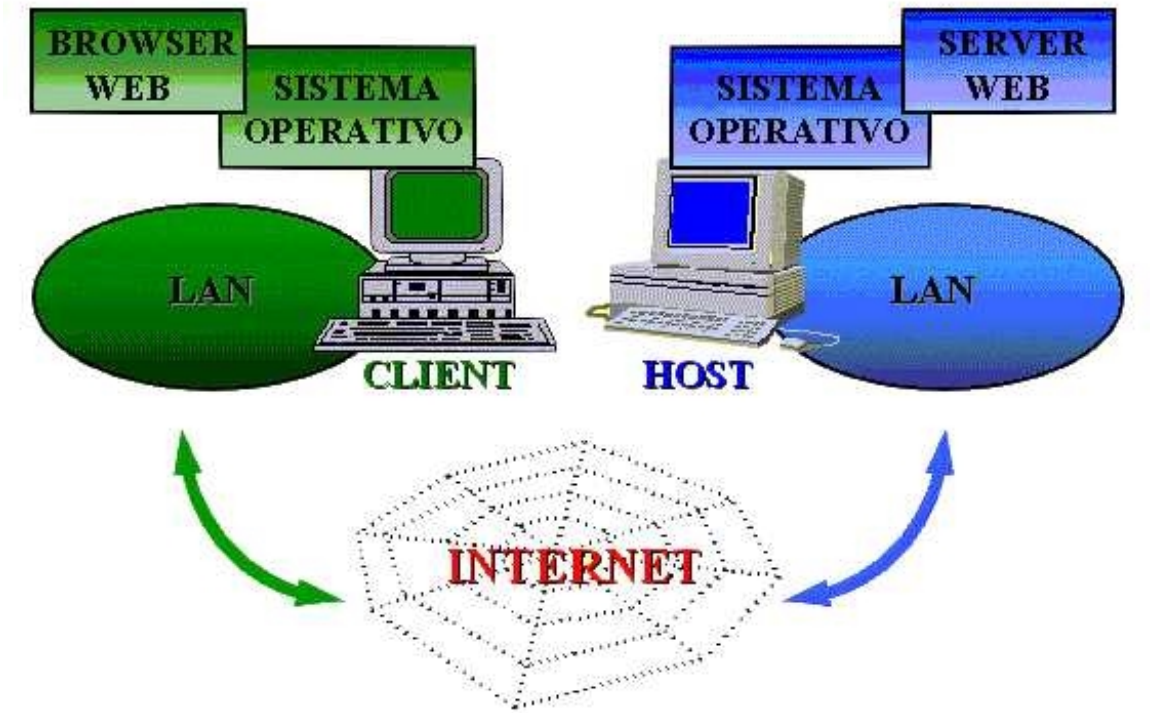
Sicurezza nell'utilizzo di Internet

Sicurezza – Definizioni

- Pirati informatici (hacker, cracker): persone che entrano in un sistema informatico senza l'autorizzazione per farlo
- Sicurezza:
  protezione applicata ad un sistema informatico per garantire il soddisfacimento degli obbiettivi di preservazione dell'integrità, disponibilità e confidenzialità delle risorse del sistema

Sicurezza – Struttura del web

- Elementi da prendere in considerazione nell'analisi della sicurezza (punti deboli)



Sicurezza - Pericoli

- Cavallo di Troia: programma o documento che contiene software dannoso nascosto da una normale applicazione (es. virus in file o email)
- Hacking: spezzare i meccanismi di autenticazione della password (“intuizione”, furto, generazione automatica di password)

Sicurezza - Pericoli

- Sniffing: “fiutare” le password attraverso software in grado di monitorare il flusso di pacchetti di dati che attraversano la rete
- Spoofing: possibilita’ di modificare in maniera fraudolenta il contenuto dei pacchetti in circolazione
(es. falsificando l’indirizzo IP di provenienza e assumendo indebitamente l’identita’ altrui)

