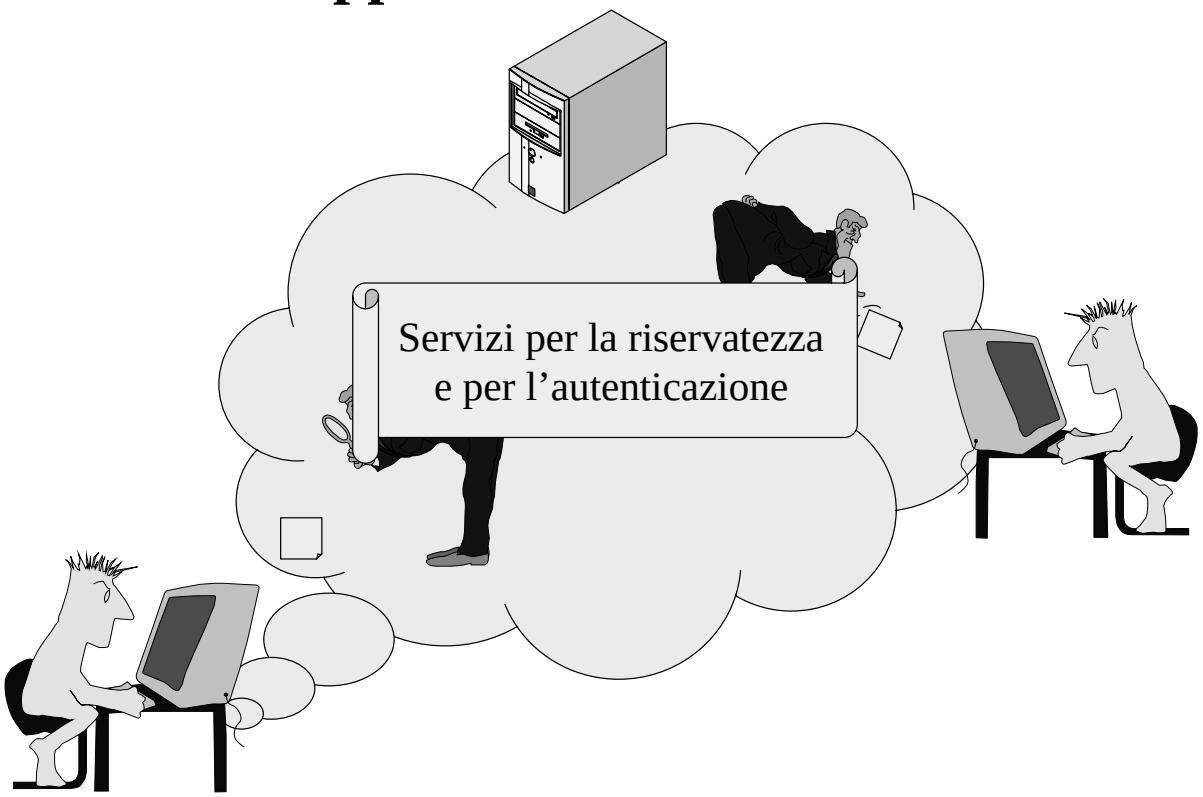
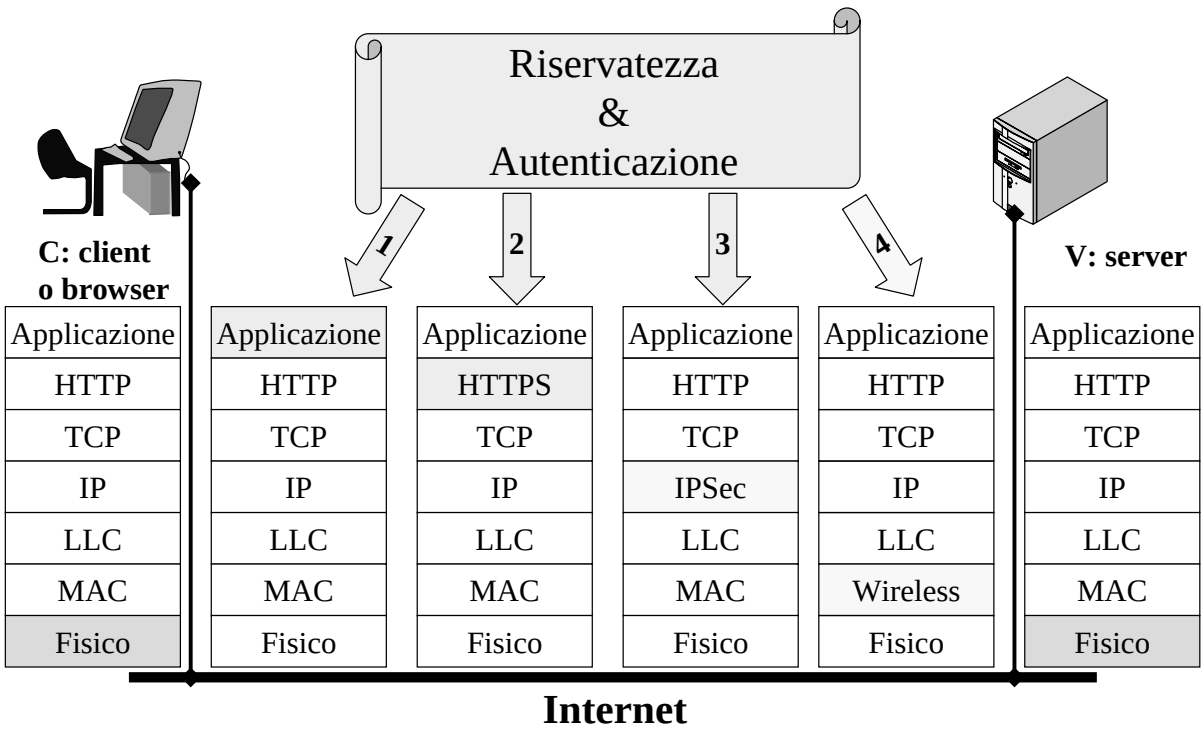
Applicazioni distribuite



Sicurezza a vari livelli

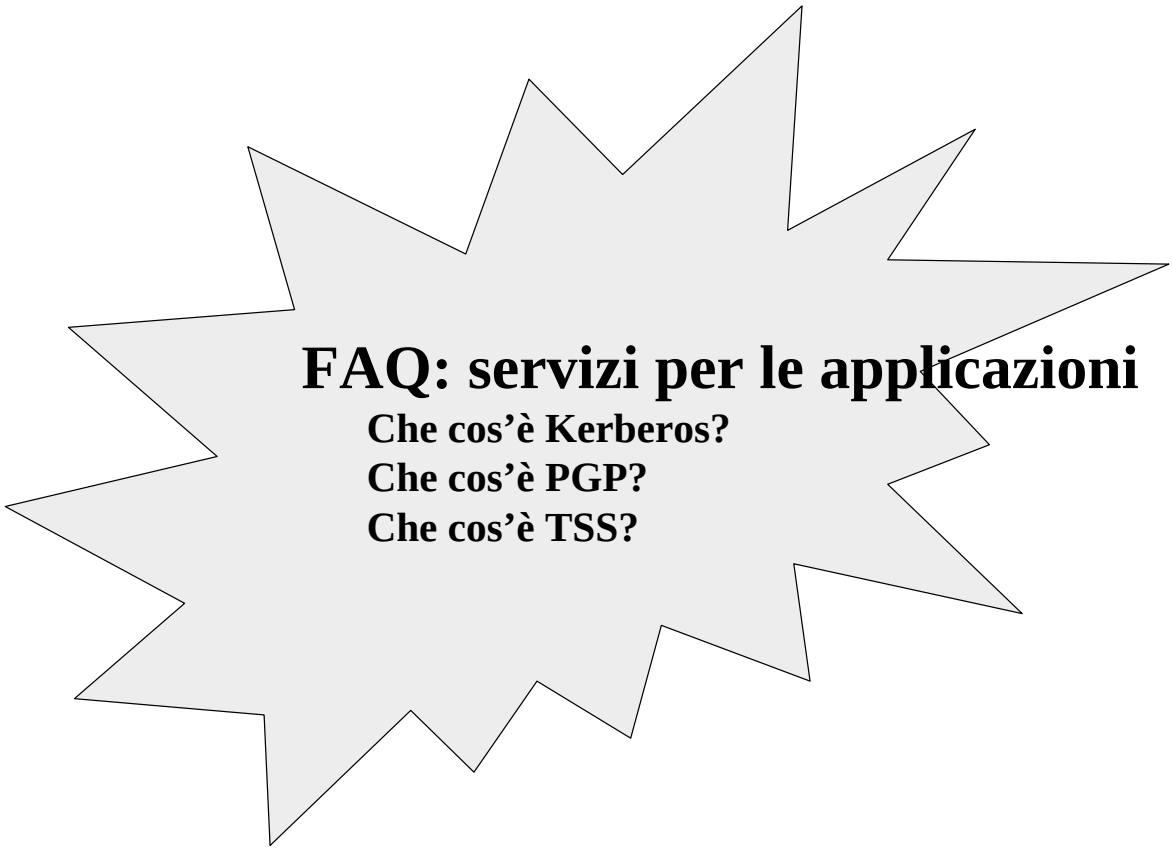


Comunicazioni sicure

Servizi per la riservatezza e per l'autenticazione

- all'interno dell'applicazione (**Kerberos**, **PGP**, **TSS**)
- negli strati di rete (**SSL/TLS**, **IPSec**, **IPv6, 802.11**)

Strumenti per il livello applicazione:
-estensioni dei linguaggi di programmazione (**Java**)
- librerie e servizi ad hoc (**OpenSSL**)



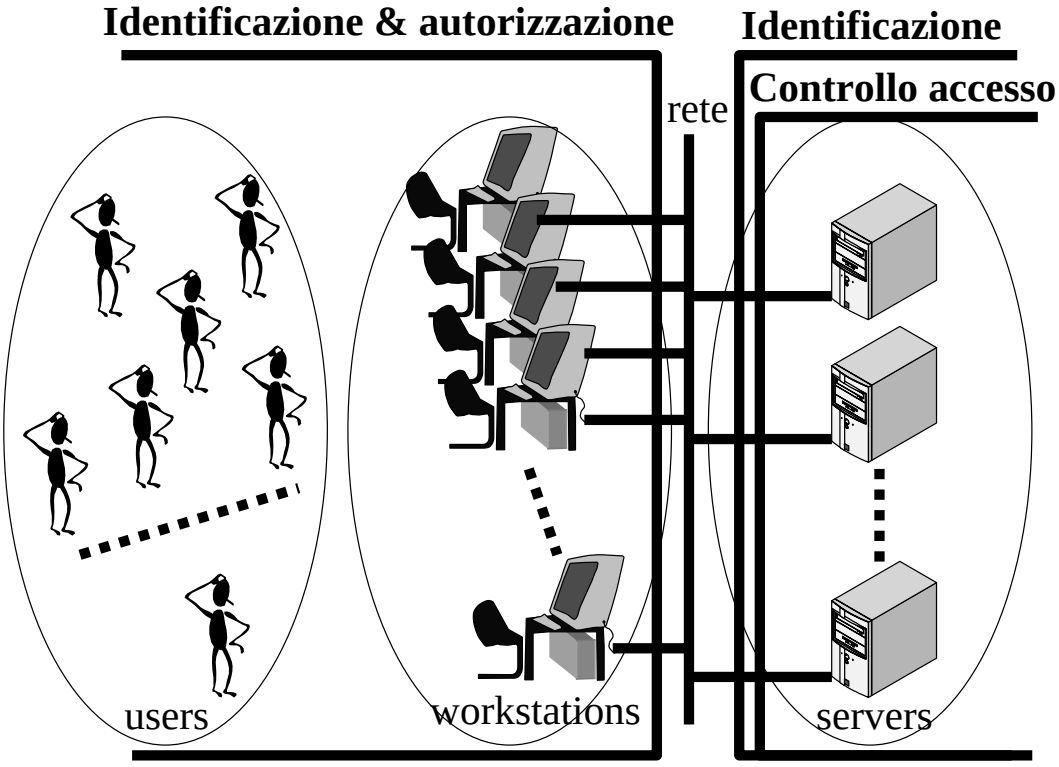
FAQ: servizi per le applicazioni

Che cos'è Kerberos?
Che cos'è PGP?
Che cos'è TSS?

