Autenticazione Forte

…e uso delle carte

...autenticazione forte

- Challenge and Response (Sfida e risposta)
  - Basato su chiavi segrete e su una funzione unidirezionale
  - Lo scopo è stabilire indirettamente che l'utente possiede la chiave (senza rivelarla)
  - Il claimant prova la sua identità al verifier rispondendo ad un challenge (un numero casuale e segreto)

...Challenge-Response...

- Protocolli di identificazione basati sul Challenge-Response, tecniche:
  - A chiave simmetrica
  - A chiave pubblica
  - Zero-knowledge

Challenge and Response

- Si fa uso dei parametri time-variant
  - Servono per prevenire attacchi
  - Per garantire unicità e tempestività (timeliness)
  - Per distinguere istanze (nonce)
  - Abbiamo tre classi:
    - Random number
    - Sequence number
    - Timestamp

Parametri Time-Variant...

- Otteniamo tempestività usando:
  - Random number come challenge-response
  - Timestamp se con timeclock distribuiti
  - Sequence number, mantenendo informazioni sul claimant-verifier

...parametri Time-Variant...

- Requisiti di unicità o tempestività garantiti:
  - Direttamente: con i random number
  - Indirettamente: tramite serial number o grazie al timeclock

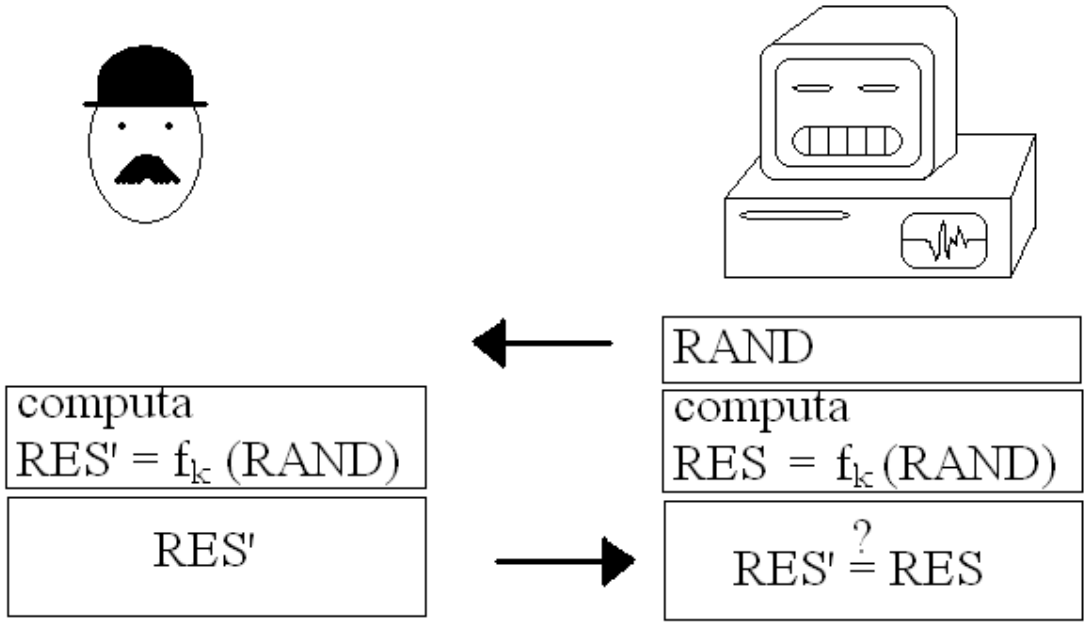
...parametri Time-Variant...