Sicurezza – Cosa fare

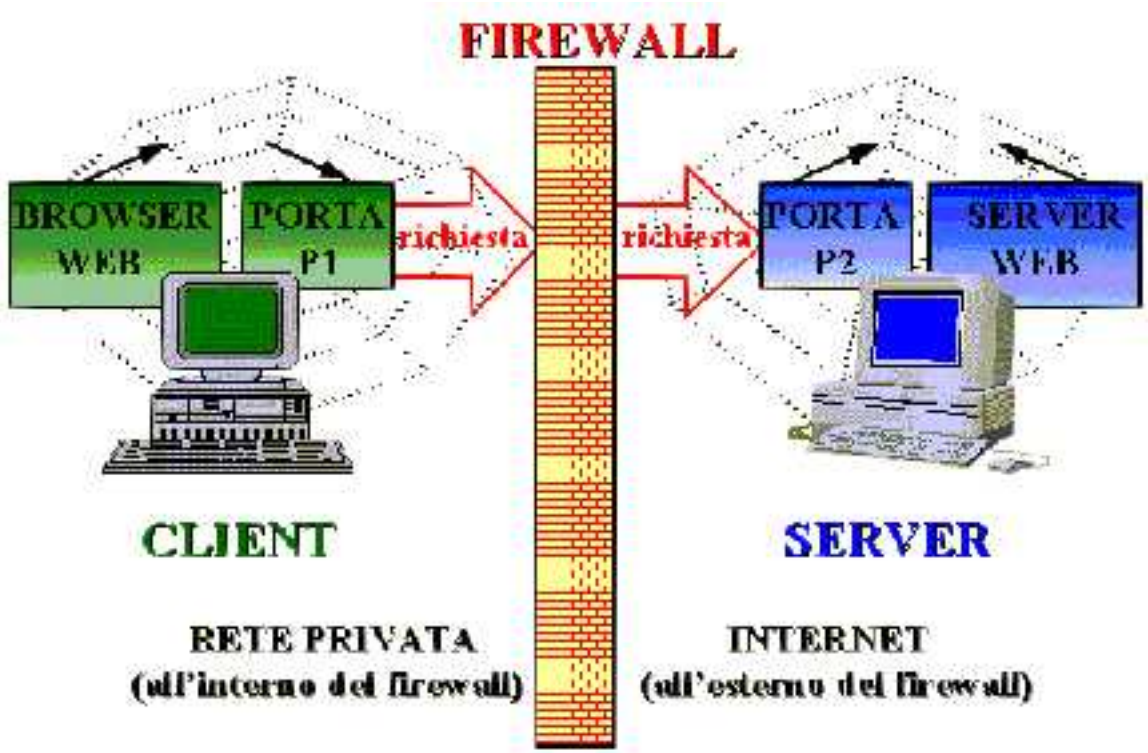
- Limitare gli accessi e usare meccanismi di autenticazione e autorizzazione
- Monitorare i registri e i log che tracciano i tentativi di accesso (tcwrapper in unix)
- Disabilitare i servizi del sistema operativo che non sono necessari
- Separare i servizi (es. Web, email)
- Tenersi informati: newsgroup e pareri del Computer Emergency Response Group (CERT)

Sicurezza – Cosa fare

- Principio del privilegio minimo: al server Web deve essere assegnata la quantità minima di privilegi di cui ha bisogno
- Limitare l'accesso alle aree CGI, directory in cui sono memorizzati script e programmi eseguibili

Sicurezza – i Firewall

- Funzioni o apparecchiature che servono a proteggere un dominio o una rete privata

