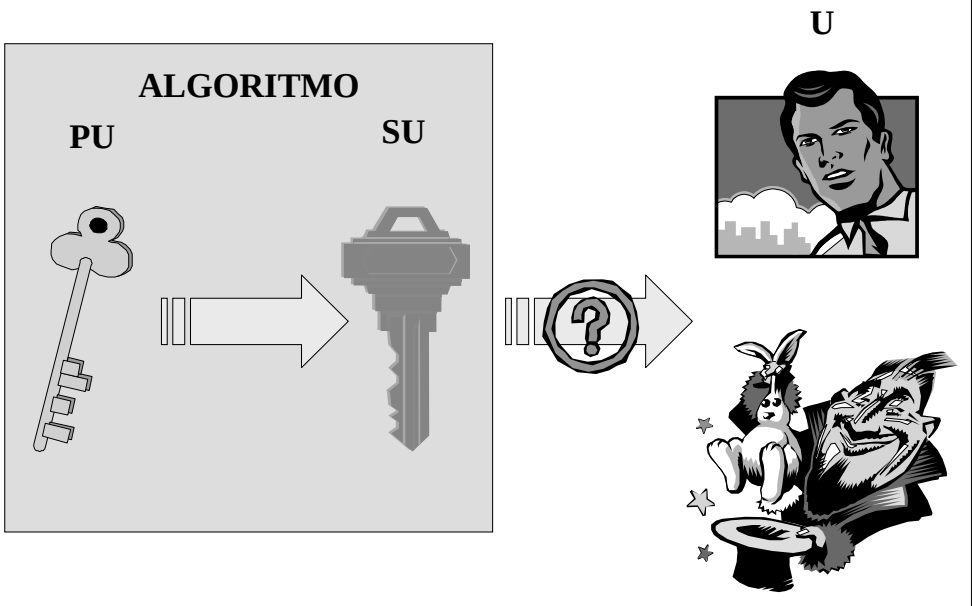
Autenticità della chiave pubblica

- **l'attacco dell'uomo in mezzo**
- **il certificato**
- **la PKI**

Chiavi e Proprietario

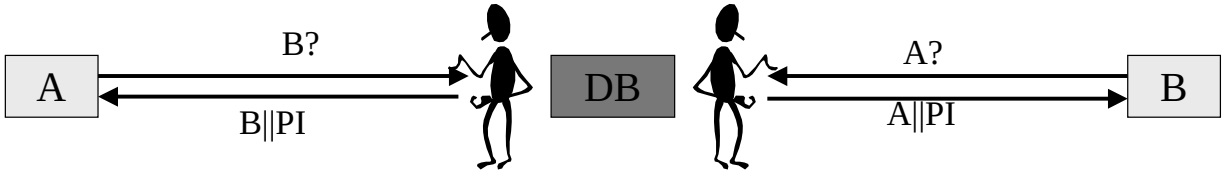


R28: "*prima d'impiegare una chiave pubblica bisogna o essere certi dell'identità del suo proprietario o poterla verificare*"