KERBEROS

In Greek mythology, a many headed dog, the guardian of the entrance of Hades

Un sistema client/server



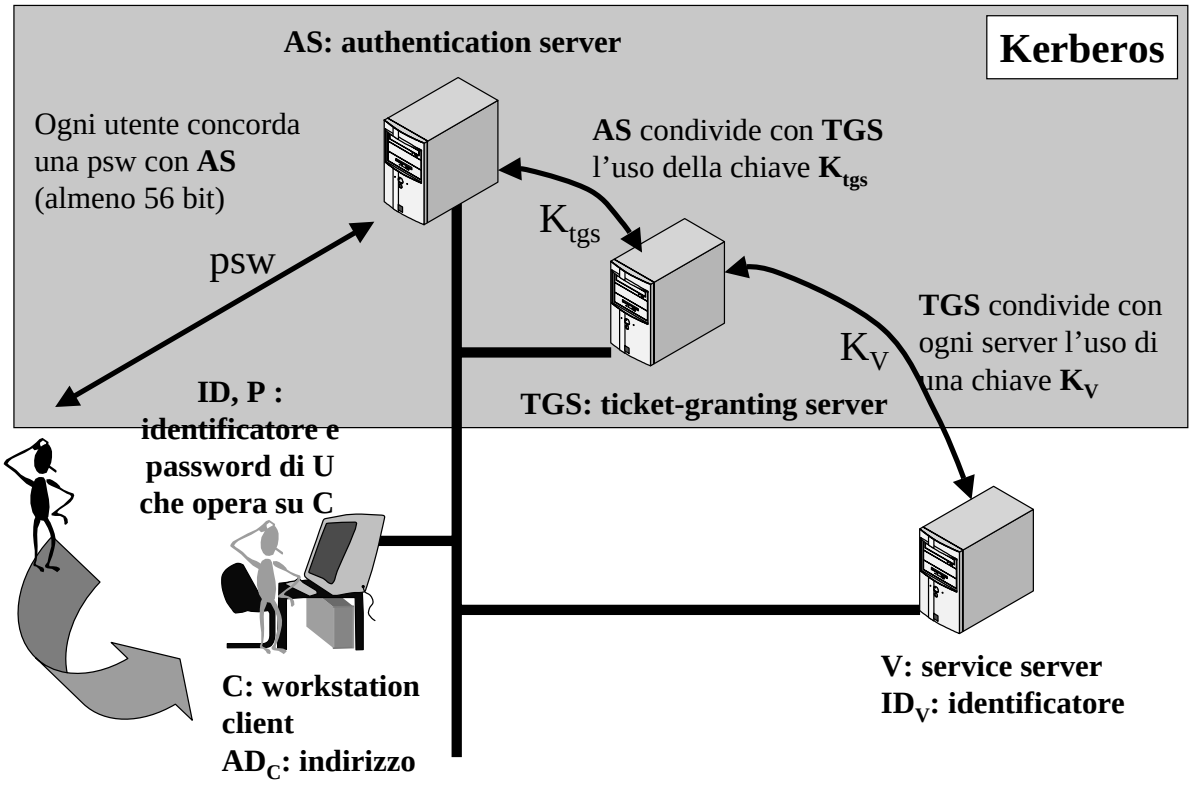
KERBEROS

- Users wish to access services on servers.
- Three threats exist:
  - User pretend to be another user.
  - User alter the network address of a workstation.
  - User eavesdrop on exchanges and use a replay attack.

KERBEROS

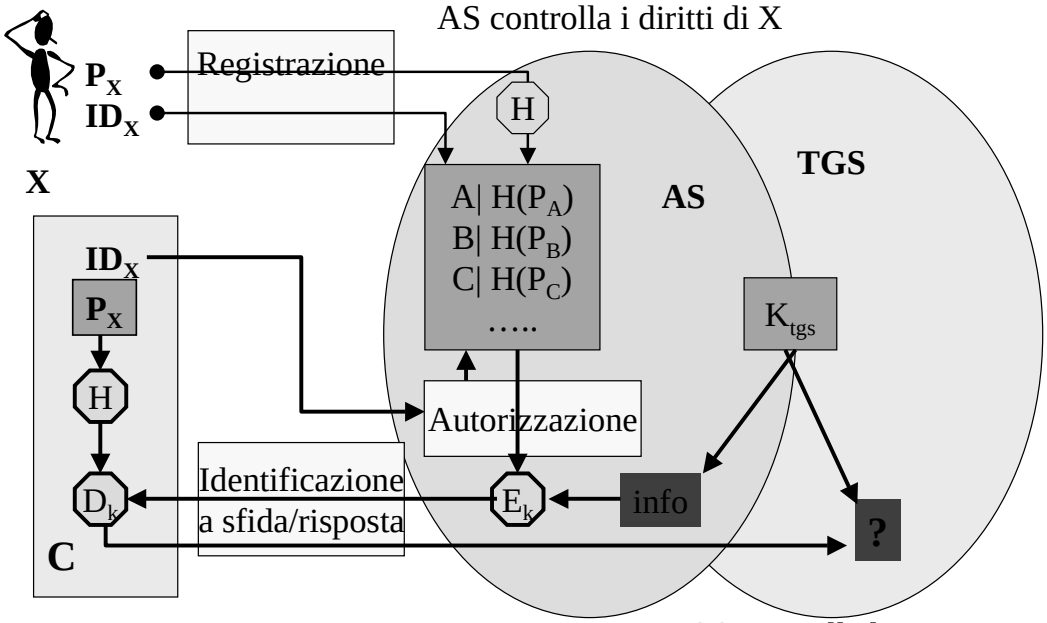
- Provides a centralized authentication server to authenticate users to servers and servers to users.
- Relies on conventional encryption, making no use of public-key encryption
- Two versions: version 4 and 5
- Version 4 makes use of DES

Kerberos: AS, TGS, V, C



Registrazione,Autorizzazione,Identificazione

AS memorizza un hash di 64 bit della password di ogni utente



AS sfida X a mettere in chiaro "info"

TGS controlla la risposta

Il dialogo tra C, AS, TGS e V

1: All'inizio della sessione di lavoro sulla stazione **C**,
l'utente dichiara la sua identità ad **AS**

