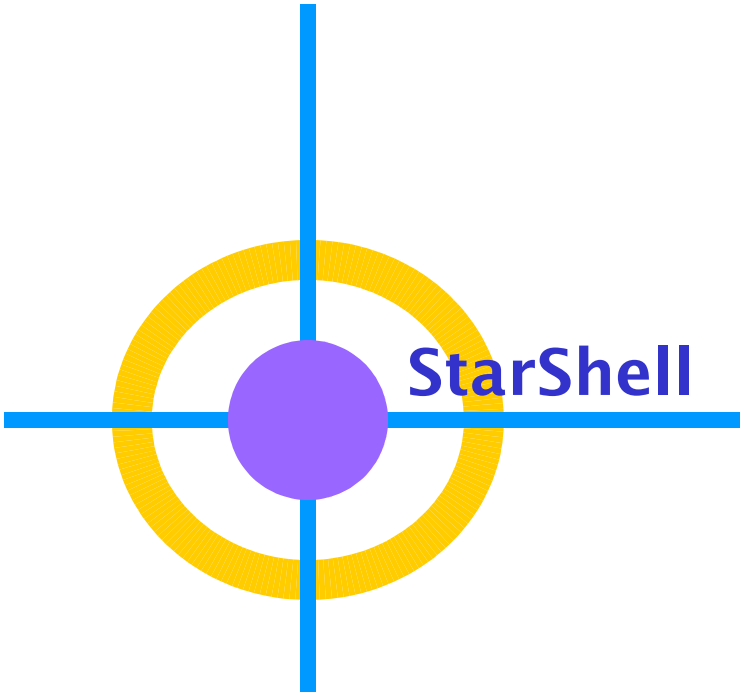


Autenticazione

Autenticazione

- Verifica dell'identità di qualcuno (utente) o qualcosa (host) in un contesto definito
- Componenti:
  - **Oggetto dell'autenticazione**
  - **Autenticatore**
  - **Informazione di autenticazione**
  - **Funzione di autenticazione F**
    - **F(informazione di autenticazione) = risultato previsto**
- Schemi:
  - **Two-Party Authentication**
  - **Trusted Third-Party Authentication**
- Pericoli:
  - **Divulgazione dell'informazione di autenticazione**
  - **Contraffazione dell'informazione di autenticazione**

