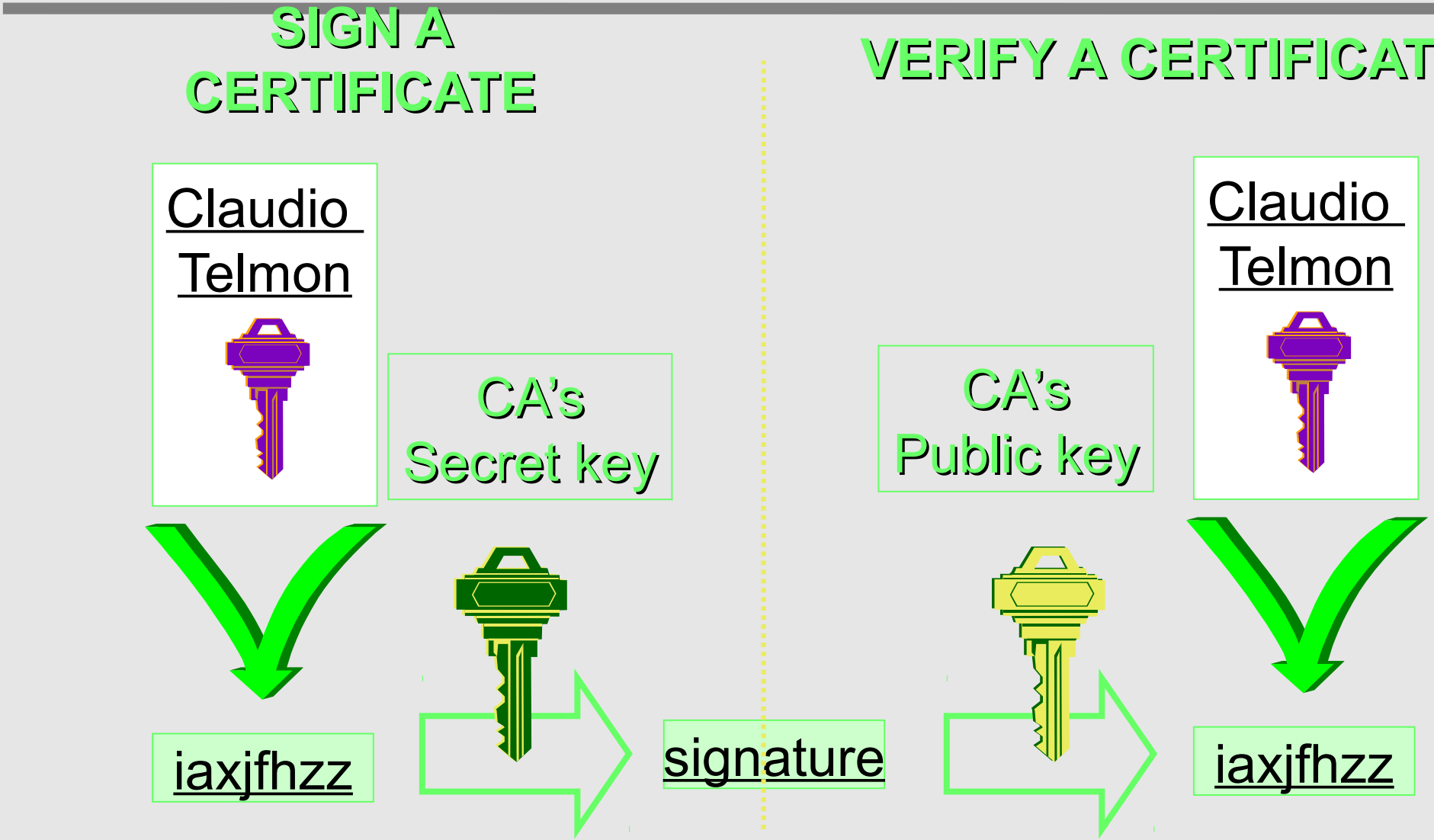
Certification Authority (2)

