La sicurezza informatica nello studio del professionista

Riservatezza e integrità dei dati giuridici alla luce delle nuove tecnologie

Silvano Marioni, CISSP

TECNOLOGIA E DIRITTO
Informatica giuridica

Scuola Superiore di Informatica di Gestione
Bellinzona, 10 maggio 2007

Agenda

- Le esigenza di sicurezza
- Aspetti tecnici della firma digitale
- L'Autorità di Certificazione
- Aspetti legali della firma elettronica

I nuovi comportamenti

Inchiesta SUPSI “Sicurezza informatica e utilizzo dei computer in azienda”, aprile 2007 (www.dti.supsi.ch/isi)

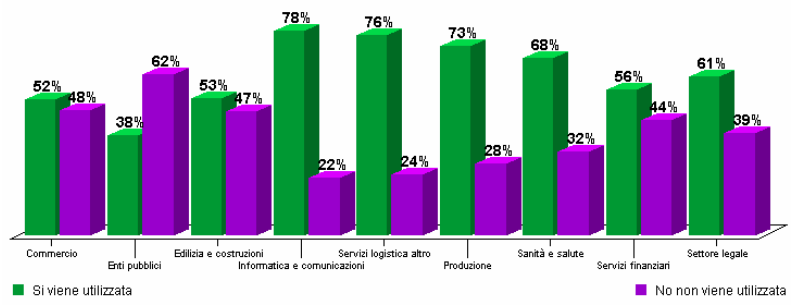


Figura 20 : percentuale di utilizzo della posta elettronica per inviare e/o ricevere documenti aziendali importanti suddivisa per settore di attività

Le nuove esigenze di sicurezza

- Protezione del posto di lavoro
  - Utilizzo di password, antivirus, firewall, aggiornamenti software, ecc.
- Protezione delle comunicazioni
  - Prudenza nell’uso di Internet, informazioni sui rischi del social engineering,
- Protezione dei documenti
  - Comportamenti e strumenti tecnici adeguati per garantire riservatezza, integrità e disponibilità dei dati

La smaterializzazione dei documenti

- Il computer, trattando le informazioni in formato digitale, rende superfluo il supporto materiale
- Per poter sostituire ai documenti reali i documenti smaterializzati, questi devono avere una serie di caratteristiche che li rendono equiparabili ai documenti reali

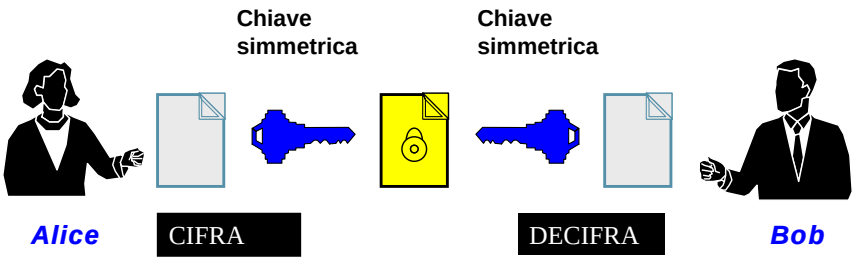
Caratteristiche dei documenti reali

- Riservatezza
  - L'esigenza di far conoscere i contenuti del documento solo alle persone autorizzate
- Integrità
  - La protezione contro modifiche non autorizzate del documento
- Non ripudio
  - La garanzia che il contenuto del documento non può essere ripudiata da una delle parti
- Evidenza temporale
  - L'indicazione affidabile che il documento é stato elaborato in un particolare momento

Trasposizione nei documenti digitali

- Riservatezza
  - Cifratura a chiave simmetrica
  - Cifratura a chiave pubblica
- Integrità
  - Firma digitale
- Non ripudio
  - Firma digitale
- Evidenza temporale
  - Marcatura temporale (basata sulla firma digitale)

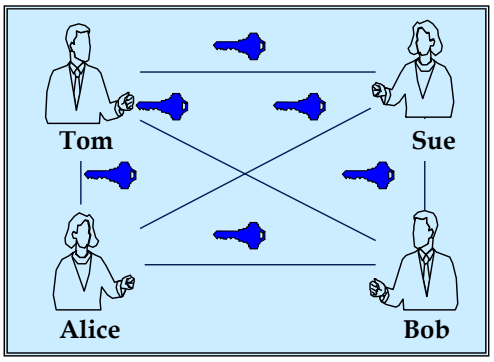
Cifratura a chiave simmetrica



- Garantisce la **riservatezza** del documento
- La chiave deve essere matenuta segreta
- Gli interlocutori utilizzano la stessa chiave per cifrare e decifrare
- Ci sono programmi per cifrare files, cartelle oppure dischi interi
  - WinZIP, SecureZIP, Truecrypt, File2File, AxCrypt, ecc.