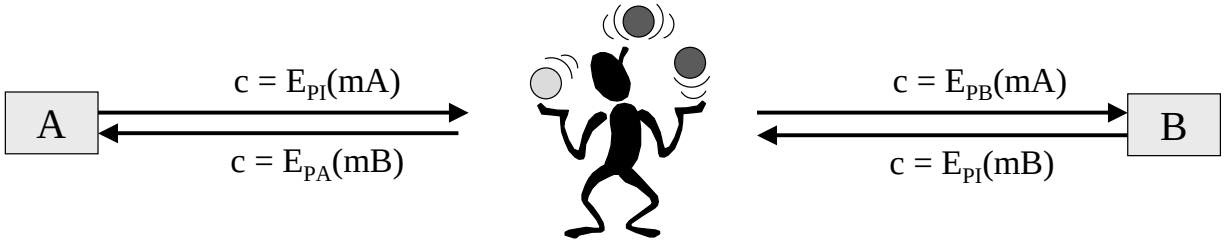
Attacco dell'uomo in mezzo

1 - Registrazione

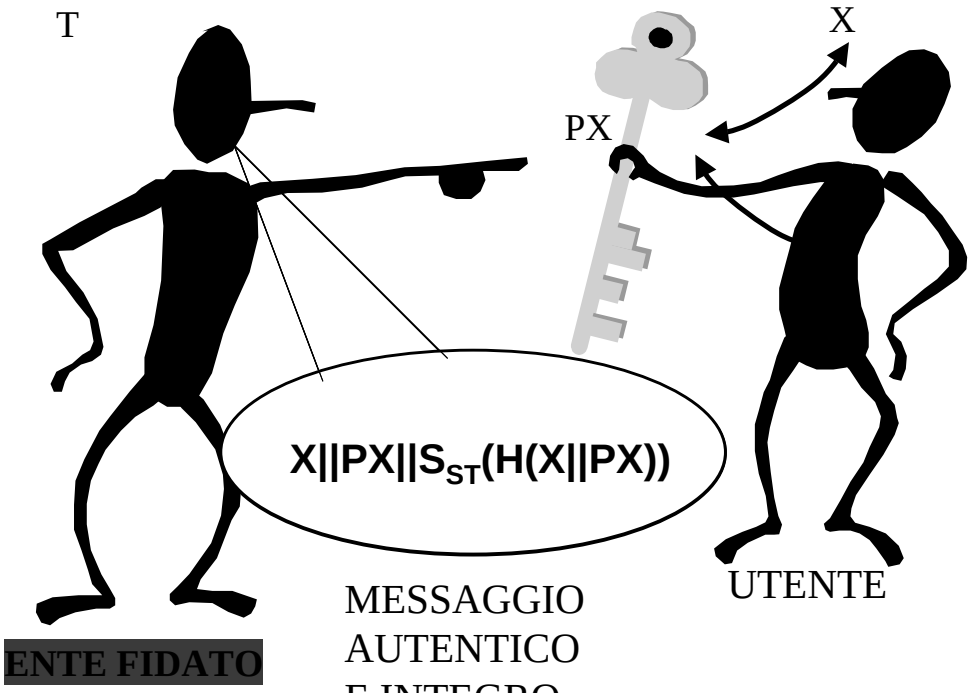
2 - Intercettazione delle interrogazioni e falsificazione delle risposte



3 - Intercettazione, decifrazione, cifratura ed inoltro.