Two-Party Authentication

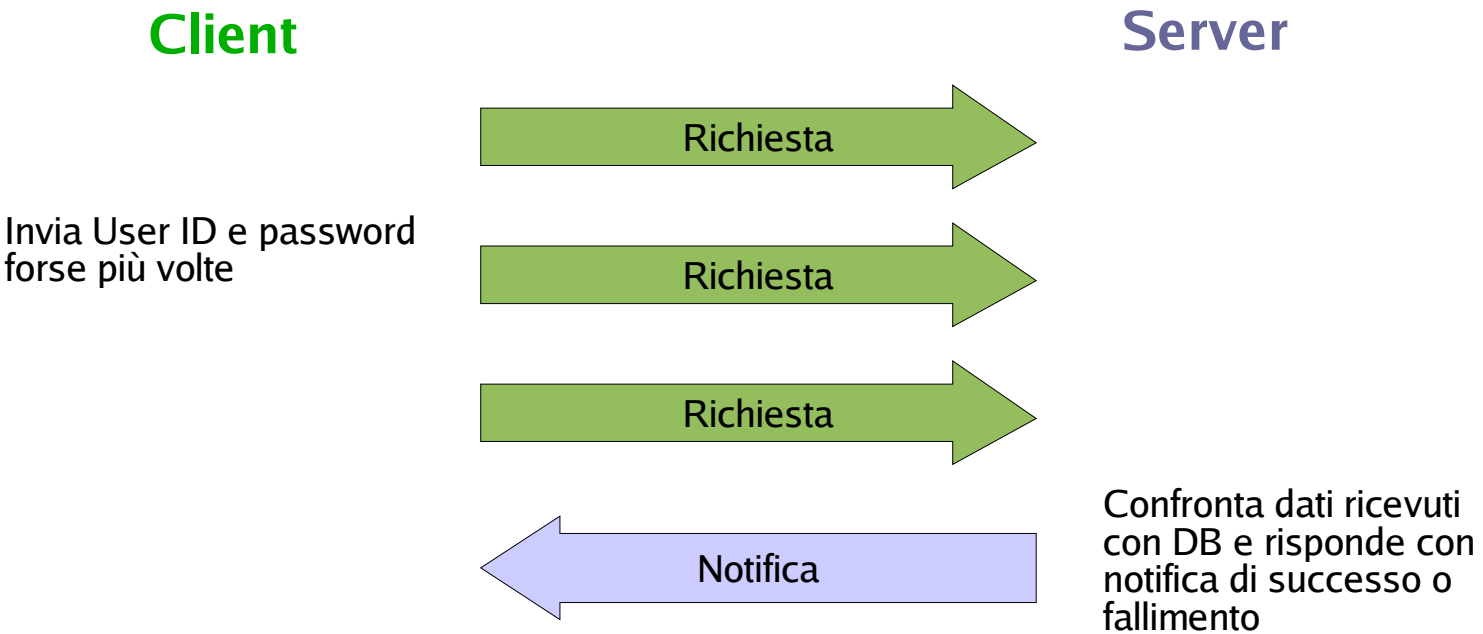
- Schemi a una via o due vie (autenticazione reciproca)
  - **Ccombinazione di due schemi a una via distinti**
- Segreto condiviso: conosciuto da entrambi i pari
  - **Citato direttamente (password e simili)**
  - **Informazioni che possono essere derivate dal segreto condiviso (challenge-response, chiavi doppie, ecc.)**
- L'informazione di autenticazione può essere:
  - **Statica (password fissa)**
  - **Dinamica (one-time password)**
- Problema di distribuzione dell'informazione di autenticazione
- Scambio dell'informazione su un canale di comunicazione
- Svantaggio: con N enti scala come N(N-1)

Password

- Difficili da ricordare
  - **Attacchi di Ingegneria Sociale**
- Possono essere indovinate
  - **Attacco di forza bruta**
  - **Attacchi basati su dizionario**
  - **Analisi del traffico**
- Contromisure:
  - **Lunghezza e complessità minime**
  - **Stringhe di “sale” per aumentare l'entropia**
  - **Numero massimo di tentativi e ritardi di retry**
- Devono essere registrate su disco
  - **Uso di hash non invertibili**
- Possono essere intercettate in transito
  - **Eliminare reti broadcast**
  - **Cambiamento frequente**