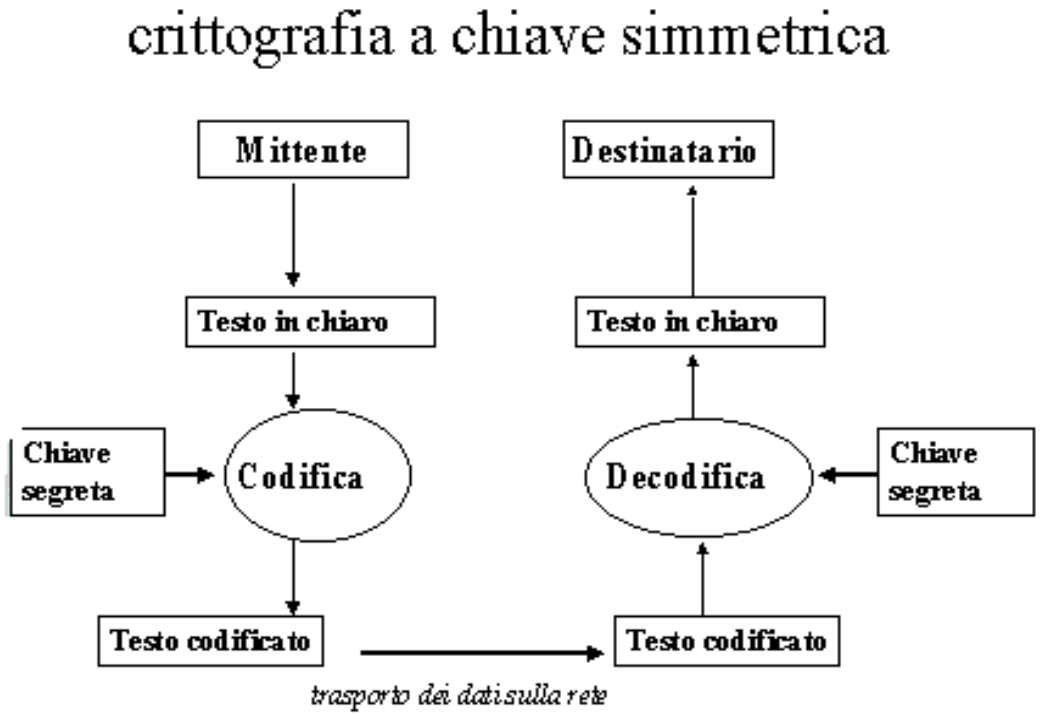


Crittografia

- La Crittografia si occupa della cifratura e della decifratura dei messaggi
- Crittografia moderna: algoritmi a chiave simmetrica e asimmetrica

Crittografia – algoritmi a chiave simmetrica (DES)

- Messaggio criptato con chiave segreta (nota solo al mittente e al destinatario)



Crittografia – Sistemi a chiave asimmetrica (chiave pubblica)