- Identifichiamo un messaggio come unico:
  - Grazie al nonce da sequenze crescenti monotoniche
    - Con timestamp o sequence number
  - Con random number
    - Ad entropia sufficiente

...parametri Time-Variant

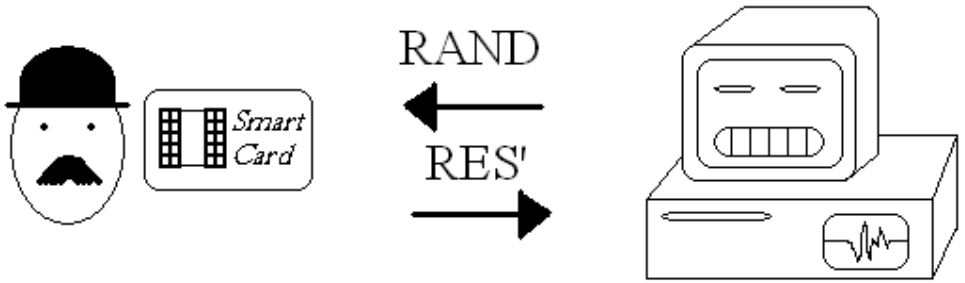
- Possono essere combinati:
  - Per garantire la non duplicazione di uno pseudonumber

Random numbers



...random numbers

- Per non fare usare un algoritmo all'utente ci affidiamo alle schede



...random numbers

- Svantaggi
  - Se si usano generatori pseudocasuali è richiesta un entropia sufficiente
  - Quando è usato un numero casuale, il protocollo necessita di un messaggio addizionale, e vanno mantenute informazioni di stato, fino a verifica effettuata

Sequence numbers

- Possono essere numeri di serie
- Sono usati come identificatore del messaggio
- Solitamente usati per coppie di entità
- Cè una politica predefinita per la numerazione

...sequence numbers

- Svantaggi:
  - Ogni claimant deve memorizzare le informazioni di stato di ogni verifier

Time Stamps

- Al messaggio originale viene legato una stampa del clock
- Ricevuto il messaggio si fa una stampa del clock
- Si sottraggono i due valori, è valido in uno dei due casi:
  - La differenza rientra in un intervallo di tempo prefissato
  - Nessun messaggio con lo stesso timestamp era stato ricevuto da quel mittente

...time stamps...

- Svantaggi:
  - Bisogna mantenere una lista dei timestamp precedenti
  - È necessario che i clock siano sincronizzati

...time stamps

- Confronto rispetto gli altri time-variant:
  - Nel timestamp vengono usati pochi messaggi (uno)
  - Nel timestamp non è necessario memorizzare:
    - Informazioni di stato long-term (sequence number)
    - Informazioni di stato short-term (random number)
  - Necessita di una sincronizzazione sicura dei clock
  - Tipicamente viene rimpiazzato da un random number challenge con aggiunto un messaggio di ritorno

Challenge-Response

- Tre tipi di challenge-response:
  - Basato su tecniche a chiave simmetrica
    - Simmetric-key encryption
    - One-way function
    - Hand-held passcode generator
  - Basato su tecniche a chiave pubblica
    - Decrittaggio a chiave pubblica con witness
    - Needham-Schroeder PK modificato
  - Basato sullo schema della firma digitale

Challenge-response con tecniche a chiave simmetrica

- Claimant e verifier condividono una chiave simmetrica
- Per piccoli sistemi chiusi si condivide una chiave a priori
- Per sistemi più grandi si usa un trusted server
  - Il server funziona come un hub di una spoked wheel
- Tre tecniche principali
  - 1 - Simmetric-key encryption
  - 2 - One-way function
  - 3 - Hand-held passcode generator

1 - Simmetric-key encryption

- Vediamo tre tecniche basate sul ISO/IEC 9798-2
  - Assumono l'esistenza di una chiave segreta condivisa
  - Il claimant dimostra la propria identità crittando un challenge

...simmetric-key encryption

- Tre semplici tecniche fondamentali
  - Autenticazione unilaterale, basata sul timestamp
  - Autenticazione unilaterale, usando random numbers
  - Mutua autenticazione, usando random numbers
- Notazione:
  - r_a: random number
  - t_a: timestamp
  - E_k: algoritmo di crittaggio simmetrico (k condivisa)
  - *: campi opzionali