2: **AS** lo sfida a dimostrare la sua identità a **TGS**

3: **C** risponde alla sfida, richiedendo anche l'accesso al server **V**

4: **TGS** fornisce a **C** il permesso di accesso a **V**

5: **C** si qualifica a **V**

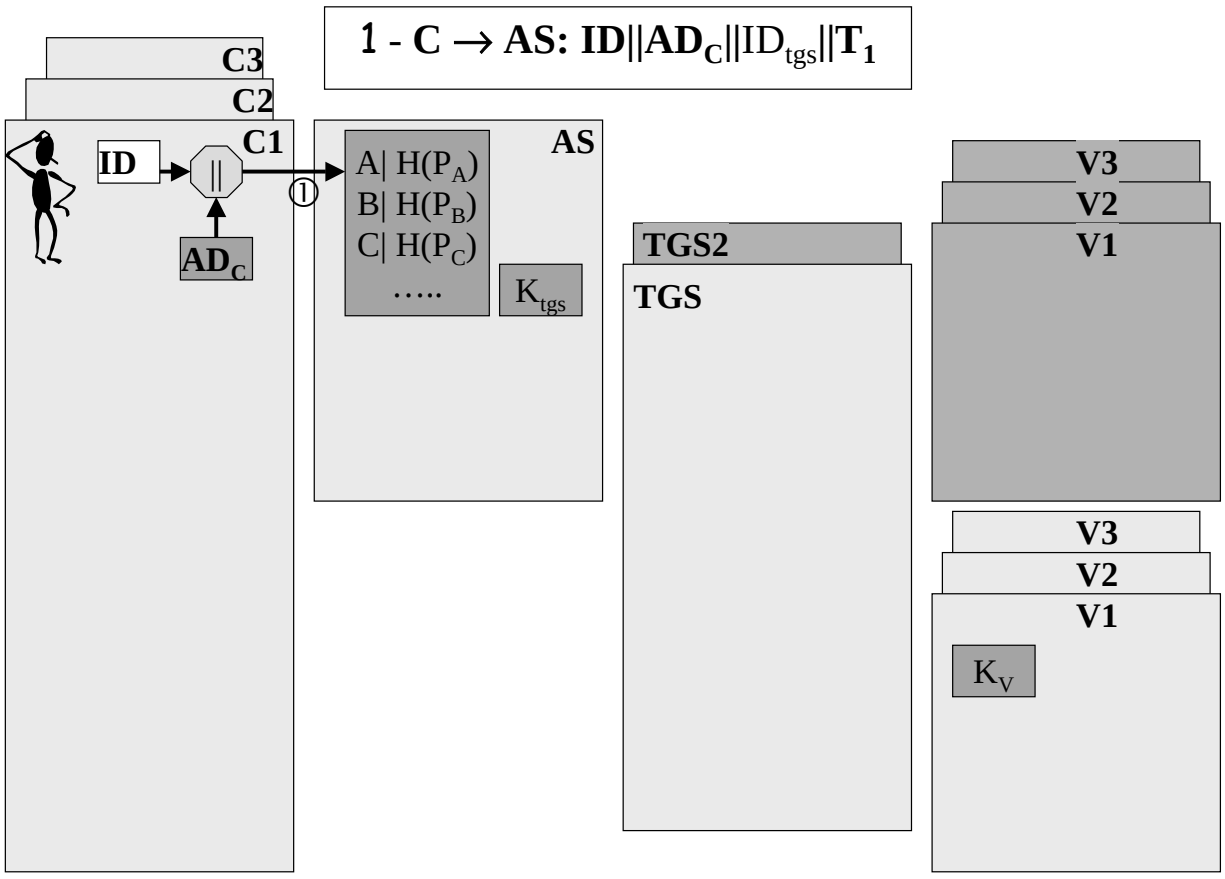
6: **V** si fa identificare da **C**

Svolgimento del servizio

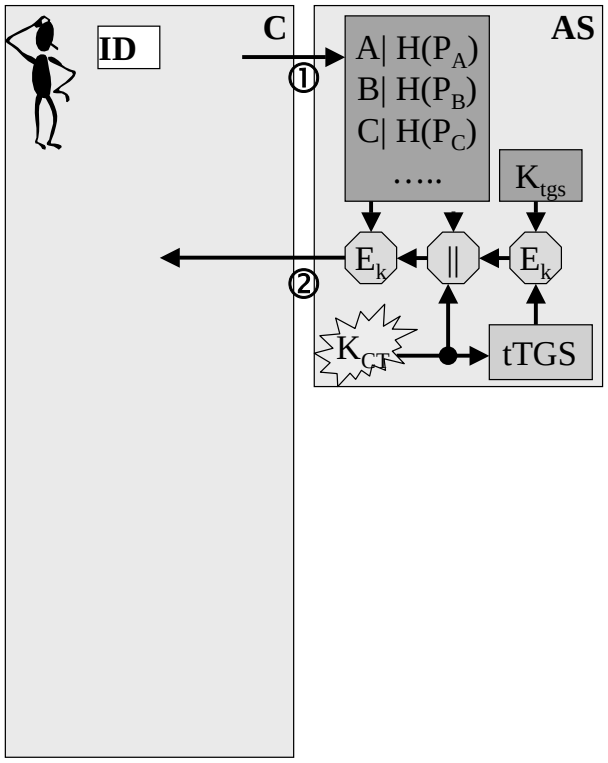
Successiva esigenza di servizio da V: **goto 5**

Accesso ad un nuovo server: **goto 3**

N: Fine della sessione o tempo scaduto

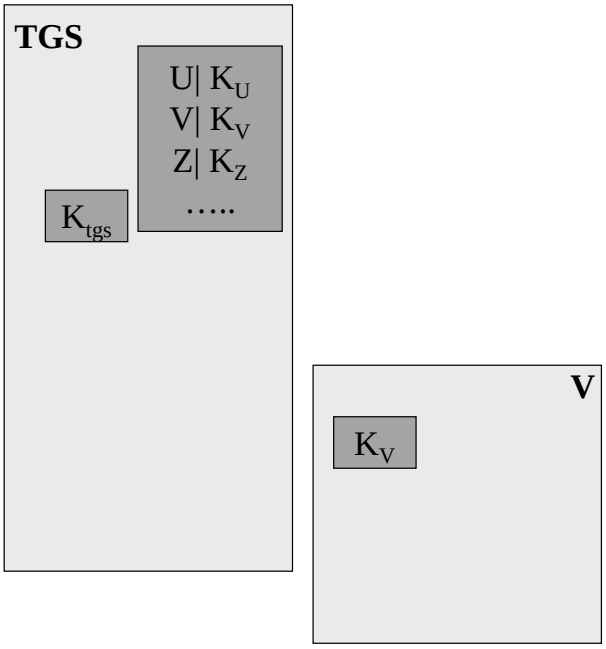


2 - AS → C: $E_{PSW}(K_{CT}||ID_{tgs}||T_2||\Delta T_2||ticketTGS)$

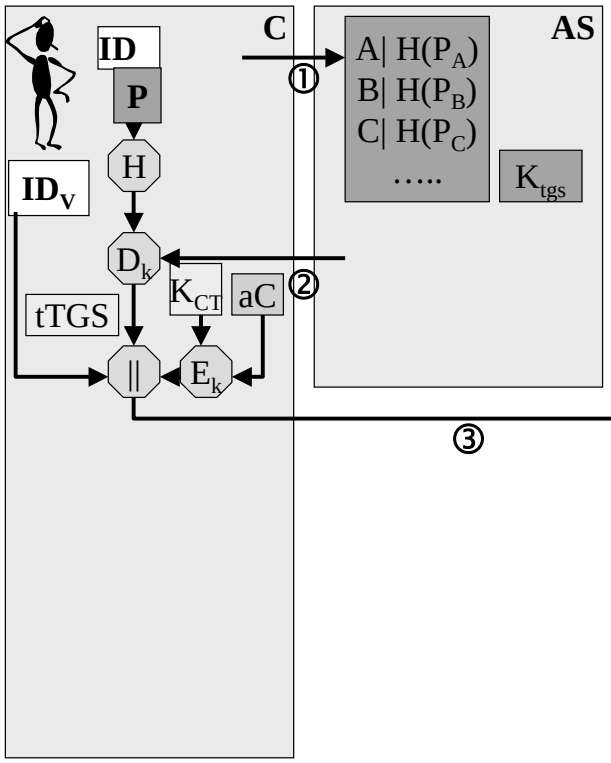


ticketTGS: E_{Ktgs}**(ticketTGS)**

ticketTGS: $K_{CT}||ID||AD_C||ID_{tgs}||T_2||\Delta T_2$

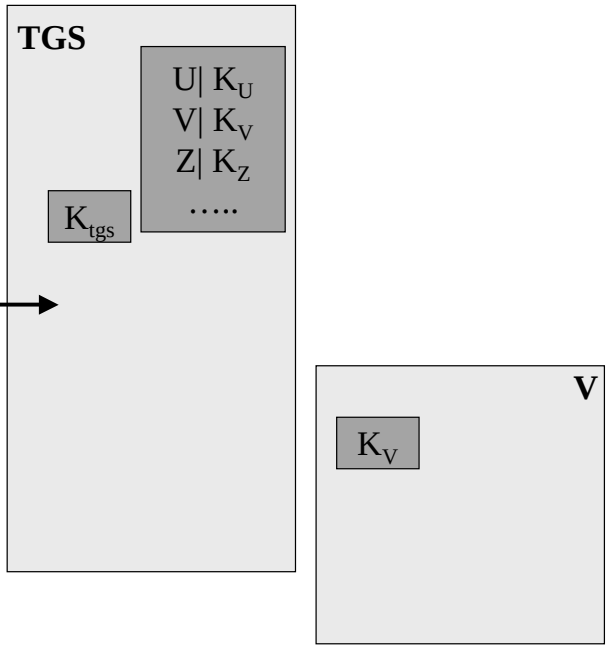


3 - C → TGS: $ID_V||ticketTGS||autenticatore_C$

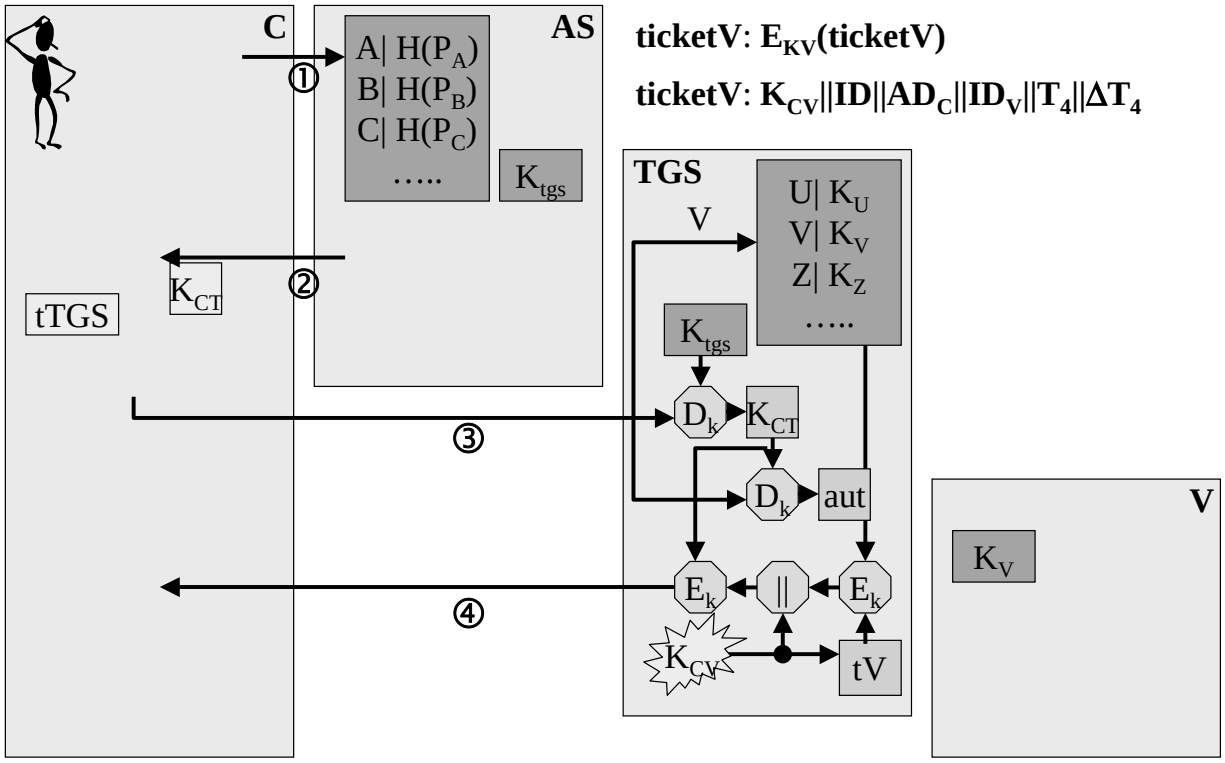


autenticatore$_C$: E_{KCT}(**autenticatore$_C$**)