Autenticazione di una chiave pubblica



Preparazione ed uso di un certificato

X identificato in modo sicuro

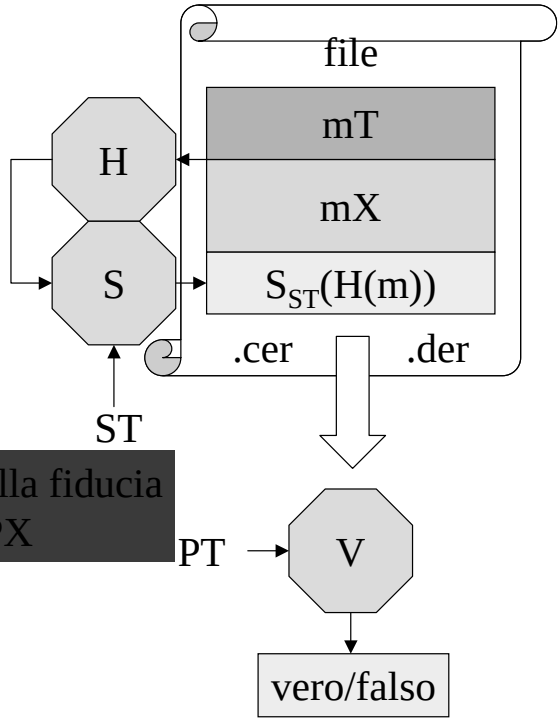
- mX = X||IX||PX||IPX

- mT = T||IT
- m = mT||mX

- H(m)
- $S_{ST}(H(m))$
- Cert(PX,T) = m|| $S_{ST}(H(m))$

PT nota in modo certo

- $V_{PT}(Cert(PX,T))$



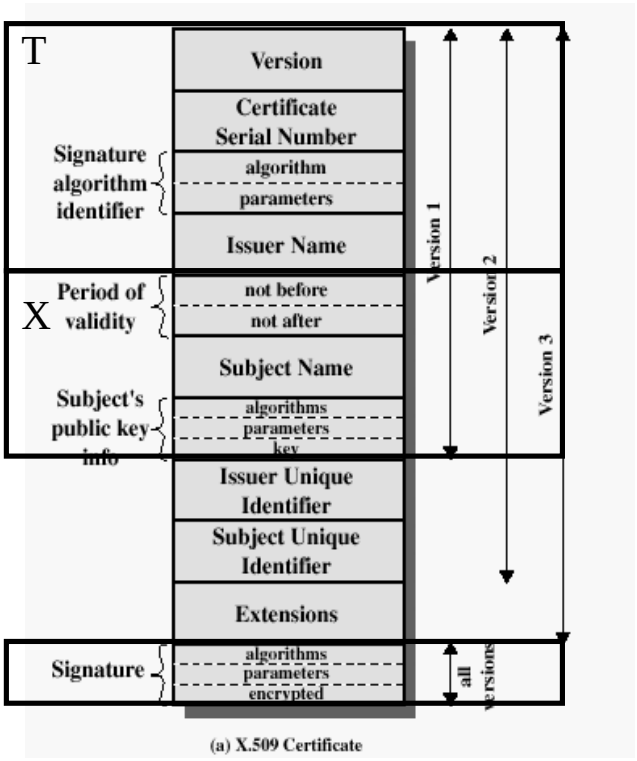
Il Certificatore

T?

- ENTE ufficialmente riconosciuto
  Certification Authority o CA (X.509)

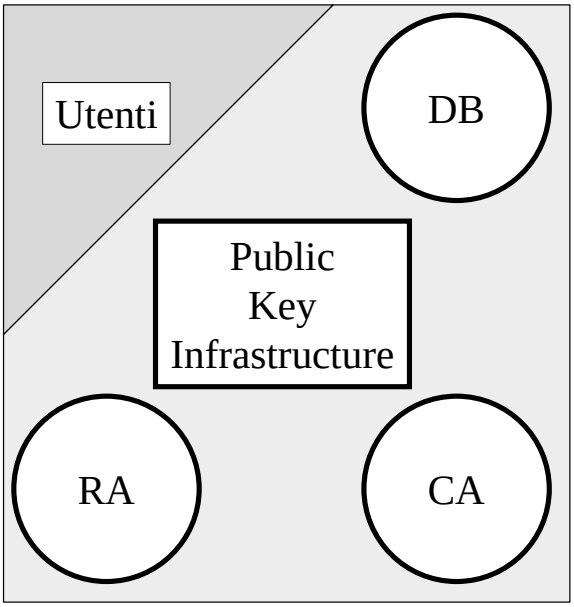
- Qualsiasi UTENTE
  (PGP)