...simmetric-key encryption

1. autenticazione unilaterale, con timestamp

$$A \dashrightarrow B: \; E_k (t_a, B^*)$$

...simmetric-key encryption

2. autenticazione unilaterale, con random numbers

$$A \leftarrow\!\!- B: r_B$$
$$A \dashrightarrow B: E_k (r_B, B^*)$$

Challenge-response: chiave simmetrica

...simmetric-key encryption

3. autenticazione mutua, con random numbers

$$A \leftarrow\!\!- B: r_B$$
$$A \dashrightarrow B: E_k (r_A, r_B, B^*)$$
$$A \leftarrow\!\!- B: E_k (r_B, r_A)$$

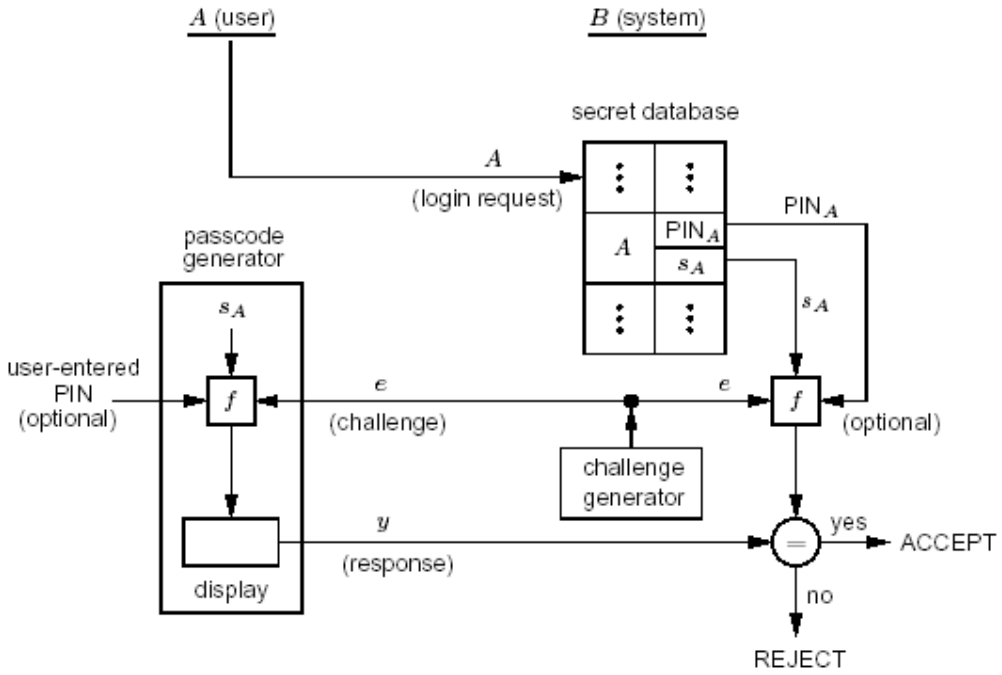
2 - funzioni unilaterali

- L'algoritmo di crittaggio può venire rimpiazzato da una funzione one-way (o non reversibile) della chiave condivisa e del challenge
  - Es: avendo proprietà simili al MAC
  - Preferibile in alcune situazioni
    - L'algoritmo può essere non voluto o non desiderabile

...funzioni unilaterali

$$A \leftarrow\!\!- B: r_B$$
$$A \dashrightarrow B: r_A, h_K(r_A, r_B, B)$$
$$A \leftarrow\!\!- B: h_K(r_B, r_A, A)$$

3 - hand-held passcode generator



Challenge-response: chiave simmetrica

...hand-held passcode generator

- Schema dell'hand-held
  - Il generatore mostra un passcode
  - L'utente dà una risposta
  - Il sistema verifica
- La risposta può dipendere da un PIN

...hand-held passcode generator

- Svantaggi:
  - Se si usano password vanno memorizzate nel sistema

Challenge-response tramite tecniche a chiave pubblica

- Il claimant dimostra di conoscere la sua chiave:
  - Decrittando un challenge crittato con chiave pubblica
  - Oppure firmando digitalmente un challenge
- Per combattere gli attacchi si incorpora un generatore casuale di numeri (confounder)

...challenge-response a chiave pubblica...

