# Certificazione delle chiavi

# Certificazione delle chiavi

- I protocolli visti prima  funzionano assumendo che la chiave pubblica sia giusta e inattaccabile ma questo non e' vero!!!
- Le chiavi si pubblicano su siti web, si scambiano via mail, ecc.
- E' possibile un “man-in-the-middle attack”, intercetta e modifica la comunicazione, sostituisce la chiave pubblica con la propria

# Certificazione delle chiavi

- Per questo motivo sono nate le (Key) Certification Authority (brevemente **CA**), enti preposti alla certificazione di validita' delle chiavi pubbliche.

# Codice dell'amministrazione digitale

D.Lgs. 7 marzo 2005, n. 82, aggiornato con D.Lgs. n. 159 del 4 aprile 2006

- Art. 26 (Certificatori)
  - 1. L'attività dei certificatori stabiliti in Italia o in un altro Stato membro dell'Unione europea è libera e non necessita di autorizzazione preventiva. Detti certificatori o, se persone giuridiche, i loro legali rappresentanti ed i soggetti preposti all'amministrazione, devono possedere i requisiti di onorabilità richiesti ai soggetti che svolgono funzioni di amministrazione, direzione e controllo presso le banche di cui all'articolo 26 del testo unico delle leggi in materia bancaria e creditizia, di cui al decreto legislativo 1° settembre 1993, n. 385, e successive modificazioni.

# Codice dell'amministrazione digitale

D.Lgs. 7 marzo 2005, n. 82, aggiornato con D.Lgs. n. 159 del 4 aprile 2006

- Art. 27 (Certificatori)
  - 3. I certificatori di cui al comma 1, devono comunicare, prima dell'inizio dell'attività, anche in via telematica, una dichiarazione di inizio di attività al CNIPA, attestante l'esistenza dei presupposti e dei requisiti previsti dal presente codice.

# Codice dell'amministrazione digitale

D.Lgs. 7 marzo 2005, n. 82, aggiornato con D.Lgs. n. 159 del 4 aprile 2006

- Art. 32 (Obblighi del titolare e del certificatore)
- 3. Il certificatore che rilascia, ai sensi dell'articolo 29, certificati qualificati deve inoltre:

  - a) provvedere con certezza alla identificazione della persona che fa richiesta della certificazione

  -b) rilasciare e rendere pubblico il certificato elettronico nei modi o nei casi stabiliti dalle regole tecniche di cui all'articolo 71, nel rispetto del decreto legislativo 30 giugno 2003, n. 196, e successive modificazioni;

# Certificazione delle chiavi

- La CA e' un intermediario di fiducia
- La CA autentica l'associazione (utente,chiave pubblica) emettendo un certificato digitale , cosi' come l'anagrafe di un comune autentica l'associazione (dati personali, fotografia) rilasciando una carta d'identita'
- Quando la chiave pubblica e' stata certificata puo' essere distribuita da qualsiasi punto (pag web, ecc.)

# Codice dell'amministrazione digitale

D.Lgs. 7 marzo 2005, n. 82, aggiornato con D.Lgs. n. 159 del 4 aprile 2006

- Art. 1. Definizioni.

g) certificatore: il soggetto che presta servizi di certificazione delle firme elettroniche o che fornisce altri servizi connessi con queste ultime;

# Codice dell'amministrazione digitale

D.Lgs. 7 marzo 2005, n. 82, aggiornato con D.Lgs. n. 159 del 4 aprile 2006

- Art. 1. Definizioni.

  e) certificati elettronici: gli attestati elettronici che collegano all'identità del titolare i dati utilizzati per verificare le firme elettroniche

- Art. 24. Firma digitale.

  3) Per la generazione della firma digitale deve adoperarsi un certificato qualificato che, al momento della sottoscrizione, non risulti scaduto di validità ovvero non risulti revocato o sospeso.

  4) Attraverso il certificato qualificato si devono rilevare, secondo le regole tecniche stabilite ai sensi dell'articolo 71, la validità del certificato stesso, nonché gli elementi identificativi del titolare e del certificatore e gli eventuali limiti d'uso.