- Vantaggi:
  - è possibile contattare entità sconosciute;
  - è chiaro in chi si ha fiducia
  - la gestione è più semplice
- Svantaggi
  - ci si deve fidare di chi si fidano gli altri
  - serve un'infrastruttura per distribuire i certificati

I certificati

- Associano un'identità (un server, una persona) a una chiave pubblica
- Sono firmati da una CA
- Contengono i dati necessari per rendere unica l'identità
- Contengono opzionalmente altri dati:
  - un periodo di validità
  - l'associazione fra l'identità e un'entità reale
  - …

Certificates



Cosa garantisce la CA?

- La CA può garantire che un'entità è la legittima proprietaria di una chiave
- La CA non può garantire che la chiave
  - non venga consegnata anche a un'altra persona
  - non venga "rubata"da un'altra persona
  - non venga usata da un'altra persona

Revoca dei certificati

- Problema:
  - le chiavi private possono essere compromesse
  - entità possono cambiare caratteristiche (es. licenziamenti)
  - non è possibile prevedere questi eventi all'atto della creazione del certificato
- Che ne è di un certificato associato a una coppia identità/chiave non più valida?

Revoca dei certificati

- Se una chiave privata di utente o di CA è compromessa, viene revocata e il certificato è inserito in una Certificate Revocation List…
- …solo quando la compromissione è scoperta