X.509 Formats



(a) X.509 Certificate

PKI: RA, CA e Directory

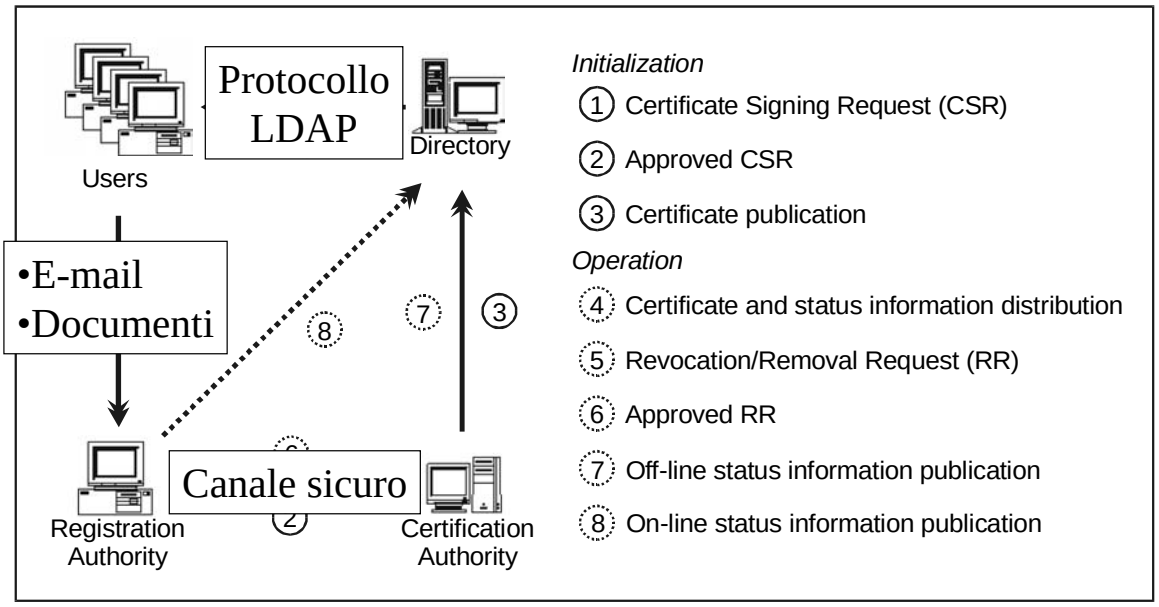


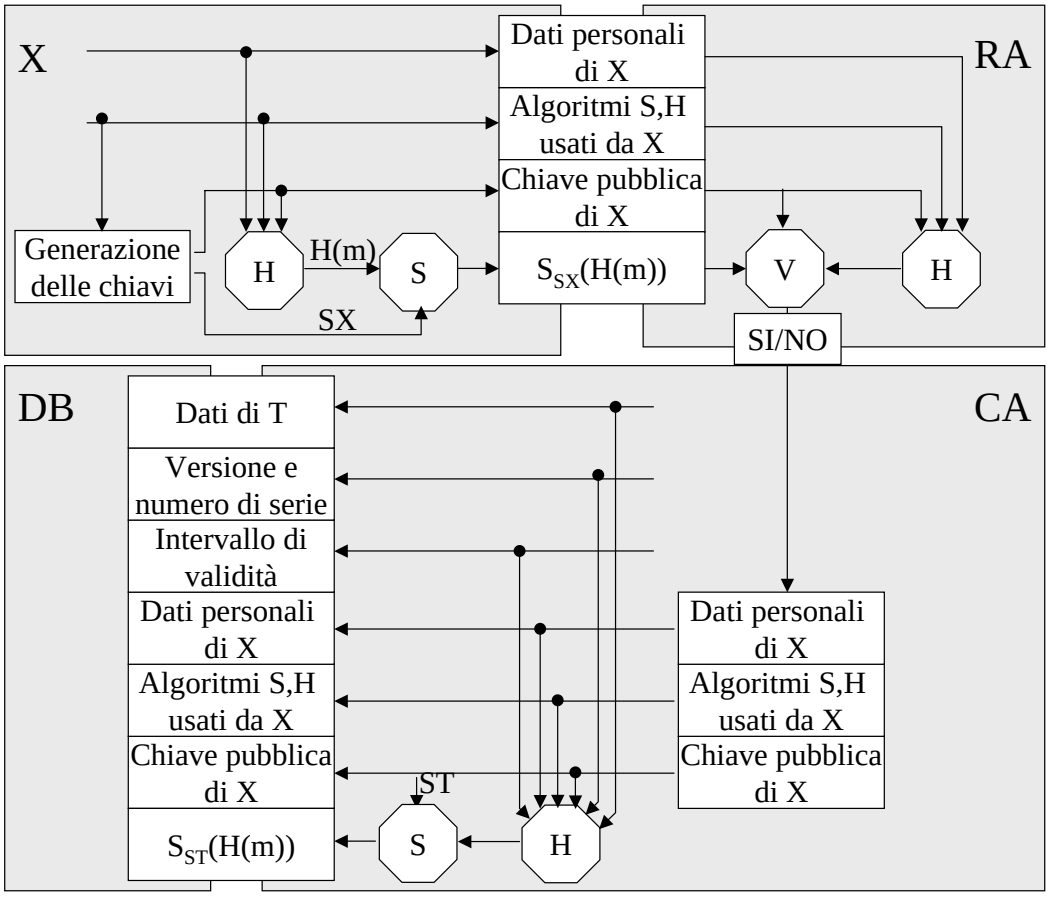
Transazioni

- U → RA
- RA → CA
- CA → U
- CA → DB
- U ↔DB

Verisign
Actalis
Trustitalia
E-trustcom
…

PKI: RA, CA e Directory





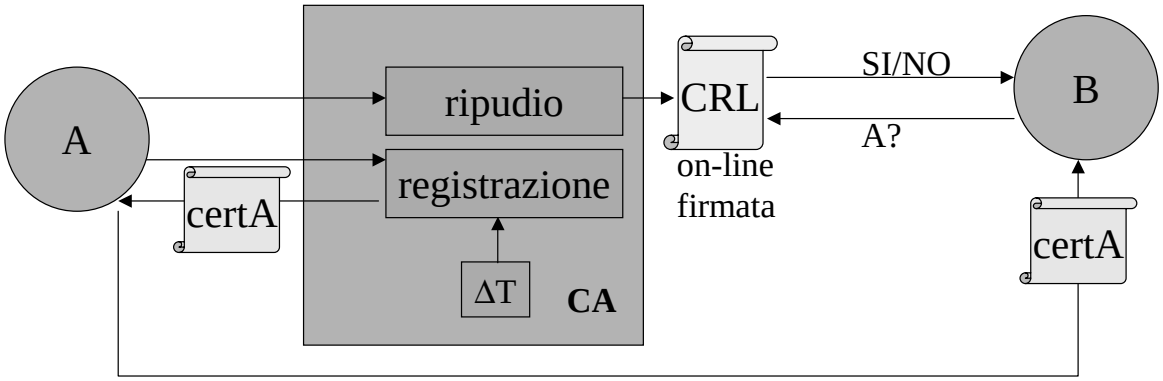