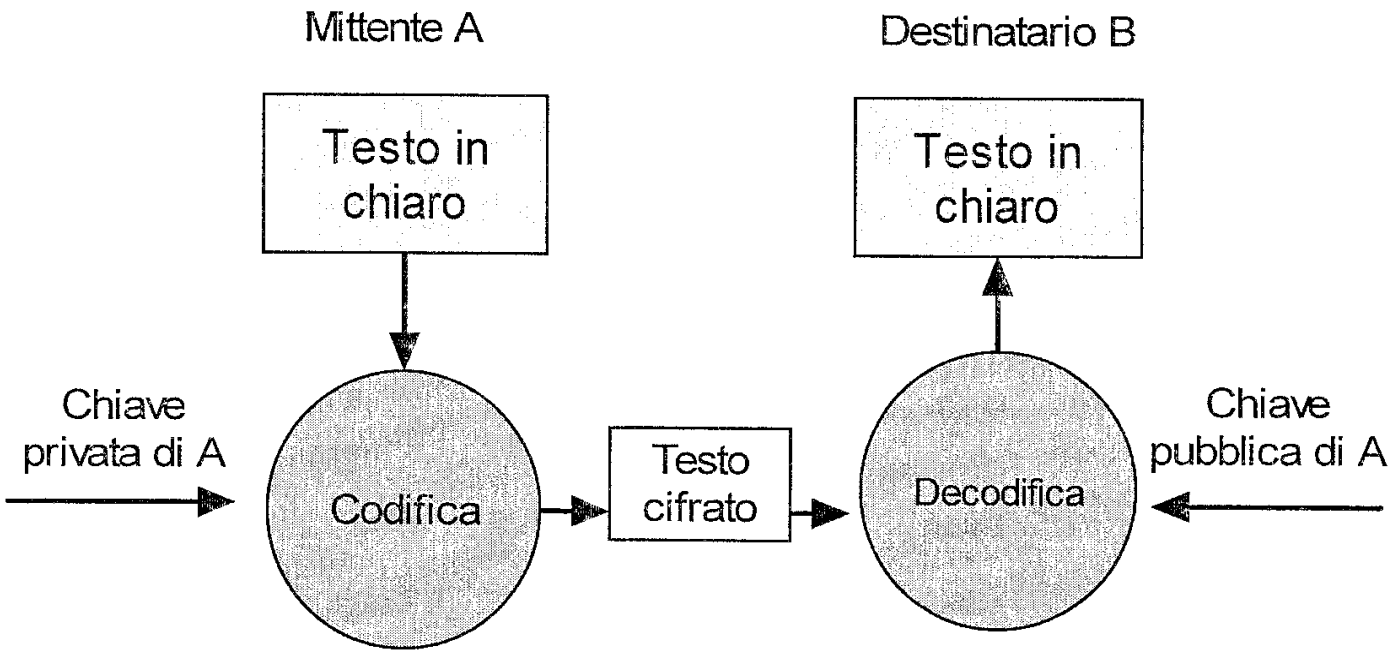
- Ad ogni persona sono assegnate due chiavi (pubblica e privata) legate tra loro ma non riconducibili l'una a l'altra.
- Sono necessarie autorità di riferimento per la detenzione delle chiavi pubbliche che siano affidabili (garantiscono l'autenticità).

Crittografia – Sistemi a chiave asimmetrica (RSA)

- Algoritmo **R**ivest, **S**hamir, **A**dleman 1977
  - scelgo p,q numeri primi grandi (~10^{200})
  - n = pq, m = (p-1)(q-1)
  - scelgo e < m, e primo rispetto a m
  - calcolo d tale che: de = 1 mod m (inverso di e mod m, es. alg. di Euclide)
  - => **chiave pubblica** e': (e,n)
  - => **chiave privata** e' : (d,n)
- cifratura: $C = M^e \bmod n$
- decifratura: $M = C^d \bmod n$
  - decrittazione: trovare d noti n,e,C (occorre fattorizzare n in pq !!)