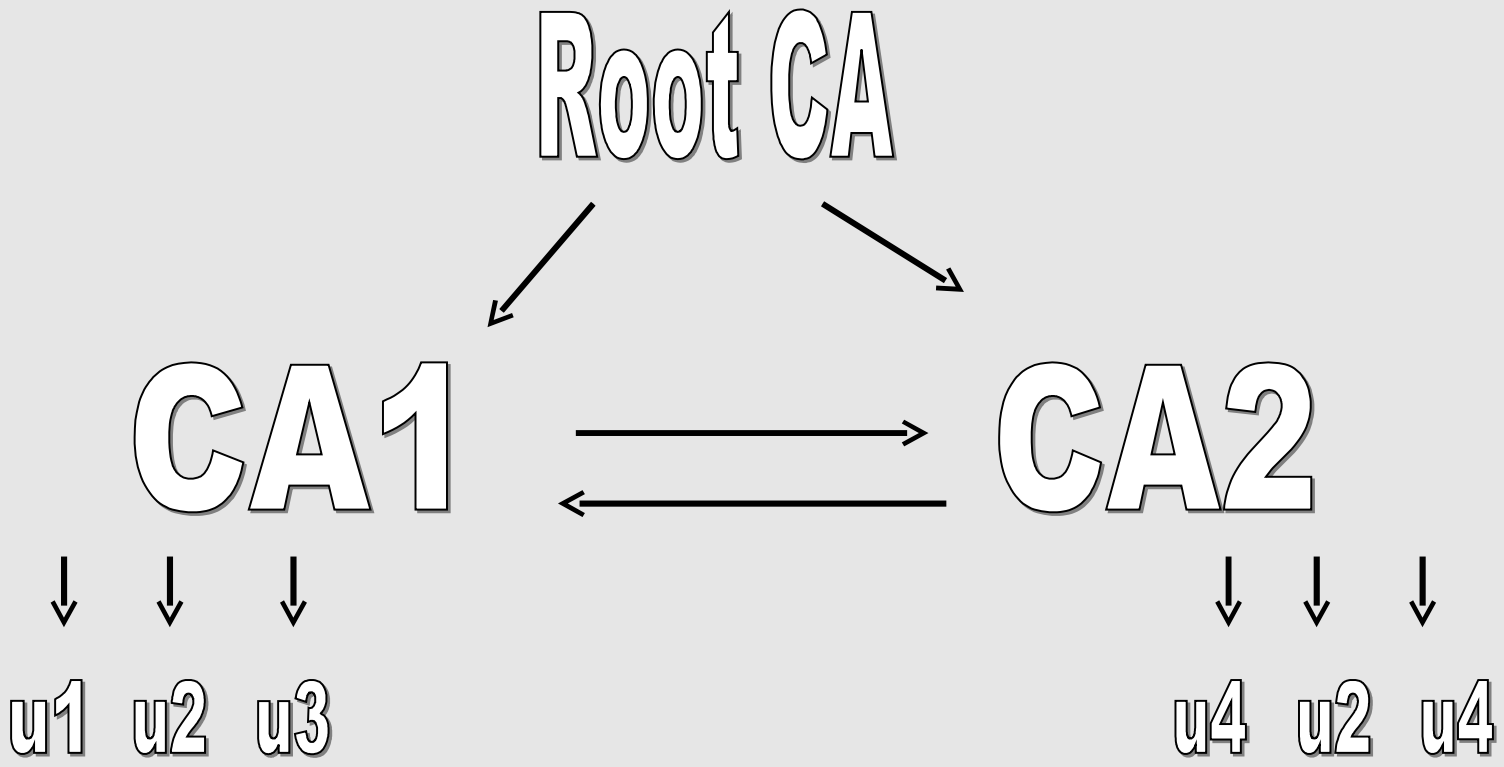
Certificate Revocation Lists: CRL

- Elencano i certificati che sono stati revocati
- Devono essere aggiornate e disponibili
- Richiedono un meccanismo di sincronizzazione

Certification path

- Le CA possono firmare certificati per altre CA, creando delle catene di certificati
- Per fidarsi di un certificato bisogna fidarsi di tutta la catena a monte
- La fiducia si basa sulle politiche delle diverse CA

Firme reciproche: modello gerarchico e piatto



Servizi di timestamp

- Un servizio di timestamp firma una coppia (hash del documento, orario)
- Garantisce l'esistenza del documento a una data
- Limita i danni della compromissione di una chiave
  - in particolare la chiave di una CA

Politiche di certificazione

- Definiscono:
  - chi genera le chiavi
  - lunghezze minime e massime delle chiavi
  - requisiti per l'identificazione delle parti
  - requisiti di sicurezza per la generazione di certificati e CRL nonché i controlli
  - frequenza di generazione delle CRL
  - meccanismi di revoca delle chiavi
  - vincoli sui nomi o attributi degli utenti
  - meccanismi di audit

Public Key Infrastructure

PKI: Public Key Infrastructure

- È un'infrastruttura per:
  - generare certificati
  - distribuire i certificati
  - rendere disponibili le condizioni (politiche di sicurezza) di creazione dei certificati e di cross certification
  - generare e distribuire le CRL
  - gestire il ciclo di vita delle chiavi
  - gestire il timestamp

Entità principali coinvolte in una PKI

- Utente:
  - richiede la creazione di un certificato per una propria chiave
  - richiede il certificato (o una CRL) di un altro utente per verificarne la chiave
- Certification Authority:
  - genera certificati per altri utenti, anche altre CA, secondo una certa politica

Entità coinvolte in una PKI (2)

- Registration Authority:
  - è un tramite fra gli utenti e la CA
  - identifica gli utenti ma non produce certificati
- Altre CA
  - può essere necessario accettare certificati emessi da un'altra CA
  - per questo le due CA effettuano una Cross Certification
  - non è un semplice riconoscimento reciproco ma l'accettazione delle rispettive politiche

Compiti della Registration Authority

- controlla l'identità degli utenti che richiedono la generazione di certificati
- fornisce alla CA i dati sull'identità del richiedente e la richiesta
- riceve e verifica i certificati forniti dalla CA
- consegna i certificati agli utenti

Standard: PKCS e PKIX

- PKCS è più diffuso ma meno evoluto e poco uniforme
- PKIX, sviluppato dall'IETF, è più recente e più evoluto
- Esempio: la "proof of possession"