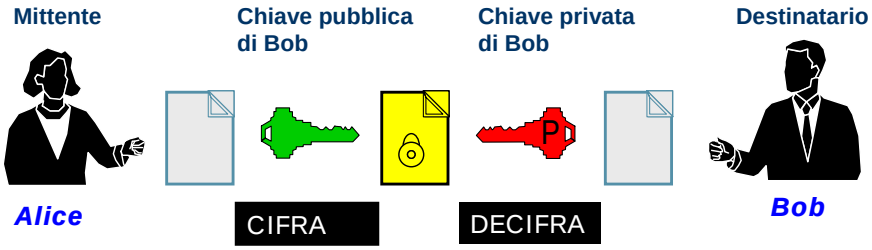
Cifratura a chiave simmetrica

Il sistema è semplice e pratico nella comunicazione tra due persone ma diventa problematico al crescere del numero degli interlocutori per il problema della distribuzione delle chiavi



- Crescita del numero di chiavi al crescere degli utenti
  - 4 utenti
    6 chiavi
  - 100 utenti
    4950 chiavi
  - 1000 utenti
    499'500 chiavi

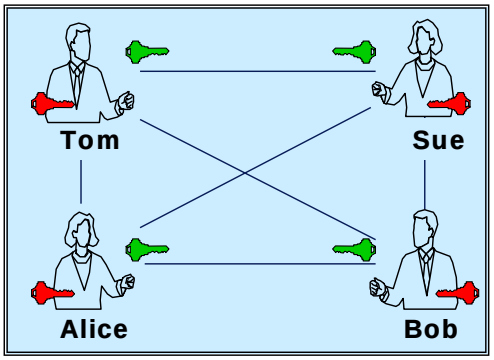
Cifratura a chiave pubblica



- Garantisce la **riservatezza** del documento
- Ogni interlocutore possiede **una coppia** di chiavi
- Una chiave serve per cifrare, l'altra per decifrare
- La chiave per cifrare deve essere resa **pubblica**
- La chiave per decifrare deve essere mantenuta **segreta**

Cifratura a chiave pubblica

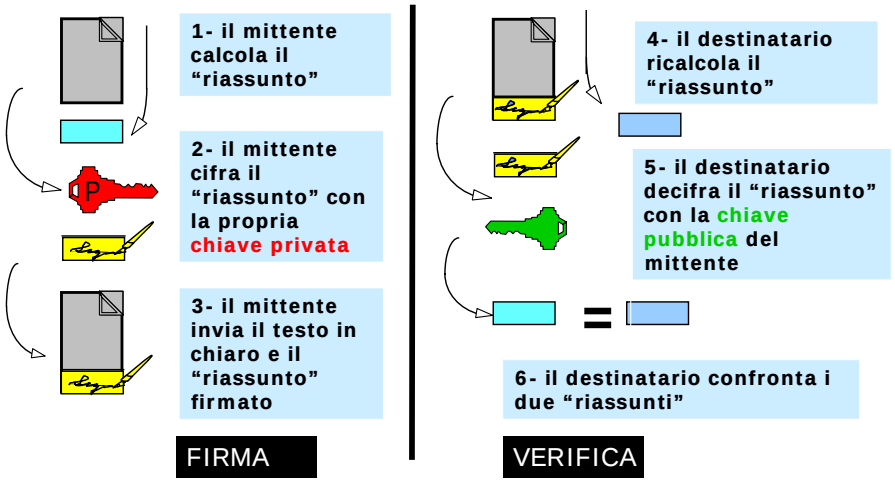
Il sistema funziona anche se le persone non si conoscono e non ci sono limiti al numero degli interlocutori



- non è necessario lo scambio delle chiavi
- deve solo essere conosciuta la chiave pubblica del destinatario
- Richiede la garanzia dell'autenticità della chiave pubblica del destinatario !!