Vita e ripudio di una chiave pubblica

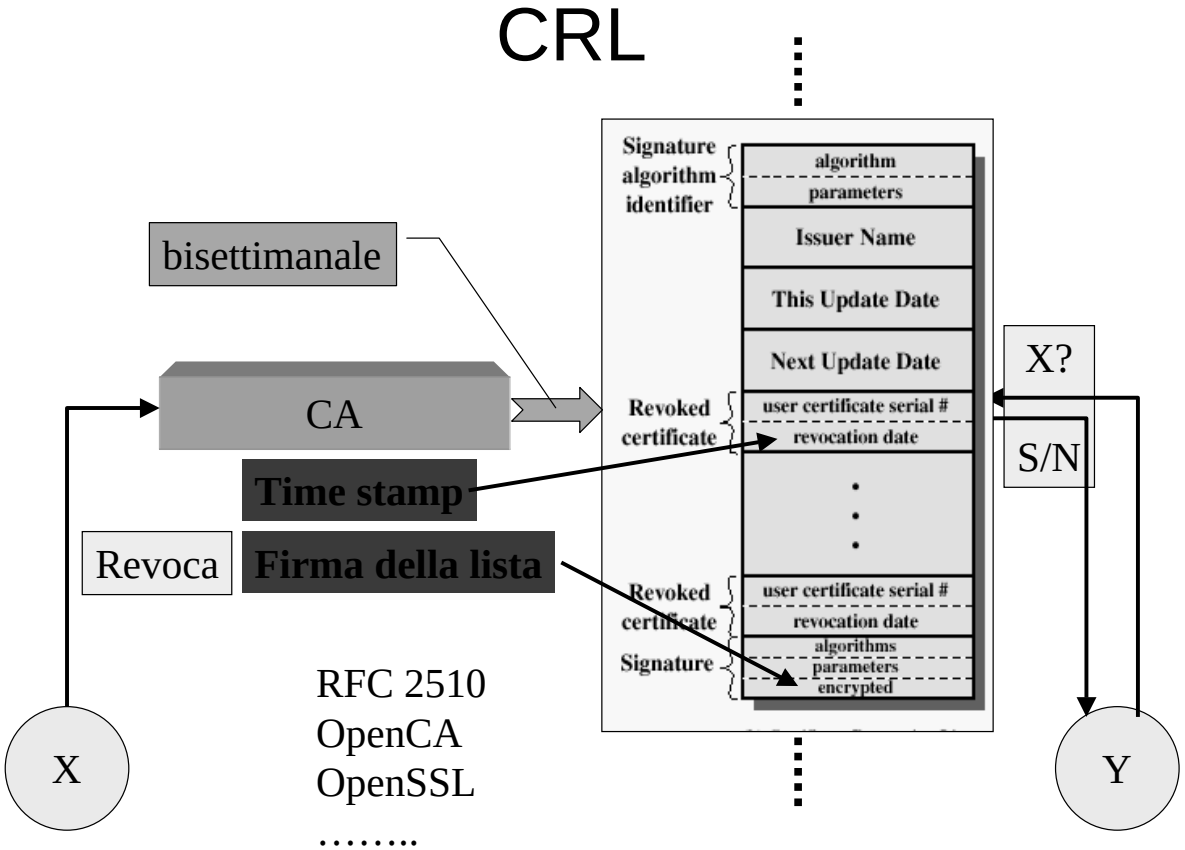
R29: "*Quando uno ha il sospetto, o la certezza, che la sua chiave segreta sia stata violata, deve*

- *rinunciare ad impiegarla,*
- *notificare immediatamente il ripudio alla CA*
- *registrarne una nuova*".

Per prevenire il rischio CA da una vita limitata ad ogni chiave.