autenticatore$_C$: $ID||AD_C||T_3$



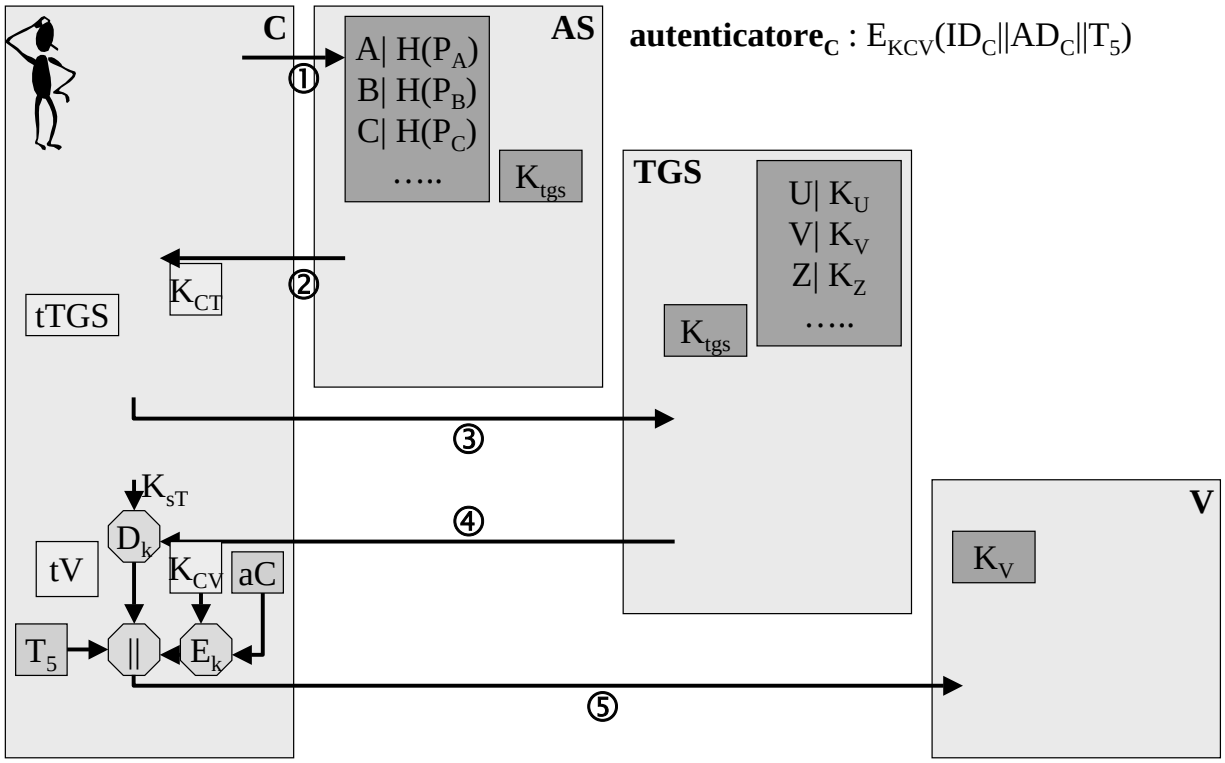
4 - TGS → C : $E_{KCT}(K_{CV}||ID_V||T_4||$ ticketV)



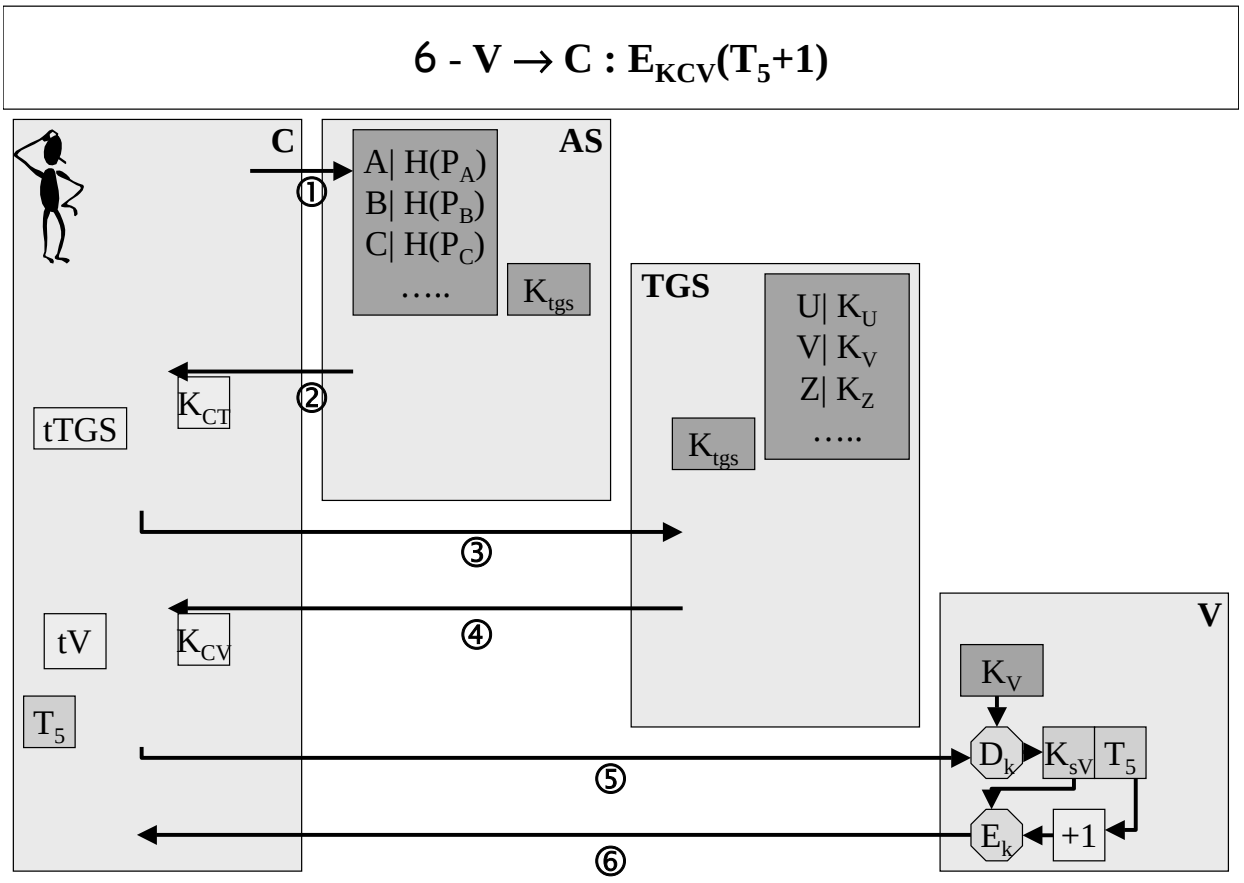
ticketV: E_{KV}**(ticketV)**

ticketV: $K_{CV}||ID||AD_C||ID_V||T_4||\Delta T_4$

5 - C → V: ticketV||$autenticatore_C$

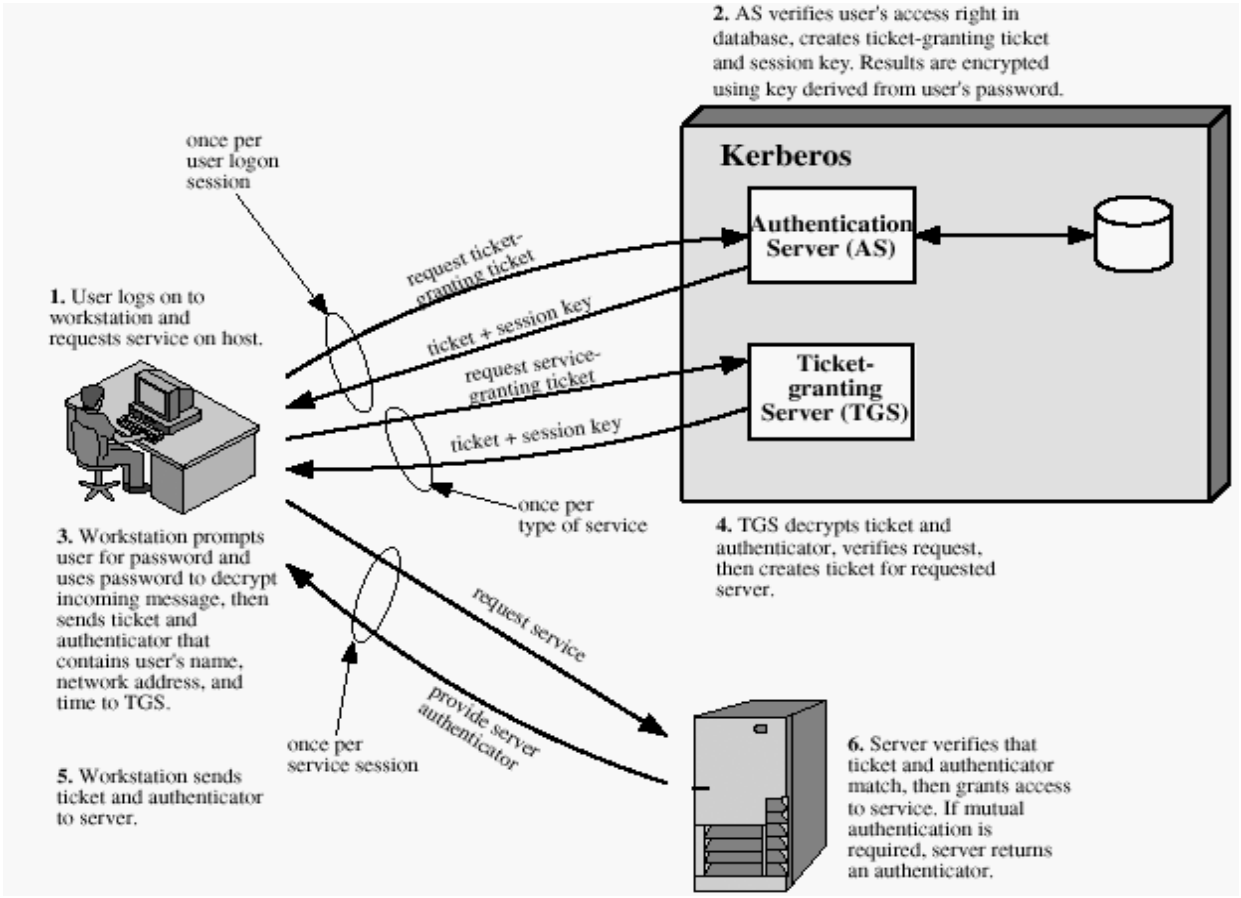


autenticatore$_C$: $E_{KCV}(ID_C||AD_C||T_5)$

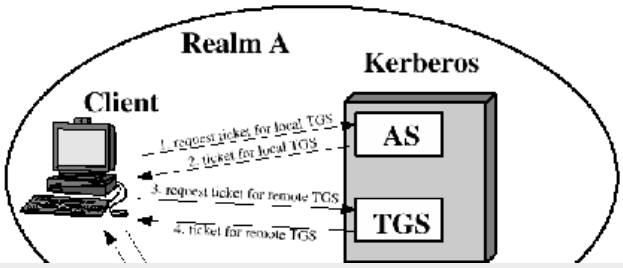


Version 4 Authentication Dialogue

- Problems:
  - Lifetime associated with the ticket-granting ticket
  - If too short → repeatedly asked for password
  - If too long → greater opportunity to replay
- The threat is that an opponent will steal the ticket and use it before it expires