PAP

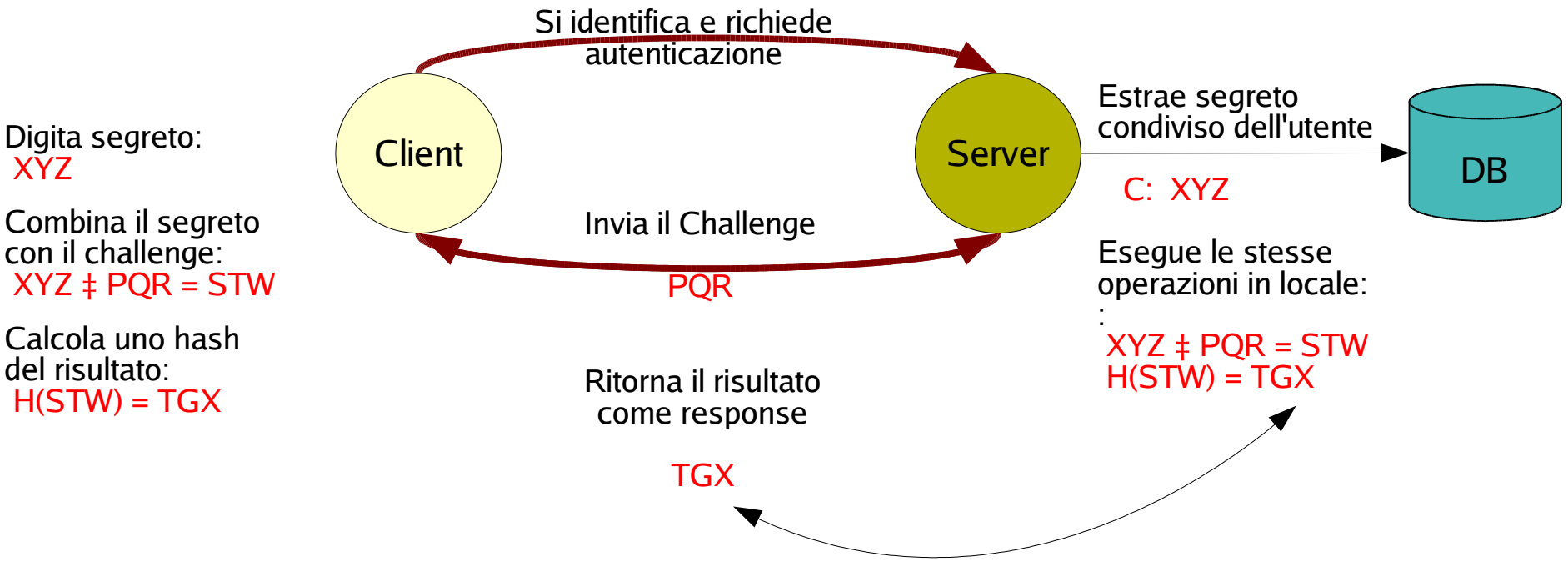
- Password Authentication Protocol
  - **Password inviate in chiaro**
  - **Sicurezza dipende da previa crittografazione del canale trasmissivo**



Altri Metodi

- Protocolli di Challenge-Response
  - **L'utente non deve citare la password, ma dimostrare di conoscerla**
  - **P. es. CHAP, APOP**
- One-Time Passwords
  - **Liste pre-distribuite, uso singolo**
  - **P. es. OTP, S/Key**
- Token Cards
  - **Generate da un dispositivo, sembrano casuali**
  - **Algoritmo di generazione è noto solo ad autenticato e autenticatore**
  - **Combinate con PIN di accesso al dispositivo**
  - **P. es. SecurID, RSA Security**
- Smartcards
  - **Ausilio alla conservazione dei dati necessari agli schemi precedenti**