Ripudio anche per cambio di ruolo e di Società



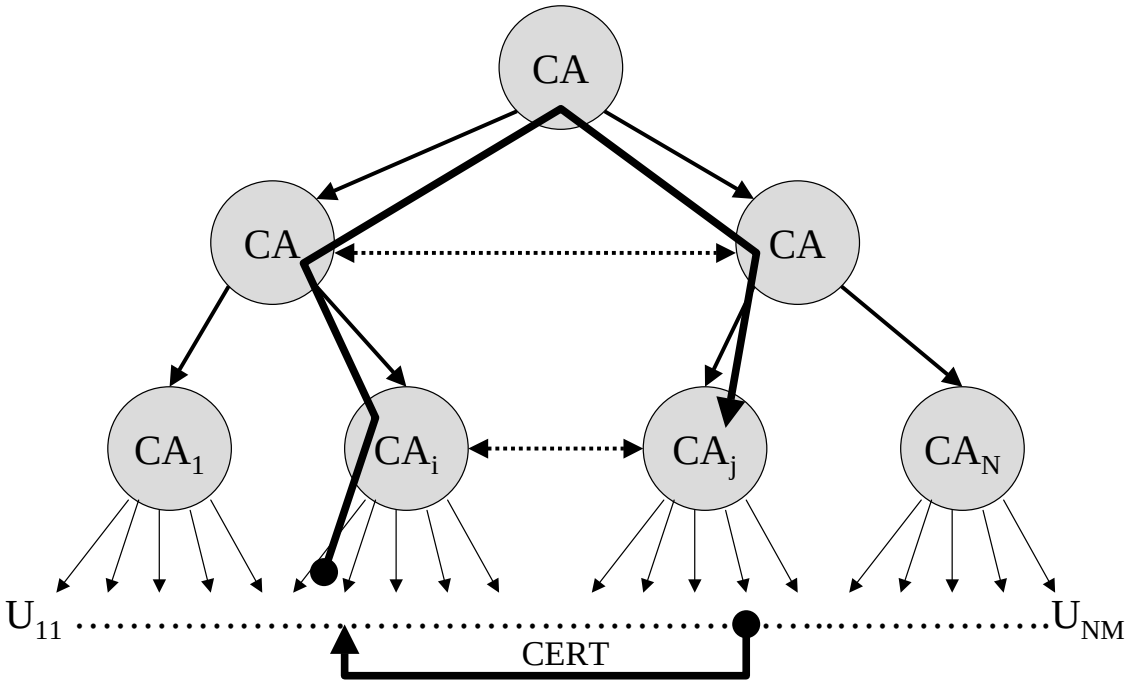


Problemi di PKI

- RA sempre disponibile
- CA rapida anche nella gestione della CRL
- Collo di bottiglia (n° max di utenti)
- Ente degno di fiducia
- Interrogazione della CRL
- Vita della chiave di firma