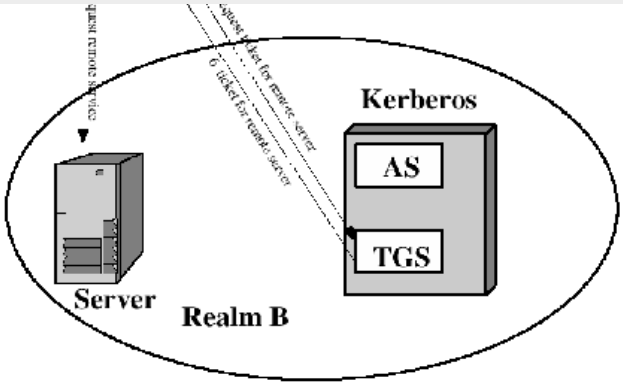


Request for Service in Another Realm



3 - $C \rightarrow TGS: ID_{TGSREM} || ticketTGS || autenticatore_C$

4 - $TGS \rightarrow C : E_{KCT}(K_{CTGSREM} || ID_{TGSREM} || T_4 ||$ ticketTGSREM)



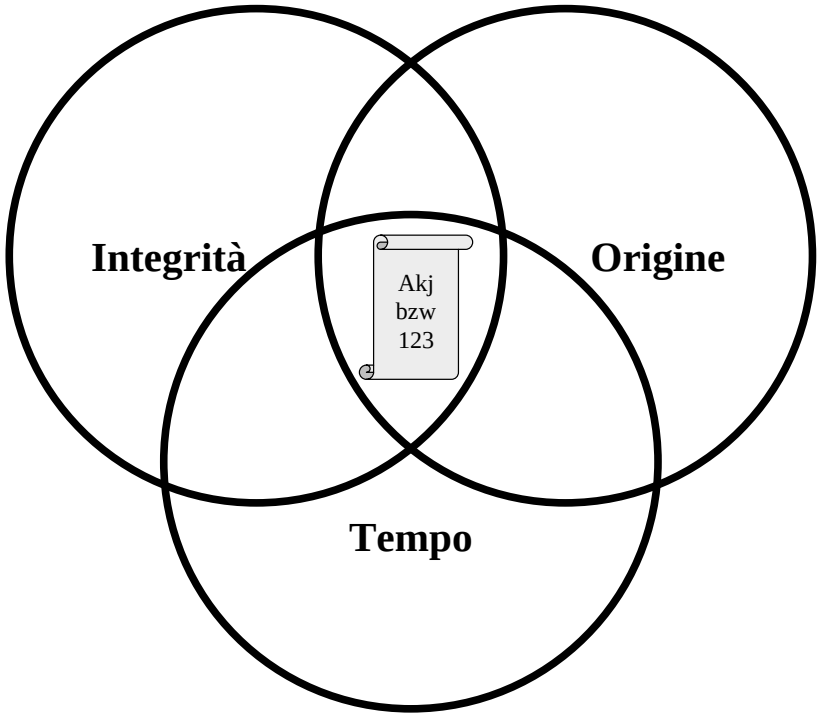
Vuoi imparare a progettare un servizio sicuro?

..leggere

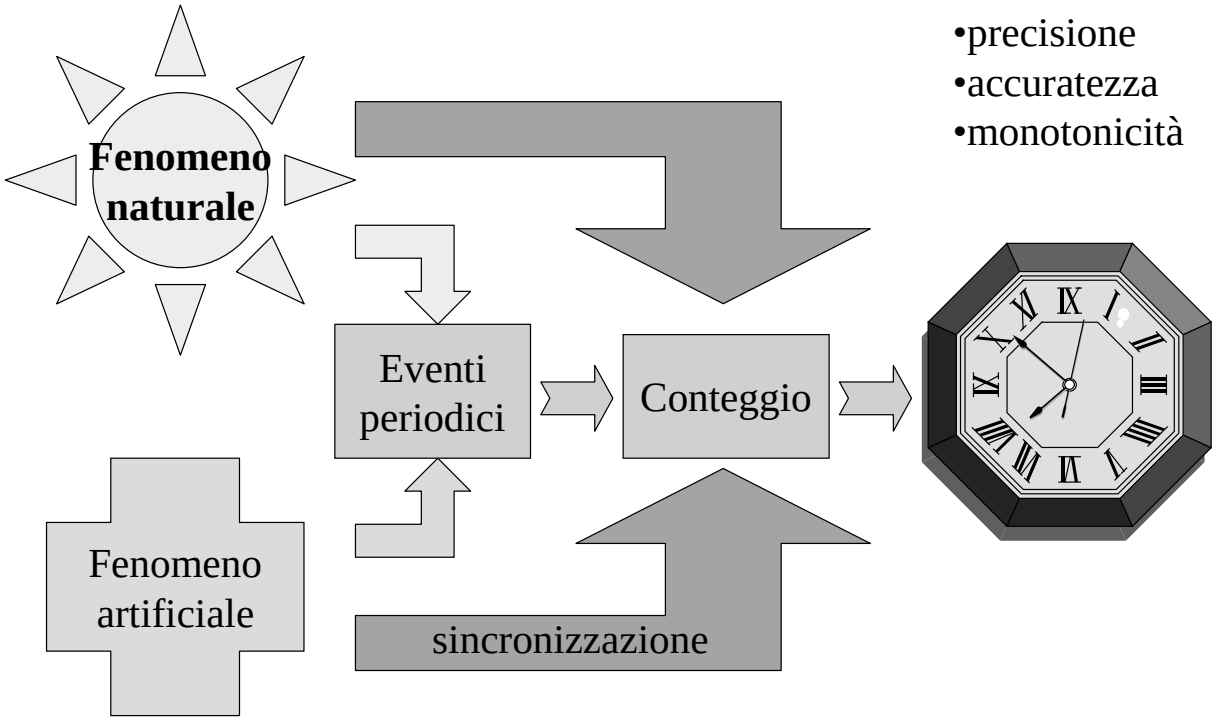
Bryant W. "*Designing an Authentication System: A Dialogue in Four Scenes*"

http://www.cert.org/annual_rpts/cert_rpt_98.html

Il documento informatico

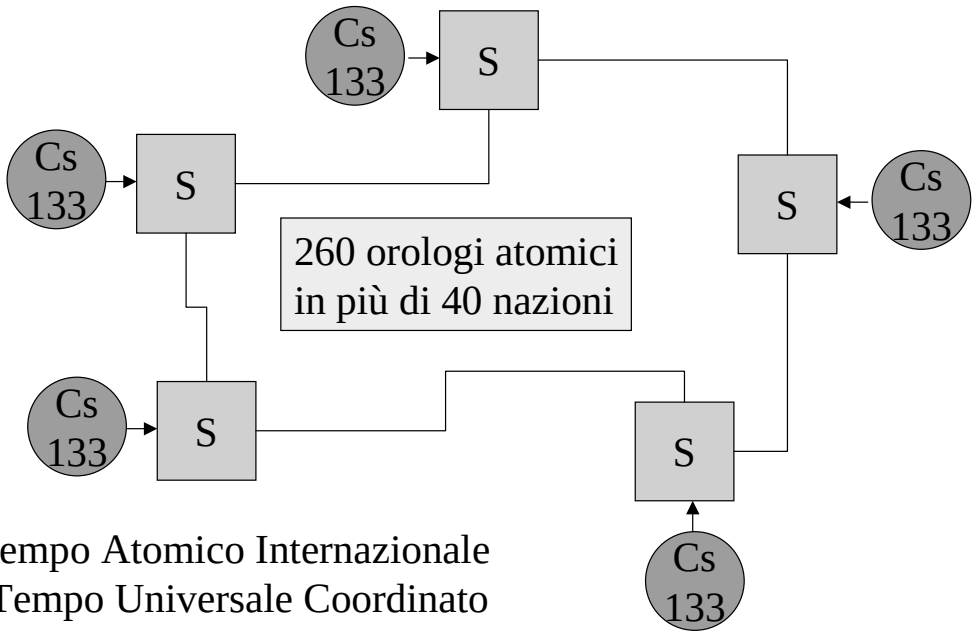


Misura del tempo



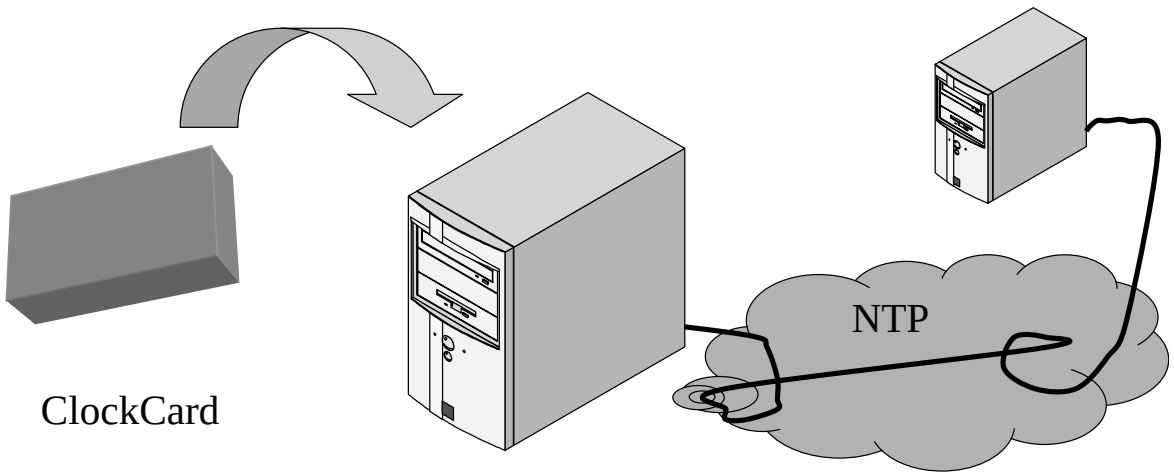
- precisione
- accuratezza
- monotonicità

Valore legale (TAI e UTC)



TAI: Tempo Atomico Internazionale
UTC: Tempo Universale Coordinato

Sincronizzazione dell'orologio del calcolatore



Marche temporali

•Messaggistica elettronica	nessun controllo
•File system, Database	monotonicità
•Applicazioni distribuite	sincronismo
•Certificato di chiave pubblica	verifica dell'intervallo
•Revoca e CRL	data/ora con grande precisione

Documento informatico + marca temporale
- collocazione temporale del testo
- validità della chiave di firma