- Due tipi:
  - Basato sul decrittaggio della chiave pubblica
    - Con testimone
    - Needham-Schroeder PK modificato
  - Basato sulla firma digitale

...challenge-response a chiave pubblica

- ***Identificazione tramite decrittaggio a chiave pubblica e con witness h(r)***

$$A \leftarrow\!\!- B: h(r), B, P_A(r, B)$$
$$A \dashrightarrow B: r$$

...challenge-response a chiave pubblica...

Protocollo Needham-Schroeder PK modificato

$$A \text{ ---> } B: P_B(r1, A)$$
$$A \text{ <--- } B: P_A(r1, r2)$$
$$A \text{ ---> } B: r2$$

Challenge-response basato sulla firma digitale

1. autenticazione unilaterale, con timestamp

$A \text{ ---> } B: cert_A, t_A, B, S_A(t_A,B)$

2. autenticazione unilaterale, con random number

$A \text{ <---} B: r_B$

$A \text{ ---> } B: cert_A, r_A, B, S_A(r_A,r_B,B)$

3. autenticazione mutua, con random number

$A \text{<---} B: r_B$

$A \text{---> } B: cert_A, r_A, B, S_A(r_A,r_B,B)$

$A \text{<---} B: cert_B, A, S_B(r_B,r_A,A)$

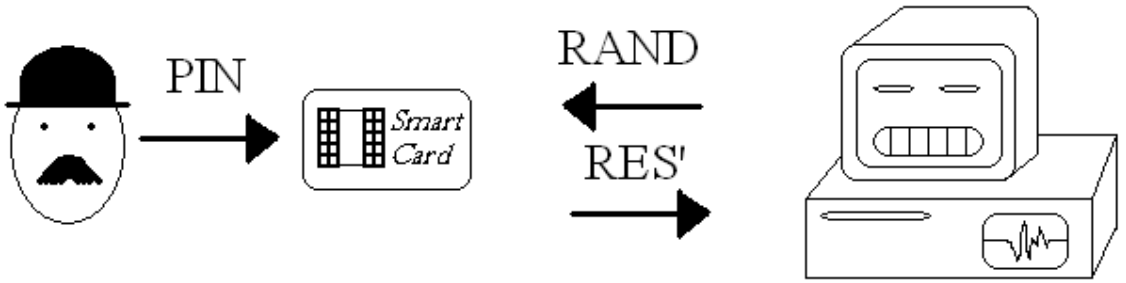
Smart Card

- Perchè “smart”?
  - Contengono un chip e possono memorizzare dati
- Perchè proprio le smart card?
  - Sono ideali per la crittologia
  - Sono ideali per l'utente umano

Smart card per il controllo d'accesso

- Facilitano i sistemi di autenticazione
  Es: parola d'ordine
  - L'utente si fa autenticare tramite il suo PIN
  - La carta si fa autenticare con un protocollo dinamico di autenticazione
- Un nemico deve entrare in possesso sia del PIN che della rispettiva scheda

...smart card nel controllo d'accesso...