# Codice dell'amministrazione digitale

D.Lgs. 7 marzo 2005, n. 82, aggiornato con D.Lgs. n. 159 del 4 aprile 2006

- Art. 32 (Obblighi del titolare e del certificatore)
- 3. Il certificatore che rilascia, ai sensi dell'articolo 29, certificati qualificati deve inoltre:

  - a) provvedere con certezza alla identificazione della persona che fa richiesta della certificazione

  -b) rilasciare e rendere pubblico il certificato elettronico nei modi o nei casi stabiliti dalle regole tecniche di cui all'articolo 71, nel rispetto del decreto legislativo 30 giugno 2003, n. 196, e successive modificazioni;

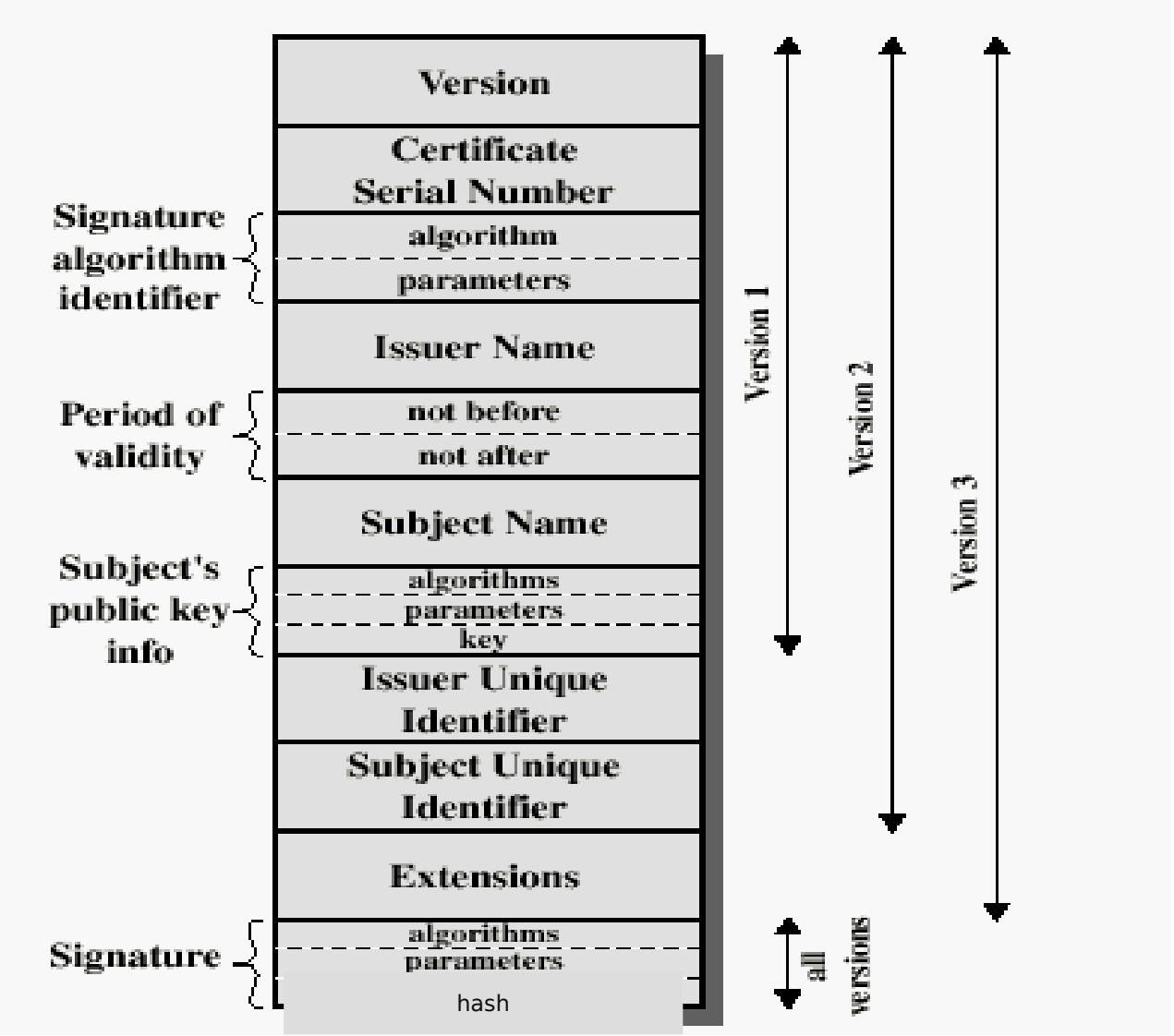
# Il certificato digitale

- Il certificato digitale consiste in una chiave pubblica e in una lista di informazioni relative al suo proprietario, opportunamente firmate dalla CA.