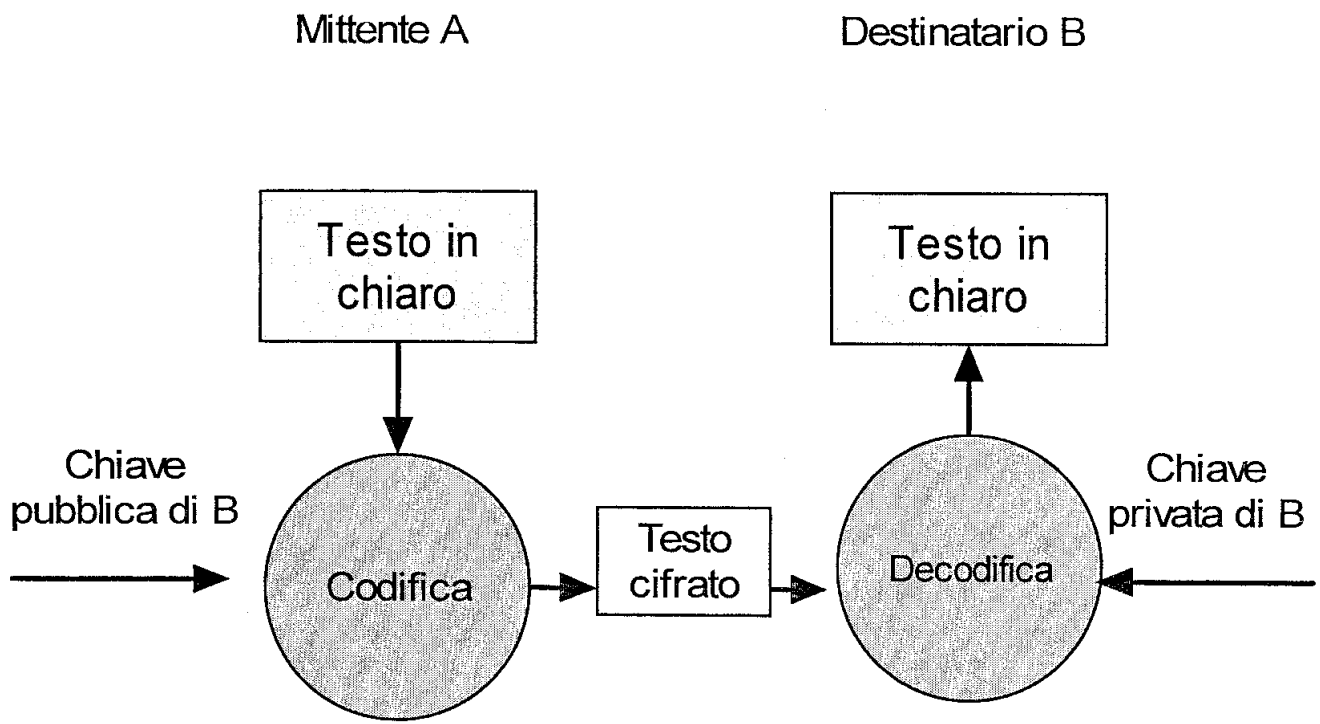
Crittografia – Sistemi a chiave asimmetrica (RSA)

- Autenticazione del mittente



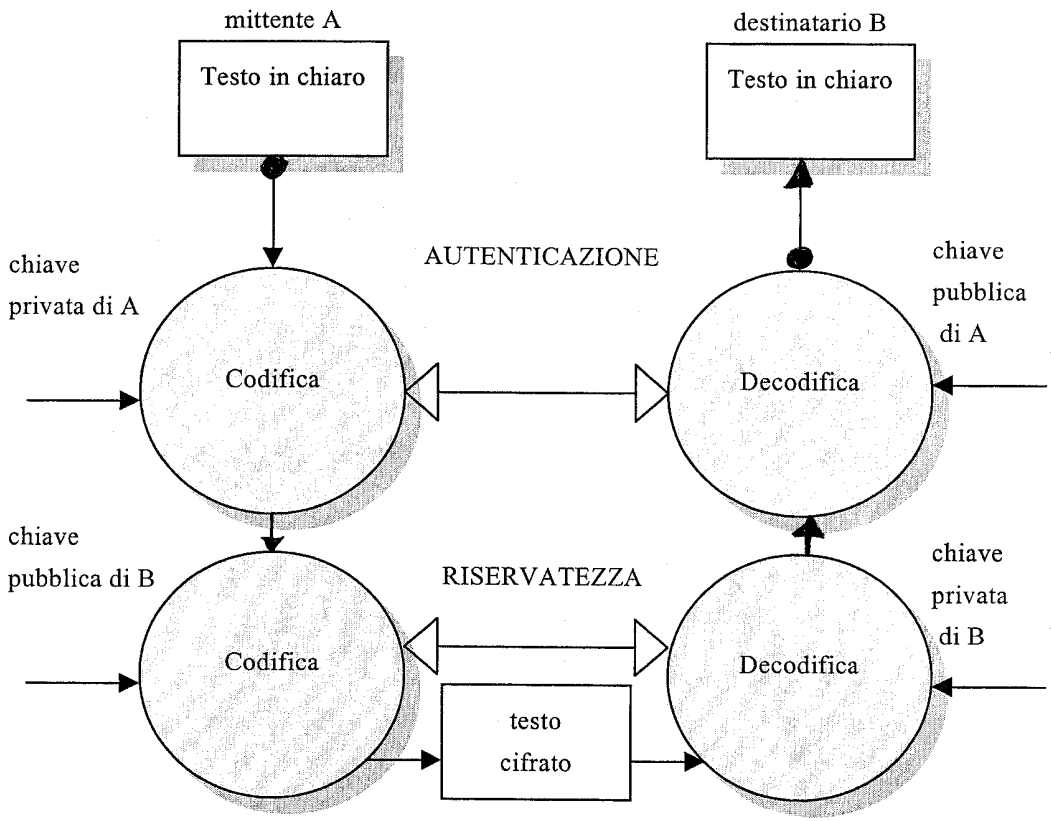
Crittografia – Sistemi a chiave asimmetrica (RSA)