TSS: Time Stamp Service

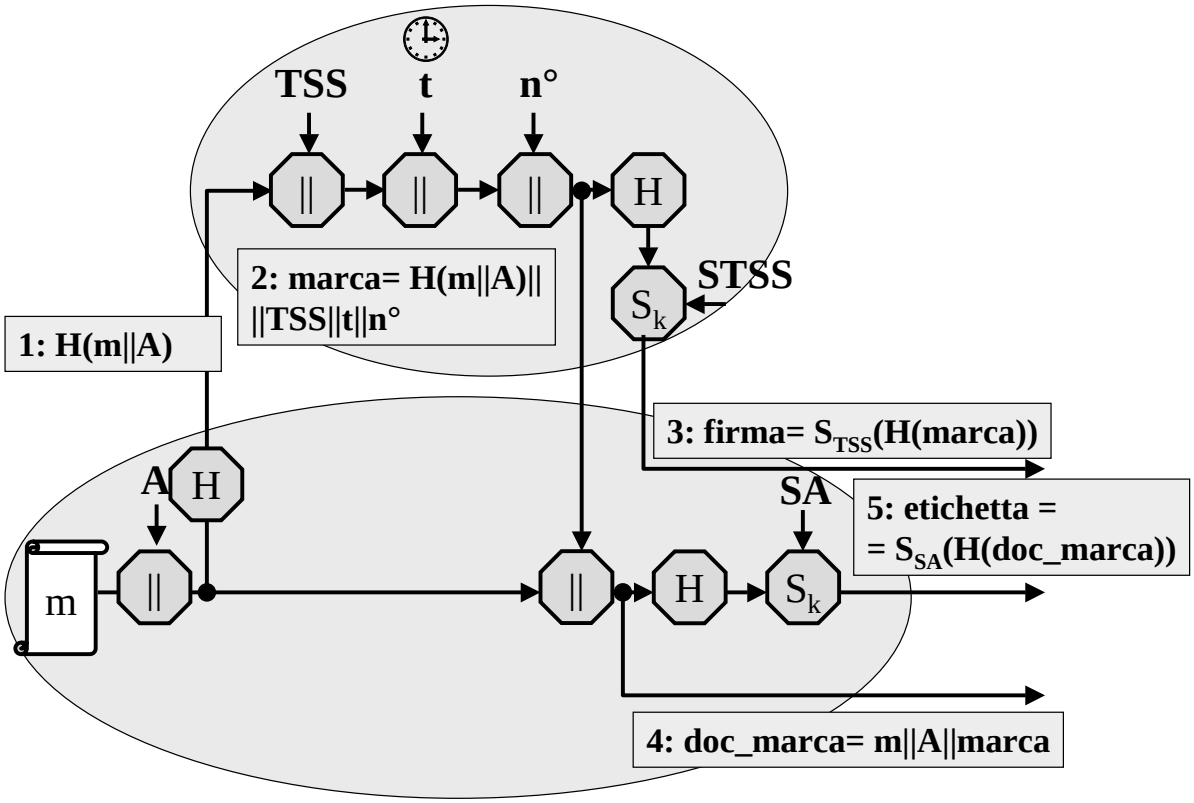
Sicurezza della marca temporale

- Il tempo della marca non deve essere falso — **Ente fidato**
- Tramite la marca deve essere possibile individuare in modo sicuro un documento, un istante ed un autore — **Firma digitale**
- La modifica anche di un solo bit di una marca deve poter essere rilevata
- Deve essere possibile farsi marcare documenti mantenendone riservato il contenuto

  — **Hash sicura**
- Chiunque deve poter sia farsi marcare i suoi documenti, sia verificare la marcatura dei documenti di chiunque altro — **Servizio pubblico**

Chiave di verifica sicura

Marcatura e firma di un documento



Problemi

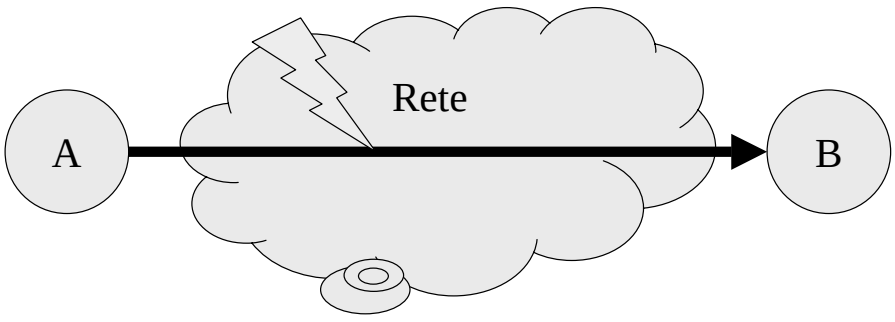
- PKIX: PKI&TSS
- efficienza
- vita della chiave/vita dei documenti
- fidatezza

- Nuovi standard?
- notarizzazione
- tempo relativo

FAQ: rete sicura

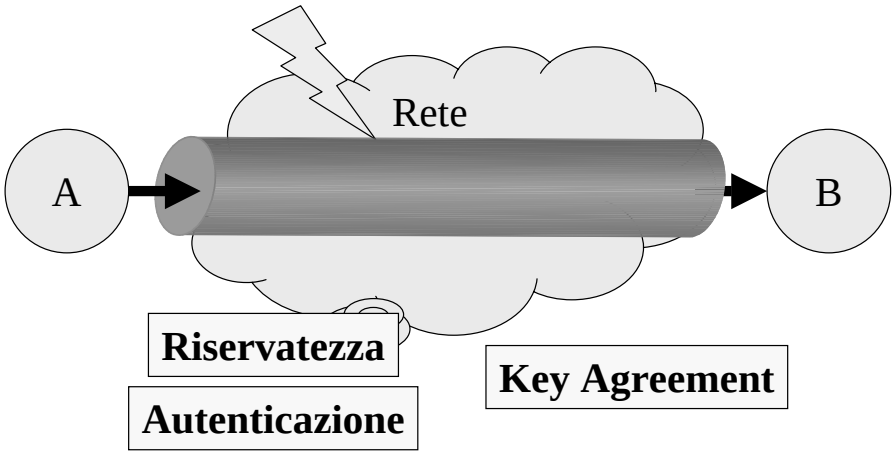
Che cosa sono IPSec e IPv6?
Che cosa sono AH e ESP?
Che cos'è il tunnel mode?
Che cos'è IKE?

IPv4



- **Packet sniffing**: lettura dei pacchetti in transito
- **IP spoofing**: falsificazione dell'indirizzo del mittente
- **Connection hijacking**: inserimento di dati nei pacchetti in transito
- **Clogging**: generazione di un carico oneroso di lavoro inutile

IPSec



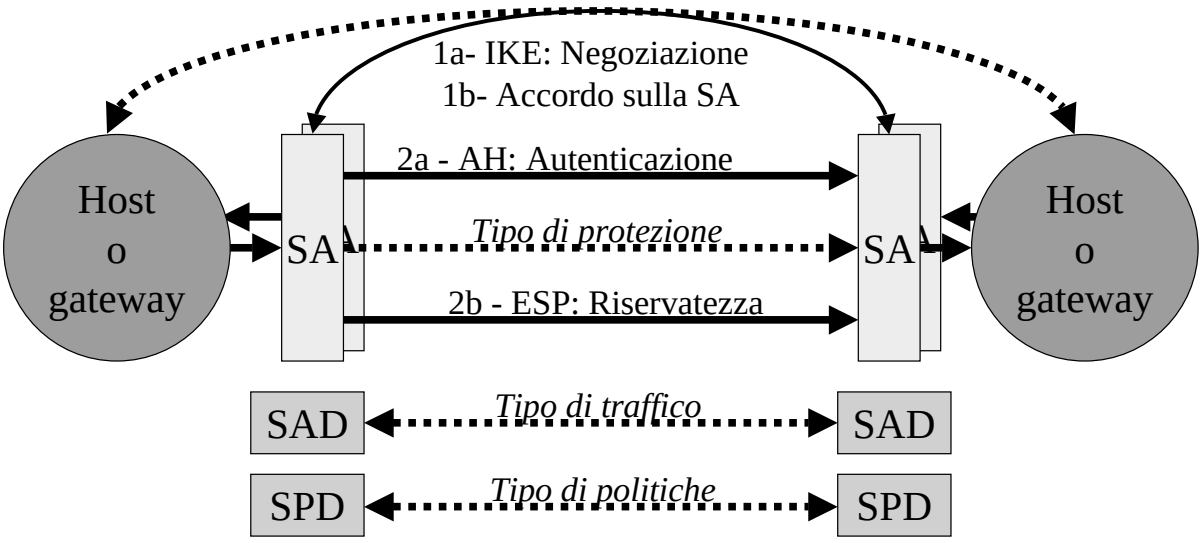
RFC 1636 (1994), RFC 2401, 2402,2406, 2408 (1998)

- Autenticazione
- Riservatezza
- Riservatezza & Autenticazione

Componenti di IPSec

IPSec è un'architettura per dare sicurezza al livello IP.
IPSec prevede:

- una suite di protocolli: IKE, AH, ESP
- un insieme di entità: SA, SAD, SPD



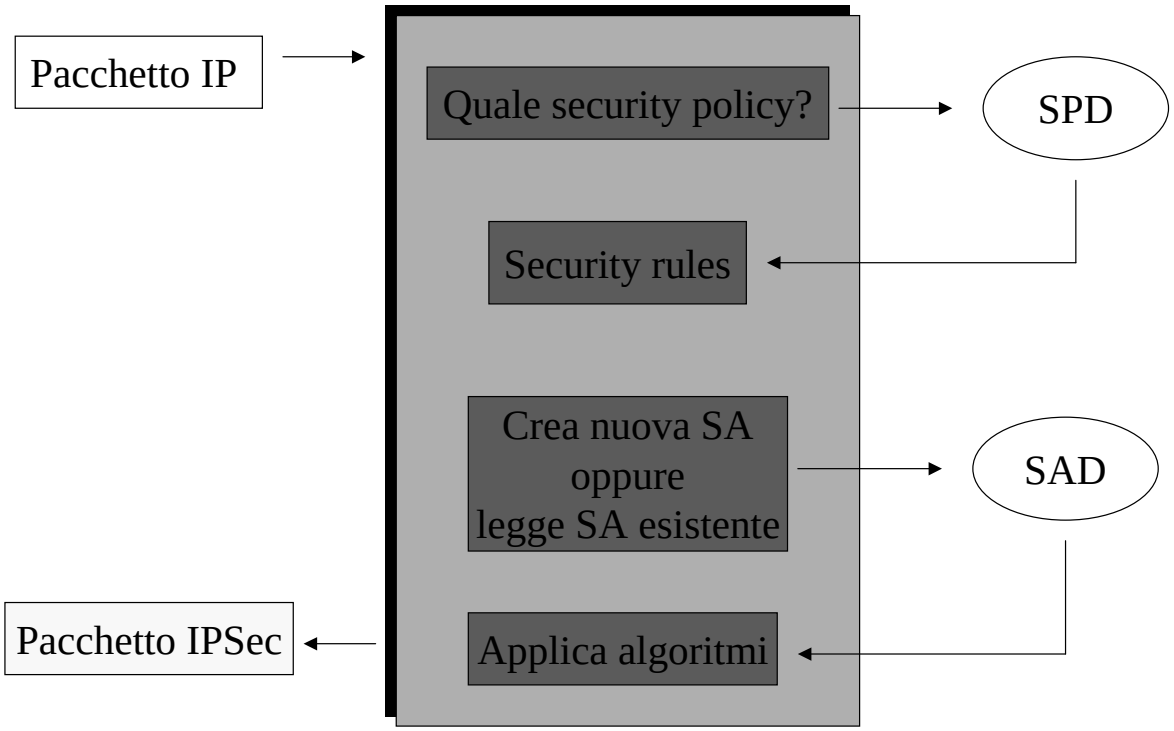
Gli elementi di IPSec

• **SPD(Security Policy Database)**: entità che esamina tutto il traffico IP, sia in ingresso che in uscita, per decidere quali pacchetti debbano usufruire dei servizi IPSec e per approntare di caso in caso il tipo di servizio più adatto.