Firma digitale

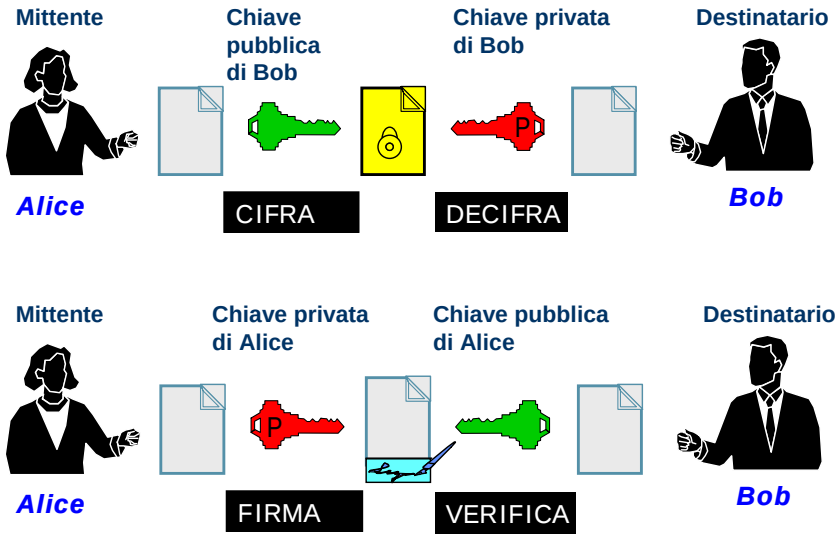
Cifratura con la chiave privata del mittente di un "riassunto" del documento
Decifratura da parte del destinatario con la chiave pubblica del mittente



Firma digitale

- Garantisce **l'integrità** del documento
- Garantisce la provenienza del documento e di conseguenza il **non ripudio**
- Utilizza la medesima tecnologia della cifratura a chiave pubblica
- Richiede la garanzia dell'autenticità della chiave pubblica del mittente !!

Confronto tra cifratura e firma



Marcatura temporale

- Serve per attestare la "data e l'ora esatta" di un documento
- Ha la stessa funzione del timbro dell'ufficio postale su un francobollo o su un documento cartaceo
- La marcatura temporale di un documento informatico consiste nella generazione, da parte di una terza parte fidata, di una firma digitale del documento cui è associata l'informazione relativa ad una data e ad un'ora garantita come certa
- Può essere fatta su un singolo documento o su un lotto di documenti

Chiave privata e chiave pubblica

- La chiave privata,
  - Viene utilizzata per decifrare e firmare
  - Deve essere conservata in modo protetto dall'utente
- La chiave pubblica
  - Viene utilizzata per cifrare e verificare la firma
  - Deve essere distribuita pubblicamente
  - È memorizzata nel Certificato Digitale che:
    - Fornisce la **garanzia della chiave pubblica** dell'interlocutore
    - È firmato con la chiave privata di una **Autorità di certificazione** che fa da garante

Autorità di Certificazione

- È un'organizzazione di fiducia che garantisce il processo di verifica dell'identità e gestisce il ciclo di vita dei certificati digitali
- Attività di registrazione
  - Svolge la funzione di identificazione e se ne assume le responsabilità
  - Verifica dell'identità
- Attività di certificazione
  - Gestione dell'infrastruttura tecnica per la gestione dei certificati
  - Gestione del ciclo di vita dei certificati digitali
    - Creazione del certificati
    - Verifica della validità (Certificate Revocation List, OCSP)
    - Revoca dei certificati
    - Rinnovo dei certificati
- Deve distribuire la sua chiave pubblica

Modelli di fiducia (Trust models)

- Modello di fiducia paritetico
  - il certificato viene emesso dall'utente stesso che lo autocertifica e lo fa riconoscere come valido dalle controparti che hanno fiducia in lui
    - PGP, Web of Trust
- Modello di fiducia gerarchico
  - il certificato viene emesso da un'autorità di certificazione e viene riconosciuto valido in modo automatico secondo uno schema gerarchico
    - Autorità di certificazione interne
    - Autorità di certificazioni commerciali
    - Autorità di certificazione riconosciute per legge

Ambienti di certificazione

- Ambienti chiusi (la chiave pubblica della CA ha una distribuzione limitata)
  - Comunicazione tra applicativi software
    - Nessuna esigenza legale, firma e cifratura, funzionamento trasparente per l'utente, certificati autogenerati. Esempi: reti VPN, SSH, ecc.
  - Comunicazioni sicure aziendali
    - Nessuna esigenza legale, firma e cifratura del messaggio, certificati autogenerati o commerciali
    - Esempi: PGP, posta elettronica S/MIME
- Ambienti aperti (la chiave pubblica della CA è disponibile a tutti)
  - Gestione sicura di messaggi e documenti
    - Nessuna esigenza legale, firma e cifratura del messaggio, certificati autogenerati o commerciali
    - Esempi: PGP, posta elettronica S/MIME
  - Comunicazione sicura con server commerciali
    - Nessuna esigenza legale, identificazione del server, cifratura, certificati commerciali
    - Esempi: commercio elettronico, telebanking
  - Comunicazione sicura con valore probatorio
    - Devono essere soddisfatti i requisiti legali che permettono l'equiparazione con la firma autografa, certificati generati secondo i requisiti legali
    - Esempi: firma elettronica qualificata