- Riservatezza e identità del destinatario



Crittografia – Sistemi a chiave asimmetrica (RSA)

- Certezza del mittente, del destinatario e riservatezza del messaggio



Sistemi a chiave Asimmetrica

- Vantaggi
  - non richiede scambio di informazione segreta in rete (la chiave)
  - con N soggetti, richiede 2N chiavi anziche' N(N-1)/2
  - garantisce l'autenticita'
- Svantaggi
  - usa chiavi molto lunghe e processo criptazione computazionalmente oneroso
  - non cifra alcune strutture del messaggio che possono essere riconosciute e permettere di risalire al messaggio in chiaro

Uso sinergico dei due sistemi (PGP)

- Il Messaggio vero e proprio viene codificato con un cifrario simmetrico (+ veloce e sicuro)
- La crittografia a chiave pubblica viene utilizzata per lo scambio della chiave simmetrica:
  la chiave simmetrica viene codificata con la chiave pubblica del destinatario e allegata al messaggio (busta elettronica)

SSL (protocollo https)

- Privatezza del collegamento: i dati sono crittografati con crittografia simmetrica (RSA)
- Autenticazione: identità autenticata attraverso la crittografia asimmetrica (certificato digitale)
- Affidabilità: il livello di trasporto include un check dell'integrità del messaggio (con firma digitale)

Firma Digitale

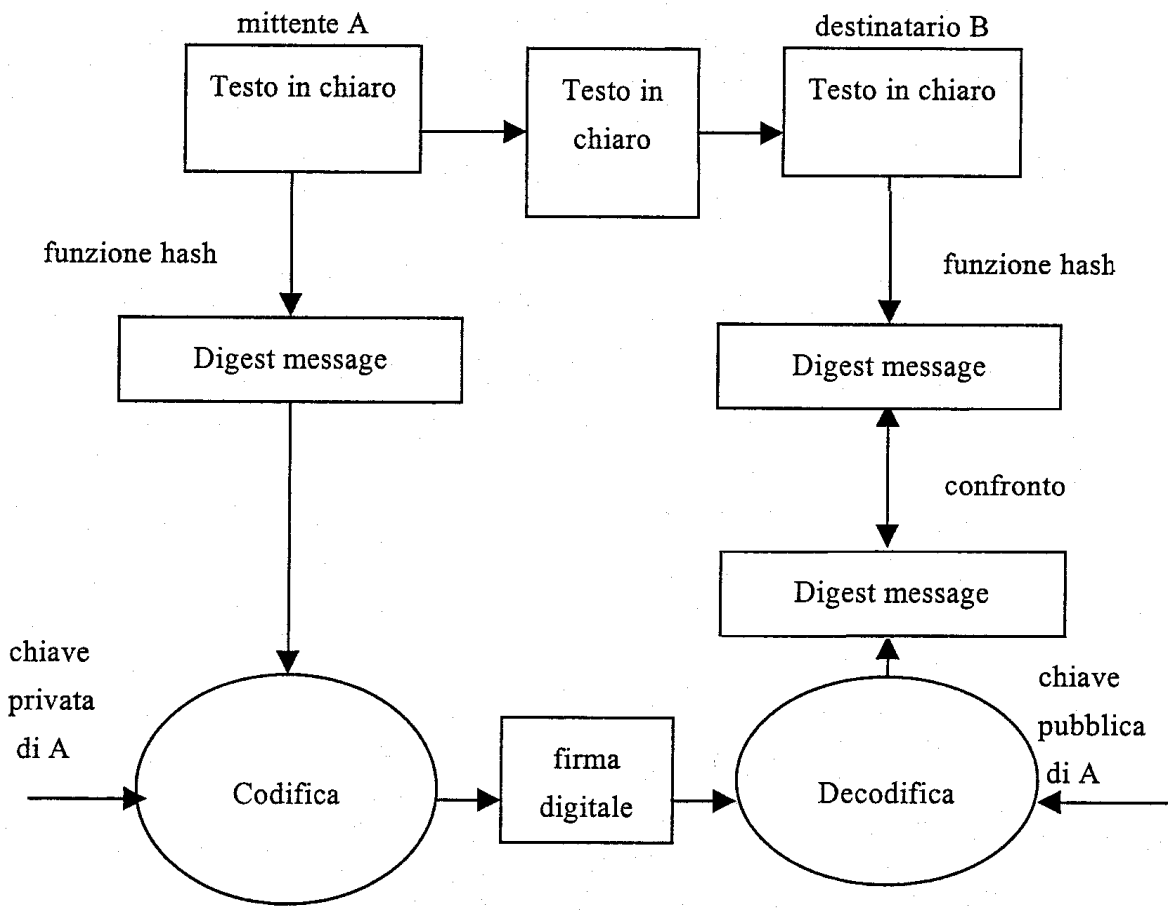
- Il Documento con firma elettronica
  - e’ stato realmente prodotto dal proprietario della firma
  - non puo’ essere stato modificato dopo la firma
  - non puo’ essere disconosciuto da chi ha firmato
- (proprieta’ verificabili da chiunque riceva il documento firmato)