# Il certificato digitale

- Indicazione del formato (numero di versione).
- Nome della CA che lo ha rilasciato.
- Numero seriale che individua univocamente il certificato all'interno della CA emittente.
- L'algoritmo e il formato dei parametri usati dalla CA per creare la firma.[1]
- Il periodo di validita' del certificato (inizio e fine).
- Il nome e altre informazioni dell'utente a cui questo certificato si riferisce.
- Il protocollo a chiave pubblica usato dall'utente per la cifratura e la firma:l'algoritmo, i parametri, la chiave pubblica dell'utente.
- Firma della CA eseguita sulle informazioni precendenti.

# Esempio: il certificato X.509



# Il certificato digitale: la revoca

- I motivi della revoca possono essere vari, es.:

  -e' scaduto il periodo di validita' (una nuova emissione importa un costo)

  -l'utente ha smesso di pagare la CA

  -la chiave privata e' stata compromessa

  -l'utente ha cambiato organizzazione o ruolo

  -la CA cessa di essere operativa e revoca tutti i certificati emessi

  -un nuovo certificato rimpiazza quello vecchio...

# Il certificato digitale: il meccanismo di revoca

- Nel browser si trova una lista dei certificati revocati **(CRL)**

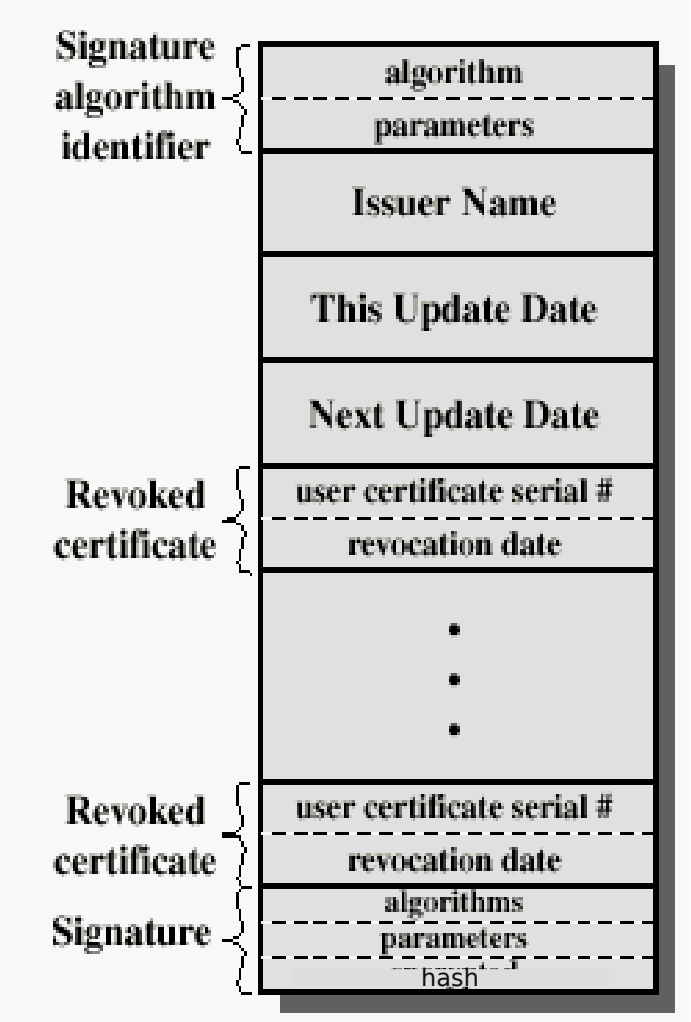
  -le CA diffondono periodicamente le liste dei certificati revocati (analogamente alle compagnie di carte di credito che diffondono i numeri delle carte di credito cancellate)

- Sistema di revoca online

  -La prima volta che il ricevente scarica un certificato deve controllare la validita' tramite un servizio speciale online (analogamente al venditore che chiama il numero della carta di credito per controllare)

- Questo meccanismo e' sufficiente per essere protetti dalla falsificazione di un certificato?
  -Si' perche' ogni certificato e' univocamente determinato da un numero di serie di una CA.

# Esempio: la CRL in X.509



# Il certificato digitale

- Come si ottiene un certificato? Lo si richiede a una CA.