Tipi di firme secondo la legge

- **Legge federale sui servizi di certificazione nel campo della firma elettronica, FiEle**
  Art. 2 Definizioni
- Nella presente legge si intende per:
  - a. *firma elettronica*: dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici e utilizzati per la loro autenticazione;
  - b. *firma elettronica avanzata:* firma elettronica che soddisfa i seguenti requisiti:
    - 1. essere connessa esclusivamente al titolare,
    - 2. essere idonea a identificare il titolare,
    - 3. essere creata con mezzi sui quali il titolare può conservare il suo controllo esclusivo,
    - 4. essere connessa ai dati ai quali si riferisce in modo tale che una successiva modifica dei dati sia riconoscibile;
  - c. *firma elettronica qualificata:* firma elettronica avanzata fondata su un dispositivo sicuro per la creazione di una firma secondo l'articolo 6 capoversi 1 e 2 e su un certificato qualificato e valido al momento della sua creazione;

Firma elettronica

- a. *firma elettronica*: dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici e utilizzati per la loro autenticazione;
- Non è una firma digitale
- Può essere un nome apposto a un messaggio di posta, una scansione digitale di una firma autografa, ecc.

Firma elettronica avanzata

- b. *firma elettronica avanzata:* firma elettronica che soddisfa i seguenti requisiti:
  - 1. essere connessa esclusivamente al titolare,
  - 2. essere idonea a identificare il titolare,
  - 3. essere creata con mezzi sui quali il titolare può conservare il suo controllo esclusivo,
  - 4. essere connessa ai dati ai quali si riferisce in modo tale che una successiva modifica dei dati sia riconoscibile;
- È una firma digitale

Firma elettronica qualificata

- c. *firma elettronica qualificata:* firma elettronica avanzata fondata su un dispositivo sicuro per la creazione di una firma secondo l'articolo 6 capoversi 1 e 2 e su un certificato qualificato e valido al momento della sua creazione;
- È una firma digitale
- È equiparata alla firma autografa (art.14 cv 2bis CO)
- È ammessa come prova

Firma elettronica qualificata

- Devono essere rispettate le seguenti condizioni
  - Utilizzare procedure e mezzi tecnici che garantiscono la sicurezza (art. 6)
    - Uso di sistemi sicuri per memorizzare la chiave privata (smart card)

  - Utilizzare un certificato garantito da una Autorità di Certificazione riconosciuta per legge (art. 3)
    - Certificato qualificato

Autorità di Certificazione riconosciute per legge

- L'Autorità di Certificazione è il garante della firma elettronica e per questo la sua attività è disciplinata per legge
  - Legge federale sui servizi di certificazione nel campo della firma elettronica (FIEle/2003)
  - Ordinanza dell'UFCOM su FiEle (OFiEle/2004)
  - L'autorità che riconosce le Autorità di Certificazione è l'Ufficio federale di metrologia e di accreditamento
- In Svizzera le Autorità di Certificazioni riconosciute per legge sono:
  - Swisscom Solution SA
  - QuoVadis Trustlink Schweiz AG
  - Die Schweizerische Post, PostMail

Riferimenti alla firma elettronica

- Messaggio relativo alla legge federale sui servizi di certificazione nel campo della firma elettronica
  http://www.admin.ch/ch/i/ff/2001/5109.pdf
- Legge federale sui servizi di certificazione nel campo della firma elettronica, FiEle
  http://www.admin.ch/ch/i/rs/9/943.03.it.pdf
- Ordinanza dell'UFCOM su FiEle
  http://www.admin.ch/ch/i/rs/9/943.032.it.pdf
- Elenco delle Autorità di Certificazione svizzere riconosciute per legge
  http://www.seco.admin.ch/sas/00229/00251/index.html?lang=it
- Istruzioni per la verifica delle firme elettroniche qualificate secondo la legge federale sulla firma elettronica (FUSC)
  https://www.shab.ch/IT/manual.pdf

Riferimenti alla firma elettronica

- Le seguenti leggi fanno riferimento alla firma elettronica:
  - Ordinanza relativa alla legge federale concernente l'imposta sul valore aggiunto, OLIVA
    http://www.admin.ch/ch/i/rs/6/641.201.it.pdf
  - Ordinanza del DFF concernente la trasmissione elettronica di dati e informazioni, OelDI
    http://www.admin.ch/ch/i/rs/6/641.201.1.it.pdf
  - Ordinanza sulla tenuta e la conservazione dei libri di commercio, Olc
    http://www.admin.ch/ch/i/rs/2/221.431.it.pdf
  - Ordinanza sul Foglio ufficiale svizzero di commercio (Ordinanza FUSC)
    http://www.admin.ch/ch/i/as/2006/573.pdf
  - Legge sul Tribunale Federale
    http://www.admin.ch/ch/i/rs/1/173.110.it.pdf