Firma Digitale

- La sottoscrizione con firma digitale ha valore legale (D.P.R. 512/97 n. 513 e Regolamento attuativo)
  - ha funzione indicativa
    (identifica l'autore)
  - ha funzione dichiarativa
    (denota approvazione del contenuto del documento da parte del firmatario)
  - ha funzione probatoria
    (l'autore si assume la paternita' dei contenuti)

Firma Digitale

- Schema di funzionamento



Commercio Elettronico (e-commerce)

- Un qualunque tipo di operazione commerciale (vendita/acquisto beni e servizi) in cui gli attori interagiscono per via elettronica piuttosto che con scambi fisici e contatti diretti
- Tipologie:
  - B2B - Business to Business (93%)
  - B2C - Business to Consumer (7%)

Commercio Elettronico

- Transazione Commerciale: inoltro dell'ordine dall'acquirente al negozio virtuale (Internet)
- Transazione Finanziaria: inoltro istruzioni di pagamento da parte dell'acquirente
  - off-line (es. via telefono o fax)
  - on-line - pagamento elettronico

Pagamento elettronico

- Metodi “hardware”
  - borsellino elettronico (smart-card)
- Metodi “software”
  - debit-based (assegni elettronici)
    Netchex, Redi-check, Netcheque, Banknet, FSTC
  - credit-based (uso di carte di credito)
    CyberCash, FirstVirtual, STT-SEPP, TelePay, SET
  - token-based (moneta virtuale)
    Millicent, Netbill, E-Cash, DigiCash

Il Sistema SET - Secure Electronic Transaction

- Nato da accordo Visa-Mastercard
- Non prevede connessione sicura (non opera a livello di pacchetto come SSL) ma gestisce la transazione di pagamento a livello di applicazione
- Basato su crittografia (RSA + DES) e certificati digitali (standard X.509)

SET - Attori

- Il possessore di carta di credito (il compratore)
- Il venditore
- Un'Autorita' di Certificazione, garante dell'identita' delle parti coinvolte (es. VeriSign)
- Un Payement Gateway (l'intermediario)
- La rete di pagamento delle istituzioni finanziarie