Protocolli di Challenge-Response

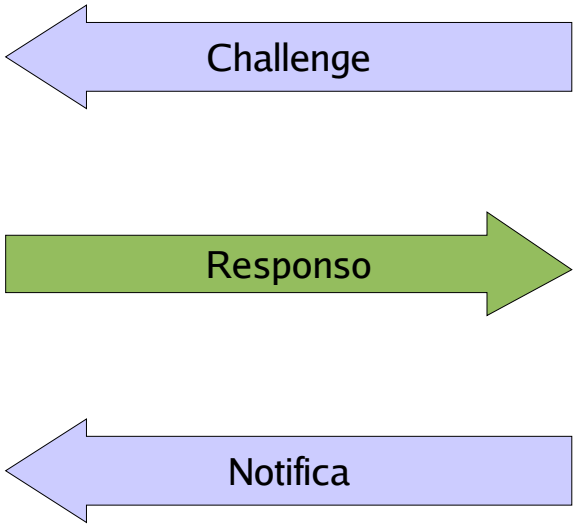


Componenti:
- algoritmo di combinazione (facoltativo)
- algoritmo di hash

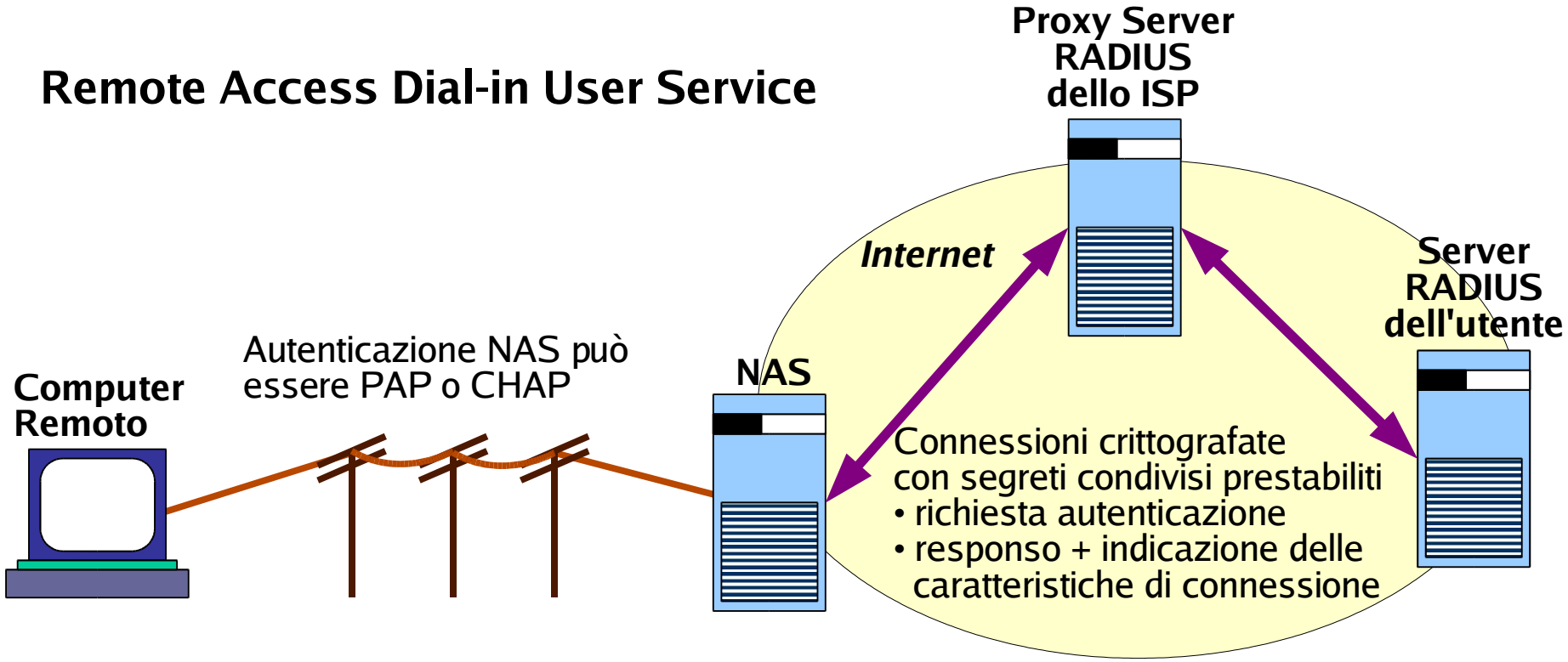
CHAP

- Challenge Handshake Authentication Protocol
  - **Password mai inviate in chiaro**
  - **Eventuale intercettazione di challenge e response non è utilizzabile dall'attaccante**