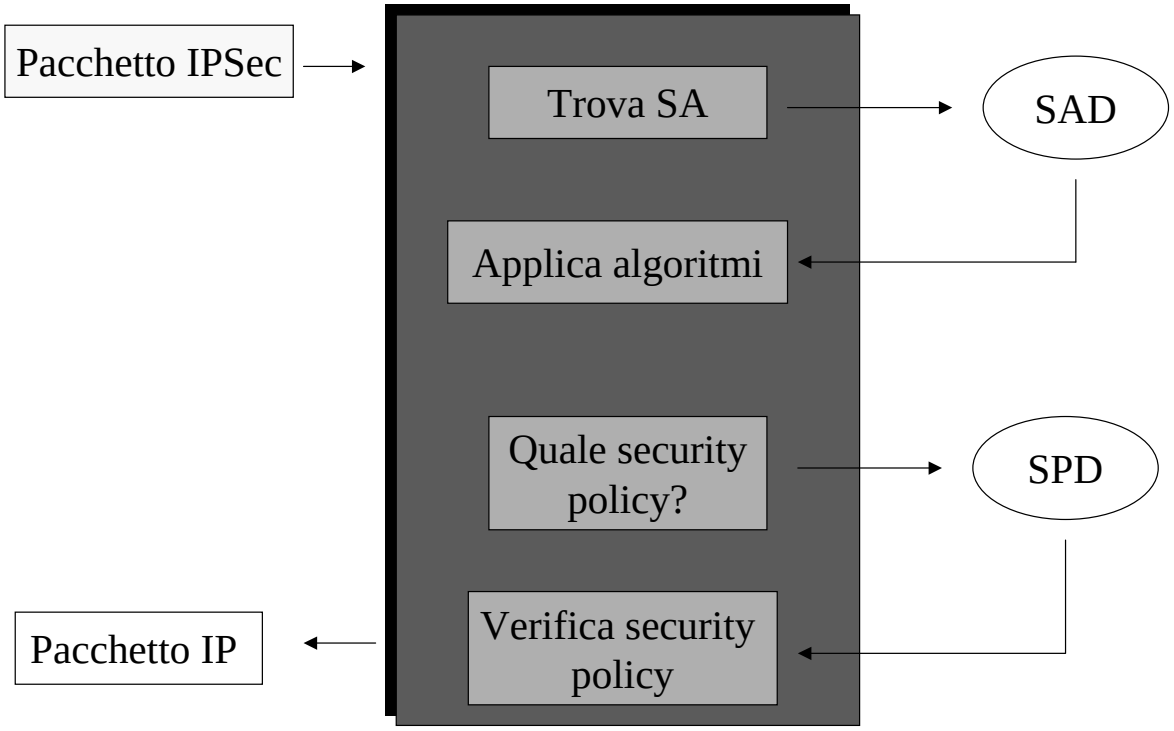
• **SAD(Security Association Database):** entità che tiene traccia di quale tipo di servizio sia stato espletato, in quale modo e dove siano stati indirizzati i pacchetti in questione.

• **SA(Security Association):** struttura che identifica in maniera univoca una connessione unidirezionale tra due interlocutori, specificando il servizio di sicurezza offerto con i relativi parametri(chiavi, algoritmi..)

Invio di un messaggio

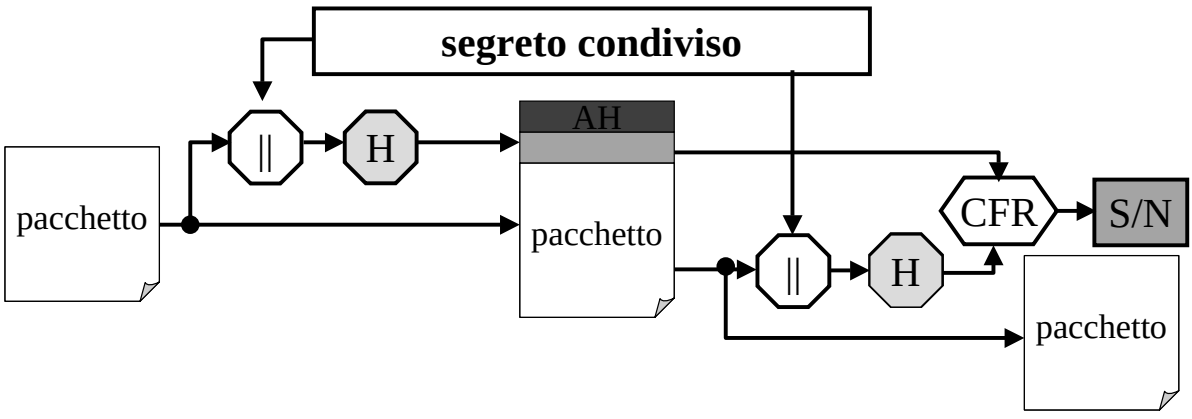


Ricezione di un messaggio



Il servizio per l'autenticazione (AH)

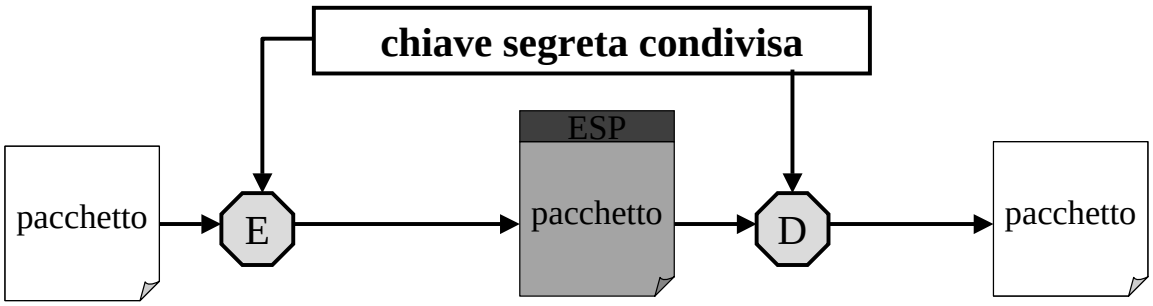
segreto → origine
hash → integrità



HMAC - MD5 96 bit
HMAC - SHA-1 96 bit
…….

Il servizio per la riservatezza (ESP)

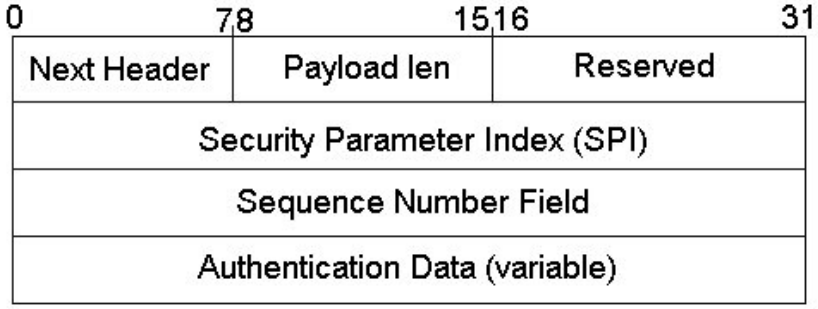
chiave → origine
cifrario → segretezza



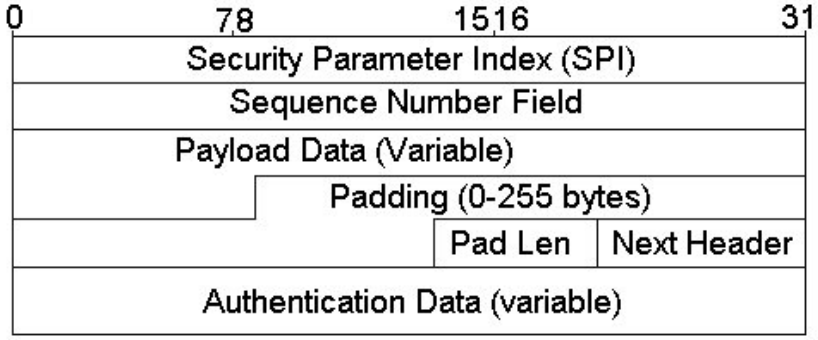
DES, TDES, IDEA,
RC5, CAST, Blowfish
…….

Intestazioni

AH (Authentication Header)



ESP (Encapsulating Security Payload)



Campi comuni

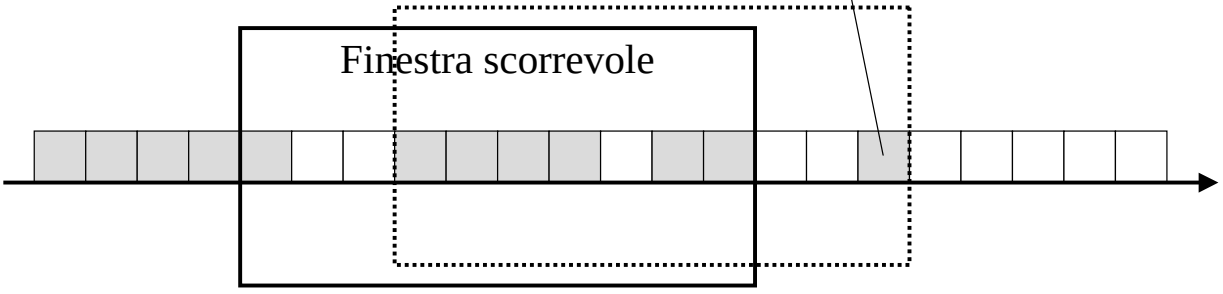
- **Security Parameter Index (SPI):** questo campo di 32 bit, insieme all'indirizzo IP di destinazione ed all'identificatore di protocollo, identifica in maniera univoca la SA relativa al datagramma.

- **Sequence number filed:** espleta il servizio di anti-replay tramite la numerazione progressiva dei datagrammi

- **Autentication Data:** contiene l'ICV (*Integrity Check Value)*, che consente di verificare l'integrità del pacchetto in fase di ricezione.