SET - Fasi operative

- User Registration:
  l'utente si registra presso un'autorita'
  e ottiene un certificato
- Purchase Request:
  l'utente invia l'ordine di acquisto
- Payment Authorization:
  il venditore richiede al gateway l'autorizzazione
  e provvede alla consegna del bene o servizio
- Payment Capture:
  avviene il trasferimento della somma

SET - User Registration (1)

- Initiate Request
  invio (non protetto) richiesta di registrazione all'authority
- Initiate Response
  l'authority risponde includendo il proprio certificato e autenticandolo apponendo la propria firma digitale
- Registration Form Request
  il richiedente fa le verifiche, memorizza il certificato ad uso futuro, e chiede il form appropriato (c/c bancario, diverse carte credito) usando la chiave pubblica dell'authority
- Registration Form
  l'authority fa le verifiche e invia all'utente il form richiesto (al solito con con certificato firmato)

SET - User Registration (2)

- Cardholder Certification Request

  il richiedente fa le verifiche sul form, se non gia' disponibili il sw genera una coppia di chiavi simmetriche per l'utente; questi compila il form (es. con dati carta di credito), che viene cifrato con una chiave simmetrica, posta in busta elettronica sigillata con la chiave pubblica dell'authority e inviata alla stessa

- Cardholder Certificate

  l'authority apre la busta, legge la chiave con cui decifra il form, prende una decisione sul rilascio dell'autorizzazione; in caso positivo genera il certificato per l'utente, lo firma digitalmente e lo invia in messaggio protetto

- Certificate

  il richiedente decifra il certificato, fa le verifiche del caso e registra il suo certificato per usi futuri

SET - Purchase Request

- Initiate Request
  invio (non protetto) del proprio certificato al venditore
- Initiate Response
  il venditore assegna alla transazione un identificatore (ID) univoco e lo pone, assieme ai certificati proprio e del payment gateway in un messaggio firmato digitalmente che invia in modo protetto al compratore
- Purchase Request
  il compratore verifica i certificati inviati, genera order information (OI) e payment instructions (PI) in cui e` inserito il TI; OI non contiene dati riservati e viene semplicemente firmato, PI viene cifrato con chiave simmetrica e posto in busta che solo il payment gateway potra' aprire; infine PI e OI sono inviati al venditore
- Purchase Response
  il venditore verifica il certificato del compratore e l'ID in OI e invia richiesta di approvazione al gateway; avuta la risposta la invia al compratore apponendo la propria firma ("ricevuta" della transazione per il compratore)

SET - Payment Authorization

- Authorization Request

  il gateway riceve dal venditore la richiesta di autorizzazione contenente PI cifrato con chiave simmetrica e posti in busta digitale dal compratore, le informazioni riguardanti la transazione cifrati con chiave simmetrica posti in busta digitale dal venditore e i certificati di compratore e venditore

- Authorization Response

  il gateway riceve la richiesta di autorizzazione, controlla i certificati, apre le buste digitali ricavandone le chiavi simmetriche di compratore e venditore con cui decifra PI e richiesta di autorizzazione; se le informazioni inviate da compratore e venditore corrispondono, la richiesta di autorizzazione viene inoltrata all'istituto finanziario (es. su rete interbancaria); se la transazione e' approvata, il gateway invia un messaggio al venditore contenente un capture token che verra' usato in seguito per l'accredito

SET - Payment Capture

- Capture Request

  il venditore crea un messaggio di richiesta, lo firma e lo cifra usando una chiave simmetrica; il messaggio cifrato viene poi inserito in una busta indirizzata al payment gateway cui viene inviato assieme al capture token e ai certificati di compratore e venditore

- Capture Response

  il payment gateway controlla i certificati, apre la busta digitale ed estrae la chiave simmetrica a lui destinata con cui decifra le informazioni e controlla la firma digitale; superati i controlli il gateway invia il capture token all'istituto finanziario affinche' venga eseguito il trasferimento di fondi; se e' tutto OK, il gateway invia un messaggio di conferma al venditore in busta digitale, assieme al proprio certificato.