Gerarchia di Autorità di Certificazione

DPR 513/97 **AIPA** → **cnipa.gov.it**

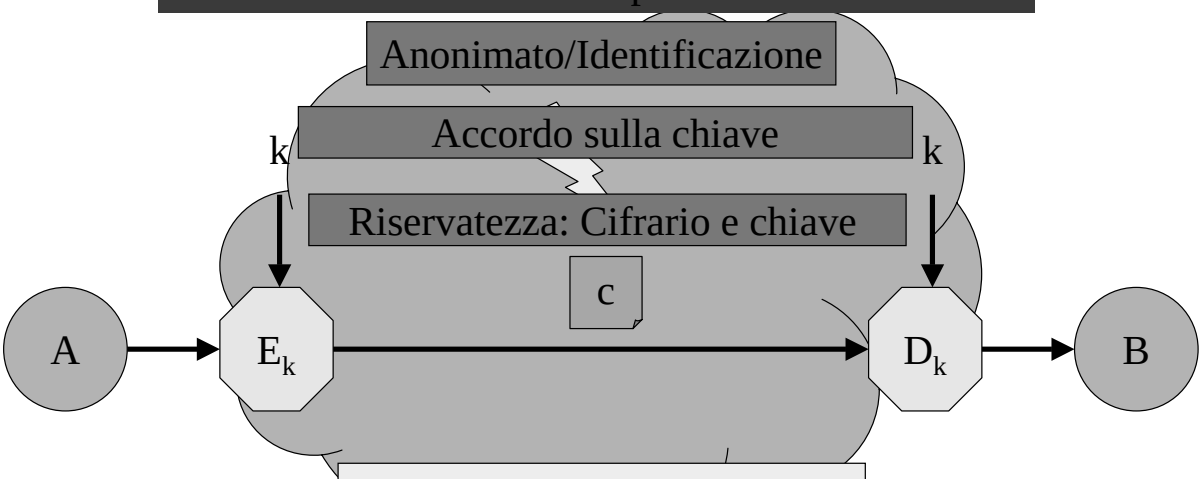


Certificati e reti sicure

- **fixed D-H**
- **ephemeral D-H**
- **IKE**

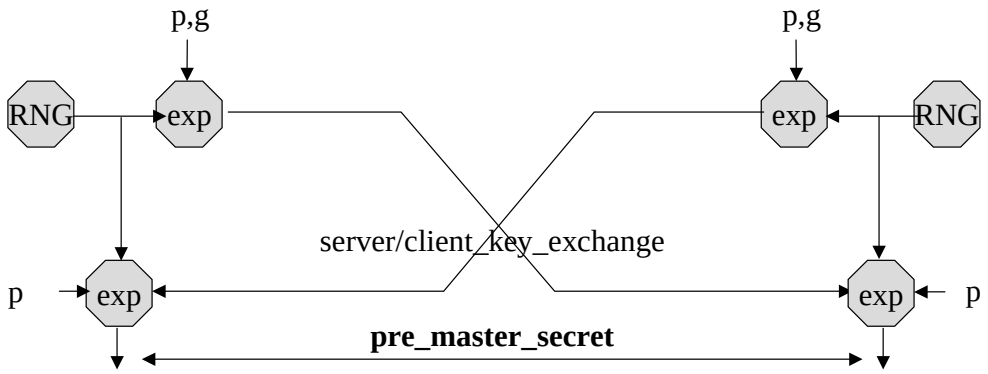
I certificati e le reti sicure

Problema: A e B vogliono scambiarsi informazioni sicure in assenza di accordi precedenti

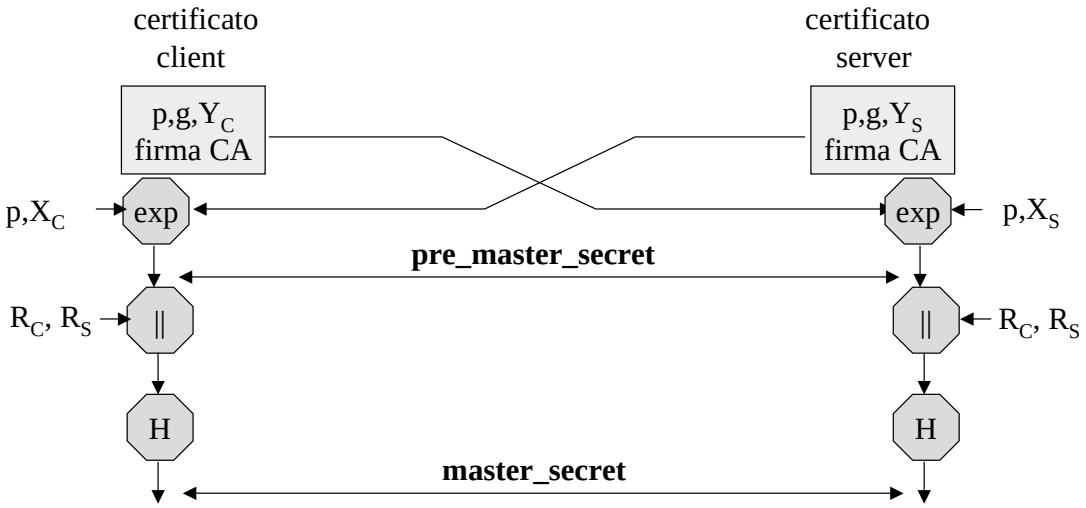


Protocollo posto:
- al livello applicazione
- sopra il livello trasporto: SSL
- al livello di rete: IPSec