Generazione delle chiavi

- Le chiavi possono essere generate:
  - dall'utente; la CA dovrà verificarne la corrispondenza alla politica
  - da un apposito meccanismo che le fornisce all'utente e poi distrugge la propria copia
- La chiave privata deve essere nota solo all'utente salvo meccanismi di key escrow

Verifica delle firme

- Per la verifica di una firma un utente si deve procurare tutta la catena di certificati
- Ogni certificato deve essere verificato rispetto alla più recente CRL
- I certificati possono essere accumulati localmente in una cache

Compromissione delle chiavi

- Se si sospetta la compromissione di una chiave privata questa deve essere subito revocata
- La CA deve verificare la correttezza e legittimità delle richieste di revoca
- La compromissione della chiave di una CA comporta l'invalidazione di tutti i certificati firmati
- Può essere utile la firma di due CA per certificato

Gestione delle CRL

- Possono essere generate:
  - periodicamente
  - a ogni nuova revoca
- Possono essere distribuite:
  - direttamente dalla CA ai propri utenti
  - attraverso il servizio di directory

Punti di distribuzione delle CRL

- Permettono di indicare dove sono reperibili le CRL:
  - entry della directory
  - altri posti dai quali può essere ottenuta la CRL: indirizzi di e-mail, URL, ecc.
- In X.509 sono un'estensione introdotta nella v.3

Rigenerazione dei certificati

- La durata di validità di un certificato non coincide in generale con quella della firma della CA
- Allo scadere della validità della firma della CA è necessario “rigenerare” i certificati

Archiviazione di certificati e CRL

- È necessario archviare certificati e CRL
- L'archiviazione oltre la data di scadenza pone molti problemi:
  - possono essere usati per dimostrare la validità di una firma?
  - Possono essere modificati dopo la compromissione della firma della CA?
  - ...

Sospensione dei certificati

- È simile alla revoca, ma è temporanea
- È meno critica, può essere accettata più facilmente (es. PIN e richieste autofirmate) e poi verificata
- Non è implementata dai prodotti più diffusi e utilizzati

Responsabilità delle CA

- Un comportamento della CA non corrispondente alle politiche o negligente può causare danni notevoli
- In caso di firme con valore legale è possibile che la CA possa essere la PA
- In questo caso la responsabilità può essere ridotta e conseguentemente anche la fiducia degli utenti
- Un esempio: Verisign e la falsa chiave Microsoft

Formato dei certificati: X.509

- 1988: versione 1, come attributo nell'ambito dello standard X.500
- Revisioni nel 1993 (v.2) e nel 1996 (v.3)

Formato di X.509

- I campi base per tutte le versioni sono:
  - numero di serie
  - identificatore algoritmo di firma
  - nome di chi ha emesso il certificato, issuer (opz. identificatore unico)
  - validità (inizio, fine)
  - nome del soggetto (opz. id. unico)
  - chiave pubblica del soggetto
  - firma del certificato

Estensioni di X.509 v.3

- L’indicatore di criticità stabilisce che chi elabora il certificato deve scartare il certificato se non sa come interpretare questi campi
- I campi devono essere “registrati” in modo da essere riconosciuti univocamente
- Esistono estensioni standard ma sono possibili estensioni private

Estensioni di X.509 v.3 (2)

- Le estensioni sono composte da:
  - un identificatore di estensione
  - un indicatore di criticità
  - un valore in ottetti (byte)
- Si possono aggiungere estensioni senza modificare il formato di X.509

Informazioni sulla chiave e sulle politiche

- Identificatori di chiave della CA o del soggetto: un soggetto può avere più chiavi o più certificati associati a una chiave, ad es. consecutivi
- Uso della chiave:
  - firma digitale, non repudiation, cifratura di chiavi, cifratura di dati, key agreement, firma di certificati, firma di CRL

Certificati diversi per usi diversi

- Certificati diversi per ruoli diversi
- Non solo persone fisiche: es. SSL
- Limitazioni alla validità dei certificati