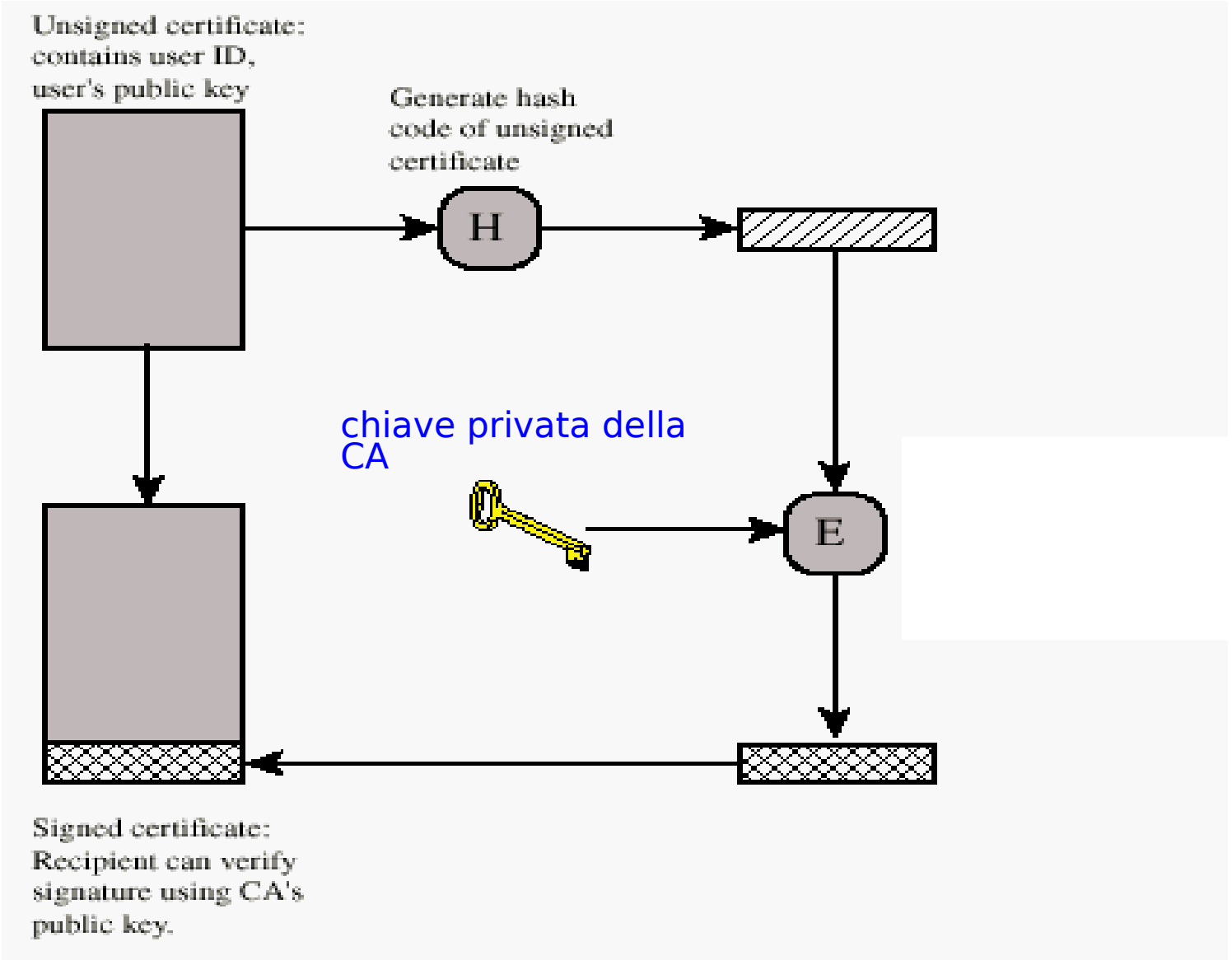
- Dove si trovano i certificati? Si possono trovare in pagine web, possono venire spediti, ecc., in quanto nessuno, salvo la CA emittente, puo' modificarli.

# Il certificato digitale

- Ogni utente conosce la chiave pubblica di alcune CA: e' una preconfigurazione del bowser del calcolatore (quindi bisogna essere sicuri di aver installato un browser affidabile!!!!).
- Come si controlla se una chiave pubblica e' quella vera?

# Il certificato digitale

copia in chiaro del certificato




NOTA: L'autenticita' della chiave pubblica si riduce all'autenticita' della chiave pubblica della CA