Autenticazione utente-carta con un PIN, che è verificato dentro la carta

Autenticazione dinamica carta-computer

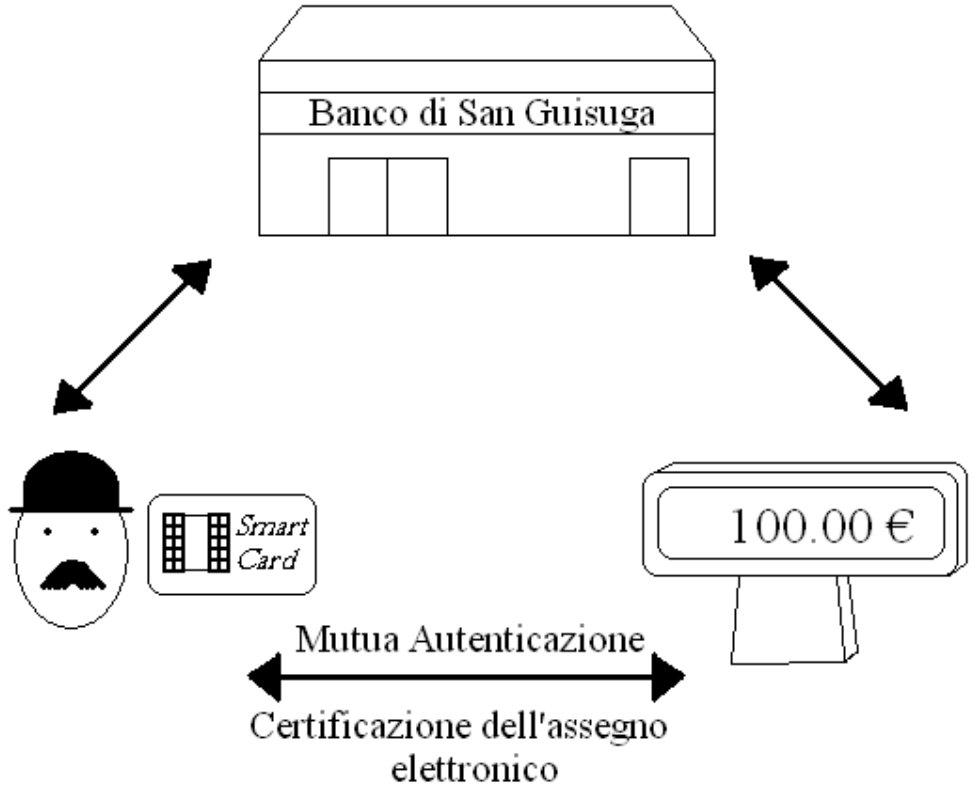
...smart card nel controllo d'accesso

- Vantaggi:
  - I numeri scambiati variano di volta in volta
  - Un nemico non può prevedere il successivo RAND o RES
- Limiti:
  - Processori e memoria limitati (dovuto al chip)
    - Ciò comporta l'uso di algoritmi simmetrici

Compere Elettroniche

Tre parti in causa:

- Acquirenti
- Negozianti
- Banche

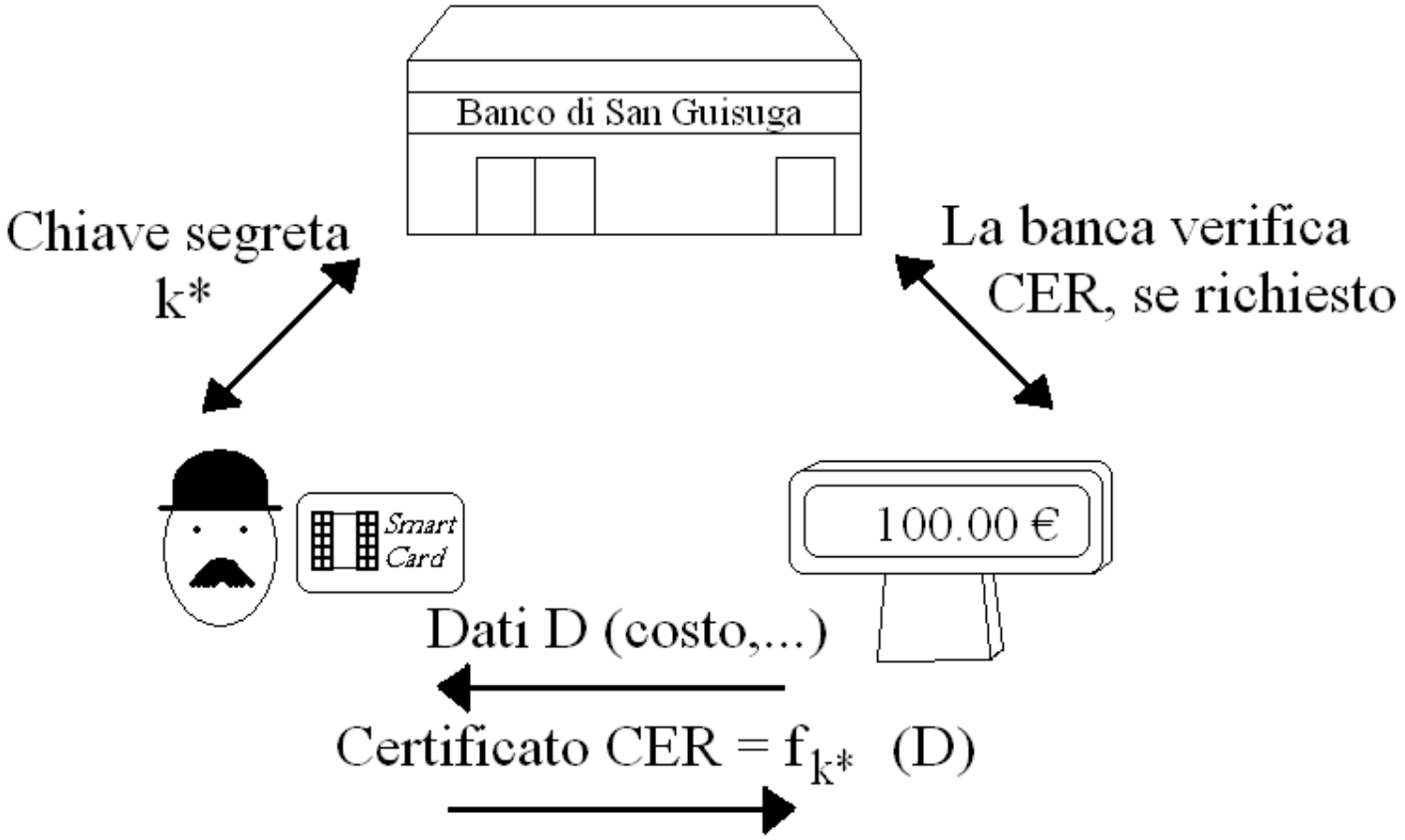


...compere elettroniche...

- Tre autenticazioni richieste:
  - Autenticazione dell'acquirente dal terminale
    - Come descritto per le smart card
  - Autenticazione del terminale da parte della carta
    - Per evitare terminali fraudolenti
  - Autenticazione dell'assegno elettronico
    - Per assicurare il venditore

...compere elettroniche...

Procedura di Certificazione (algoritmi simmetrici)



...compere elettroniche...

Il percorso dell'assegno elettronico

- viene “firmato” da una sorta di MAC
- viene trasmesso dalla carta al terminale del negozio
- tramite chiave k* si firma con un MAC l'assegno
- l'acquirente ratifica i dati (costo, spesa, negozio, ...), firmati tramite k* per computare il MAC, detti certificato
- il negoziante può chiedere alla banca di verificare il certificato

...compere elettroniche...

- Problemi con l'uso di un algoritmo simmetrico:
  - È importante l'integrità dei dati
  - Chiunque sia in grado di verificare il MAC può falsificare l'assegno e calcolare il MAC corrispondente, poiché conosce la chiave segreta
- Il problema è risolto grazie allo schema di firma a chiave publica

...compere elettroniche

- Problemi con l'uso di certificati:
  - Acquirente e negoziante devono fidarsi della banca
  - Il negoziante non può verificare l'assegno immediatamente
- È attribuita al sistema una sicurezza maggiore rispetto ad altri sistemi di pagamento tramite carte.

Fine

Autenticazione Forte
...e uso delle carte

a cura di
Alessio Dantignana

riferimenti:
Handbook of Applied Criptography by A. Menezes, P.van Oorschot and S.Vanstone

realizzato con:
OpenOffice.org 1.0.2 – contro il monopolio sul software