Servizi di directory

- Sono lo strumento adatto alla gestione e distribuzione su larga scala di informazioni su entità: persone, organizzazioni, ecc.
- A ogni utente che si registra al servizio viene associata una entry con i suoi dati
- Esiste un'infrastruttura per l'accesso distribuito alle entry per la registrazione, cancellazione, consultazione e modifica
- Sono lo strumento tipico per la distribuzione di certificati e CRL

Il servizio di directory X.500

- È un servizio di directory:
  - permette di pubblicare informazioni su oggetti
  - permette di cercare oggetti e le informazioni associate
- È previsto uno sviluppo nell'utilizzo di questo standard
- Finora ha avuto poco successo...

Key Recovery

- L’azienda si garantisce la possibilità di accedere ai documenti cifrati
- Offre un servizio agli utenti
- Non si garantisce la possibilità di falsificare le firme
- Servono due coppie di chiavi per utente
- Key escrow?

Tutte le chiavi saranno compromesse

- Le capacità di calcolo aumentano
- A meno di chiavi estremamente lunghe, prima o poi si arriva a forzarle
- È opportuno usare chiavi molto lunghe
- Si deve supporre che le chiavi vecchie siano di fatto forzate
- È necessario “rigenerare” i timestamp

Compromissione della chiave di cifratura

- Permette l’accesso ai dati cifrati
- Non invalida la firma se fatta con un’altra chiave

Compromissione della chiave di firma

- Permette di creare firme false
- La revoca della chiave (quando scoperta) non lo impedisce
- Il timestamp permette di mantenere la validità dei documenti già firmati.

Compromissione della chiave della CA

- Permette di generare certificati falsi
- La revoca comporta la revoca dei certificati emessi
- Anche in questo caso il timestamp permette di limitare i danni

Compromissione del repository

- Se è solo repository, permette di eliminare le CRL straordinarie
- Non comporta la compromissione di chiavi o la possibilità di falsificare certificati

Compromissione della chiave di timestamp

- Permette di creare documenti predatati
- Quindi anche datati a quando erano usate chiavi ora falsificabili...
- È un servizio semplice ma estremamente critico
- Può essere opportuno usarne più di uno

Inaccessibilità del repository

- Le chiavi sono verificate con le informazioni già ottenute (o altrimenti si blocca l'attività)
- Impossibilità di scaricare le CRL, ordinarie o urgenti

Altri sistemi a chiave pubblica

- PGP (Pretty good privacy)
- SSH (secure shell)
- SSL (Secure Socket Layer)
- IPSEC
- Protocolli proprietari

LDAP e CLDAP

- Il protocollo di accesso DAP per X.500 era lento e pesante
- l'IETF ha sviluppato il *Lightweight Directory Access Protocol*
- Nel 1995 ha sviluppato anche il *Connection-less Lightweight X.500 Directory Access Protocol* (UDP)

Caratteristiche di LDAP v.3 (1)

- Molto più semplice di DAP
- Permette la ridirezione delle richieste verso un altro DSA
- Dispone di un'API standard in linguaggio C (RFC 1823)
- La disponibilità di un'API permette di usarlo con directory non X.500
- Codifica delle richieste e risposte: BER/DER

Caratteristiche di LDAP v.3 (2)

- Incorpora CLDAP come versione su UDP
- Supporta set di caratteri non ASCII
- Permette all'utente di richiedere i dati in pagine o con una dimensione limite
- Supporta nuovi tipi di regole nella ricerca
- Permette vari tipi di autenticazione
- Può essere trasportato su SSL (LDAPS)

I nomi degli oggetti

- Distinguished Name: è composto dal valore di tutti gli attributi dalla radice all'entry; es. t=DL,a=1993,n=12
- Relative Distinguished Name: è il solo valore dell'attributo che lo rende unico nella sottoclasse; es n=21