Client **Server**

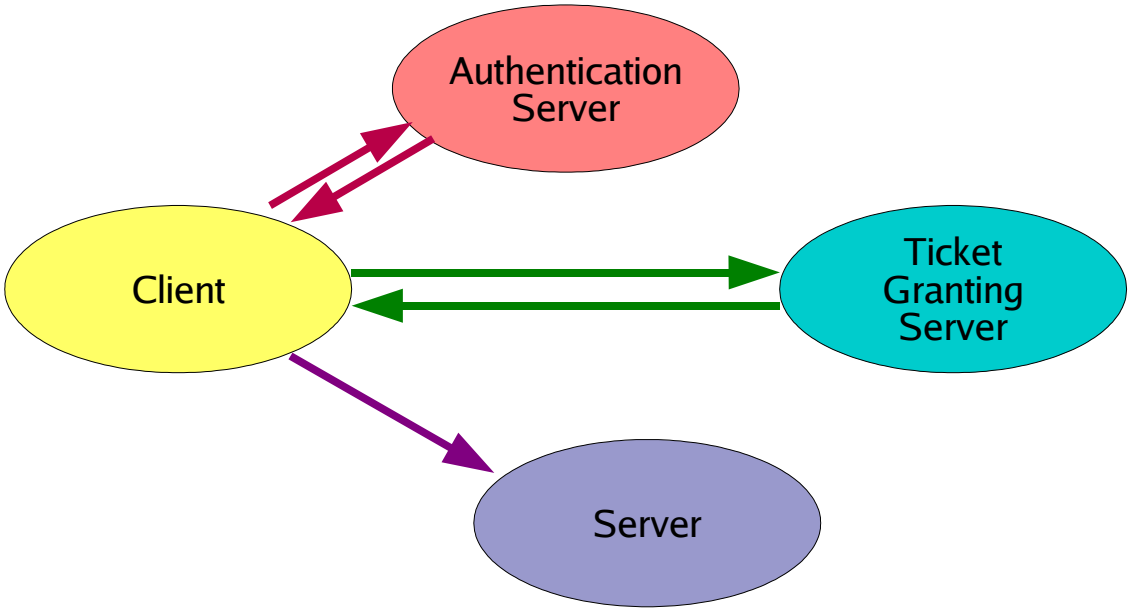


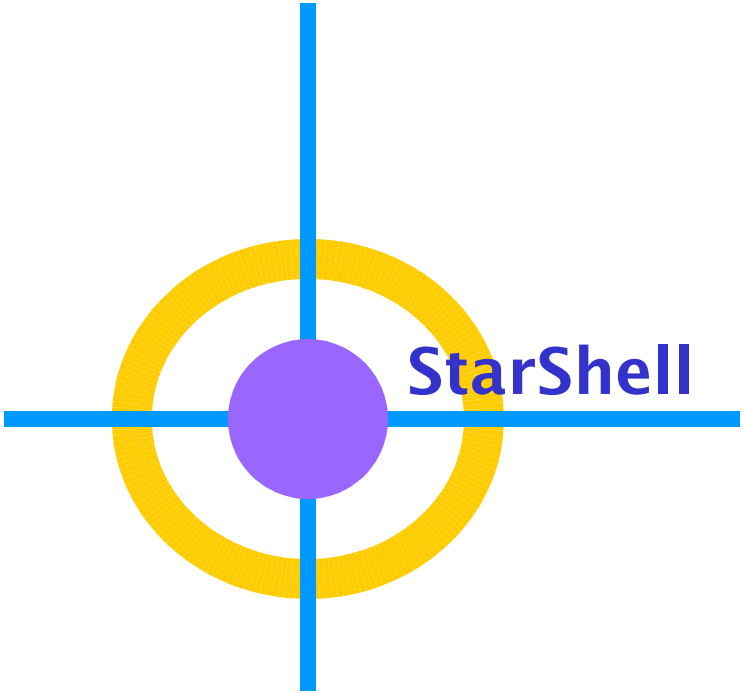
RADIUS


Remote Access Dial-in User Service
Proxy Server
RADIUS
dello ISP
Internet
Server
RADIUS
dell'utente
Autenticazione NAS può
essere PAP o CHAP
Computer
Remoto
NAS
Connessioni crittografate
con segreti condivisi prestabiliti
• richiesta autenticazione
• responso + indicazione delle
caratteristiche di connessione

Trusted Third-Party Authentication

- Kerberos
  - **Entità da autenticare: host, client e risorse (principals)**
  - **Authentication Server ha il database dei principals**
  - **Accesso tramite consegna di ticket e uso di chiavi di sessione**
  - **Ticket distribuiti dal Ticket Granting Server**
    - **Due fasi di autenticazione**




StarShell