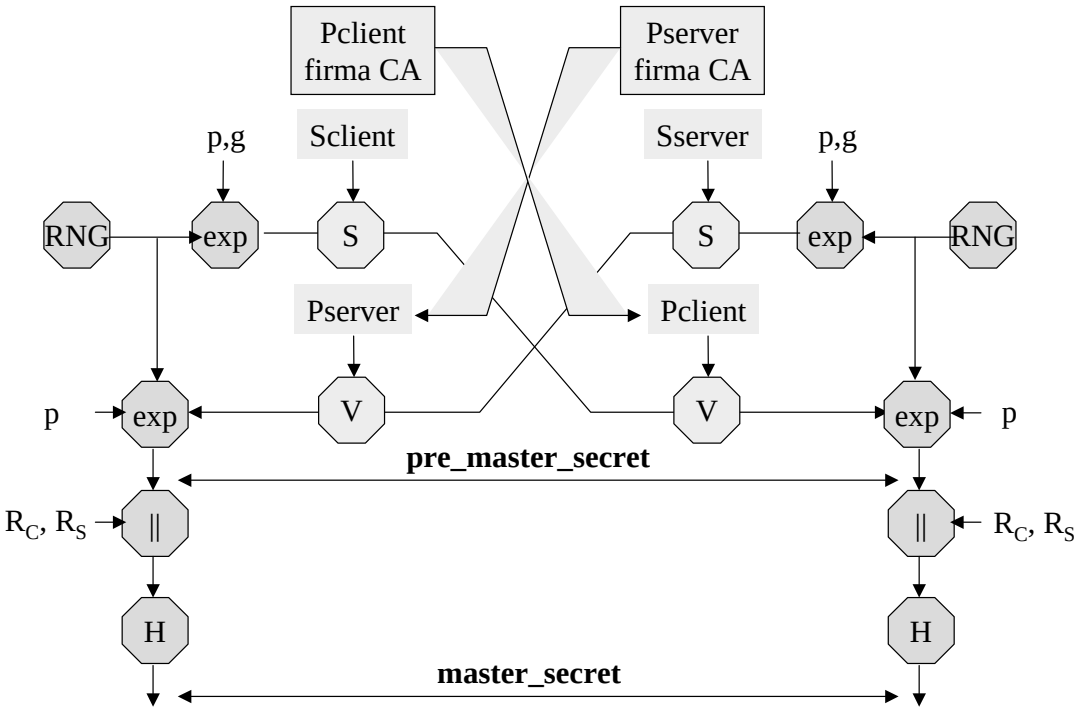
L’accordo sul segreto: anonimous Diffie-Hellman



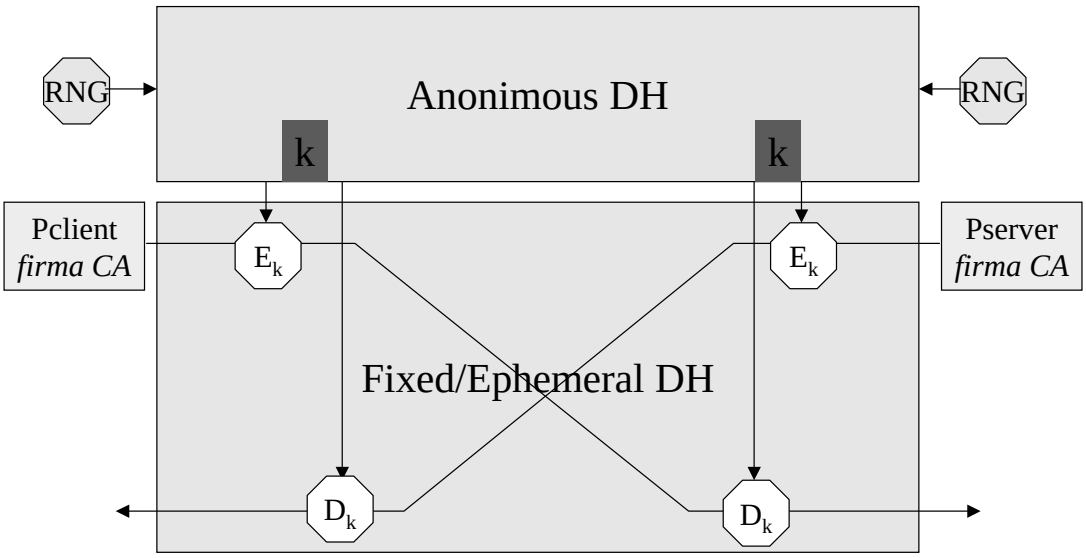
L’accordo sul segreto: fixed Diffie-Hellman



L'accordo sul segreto: ephemeral Diffie-Hellman



Accordo sul segreto e privacy: IKE (Internet Key Exchange)



IKE: anonimato ed identificazione