Servizio anti-replay

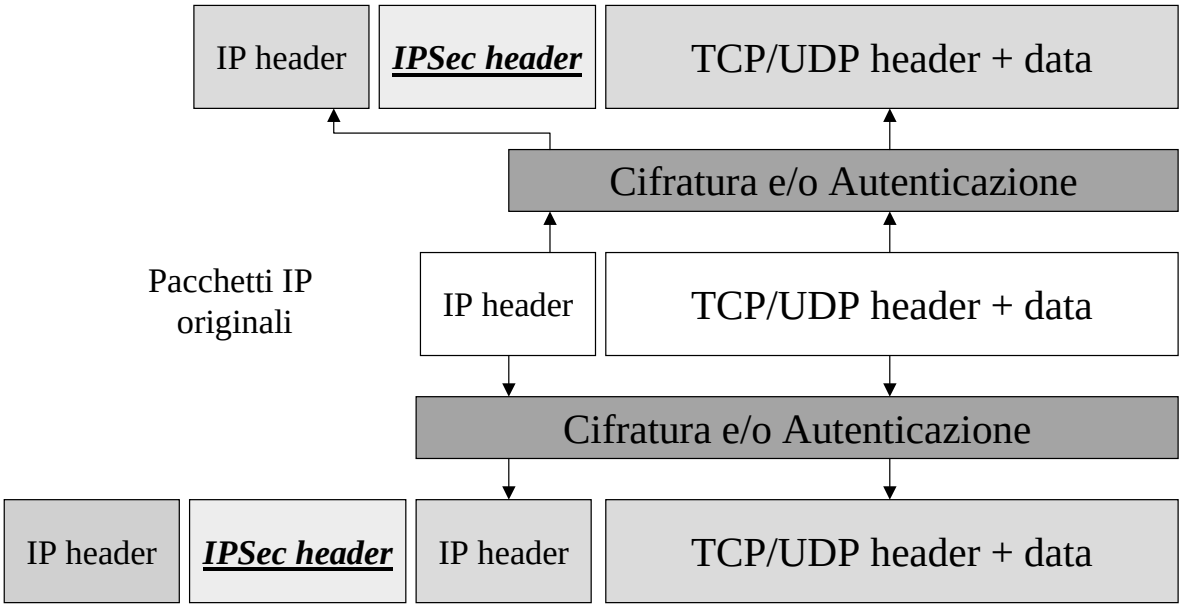
All'arrivo di ogni nuovo pacchetto valido, la destinazione lo marca e sposta la finestra in modo da disporlo all'estremità destra



Lunghezza di default della finestra: 64 pacchetti

Trasporto e Tunnel

Pacchetti IPSec con SA in modalità **trasporto**



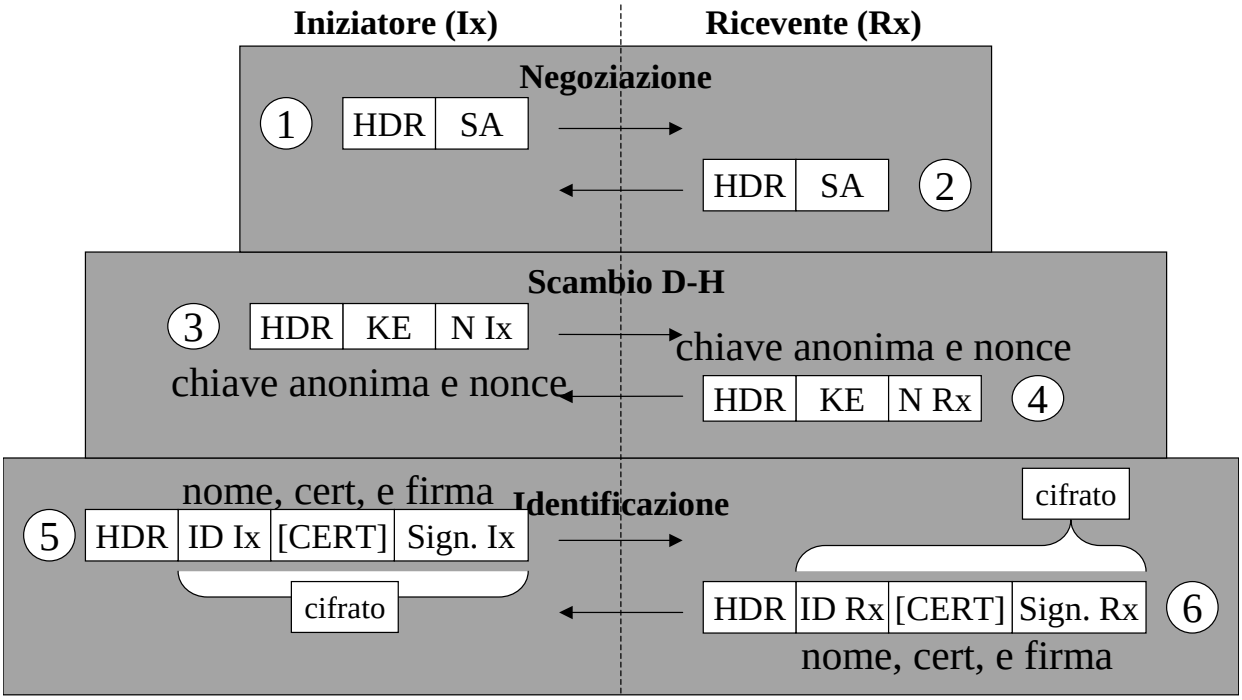
Pacchetti IPSec con SA in modalità **tunnel**

Protocollo IKE

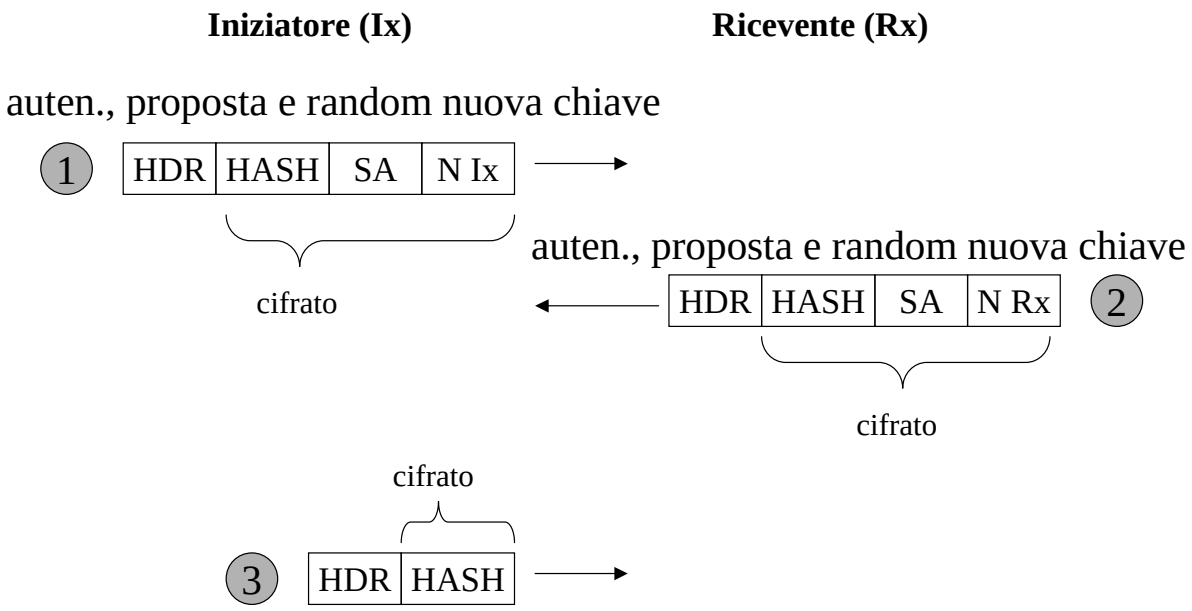
IKE (Internet Key Exchange): meccanismo con cui due interlocutori possono accordarsi sui parametri relativi ad una SA (creazione, cancellazione, AH o ESP, ecc.).

- **ISAKMP**
- **Oakley**
- **Scheme**

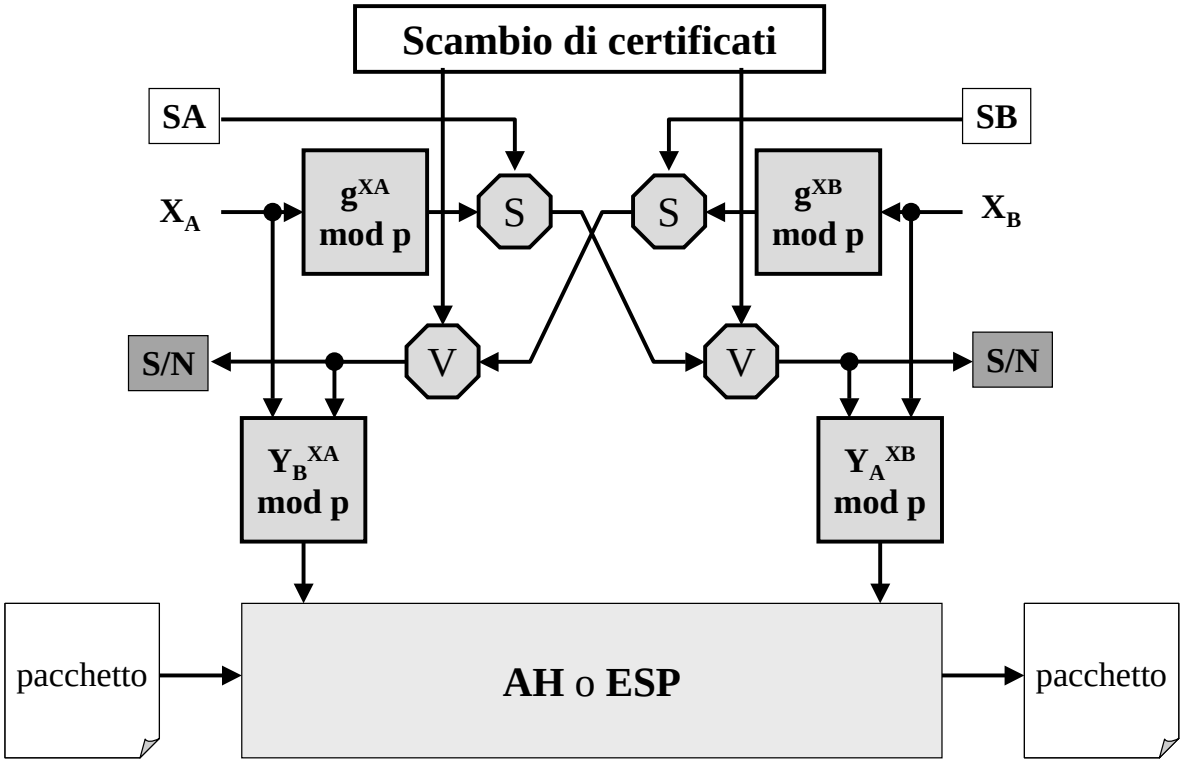
IKE fase 1: ISAKMP SA



IKE fase 2: creazione di una SA



Condivisione del segreto: Oakley



IKE: anonimato ed identificazione