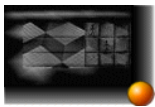


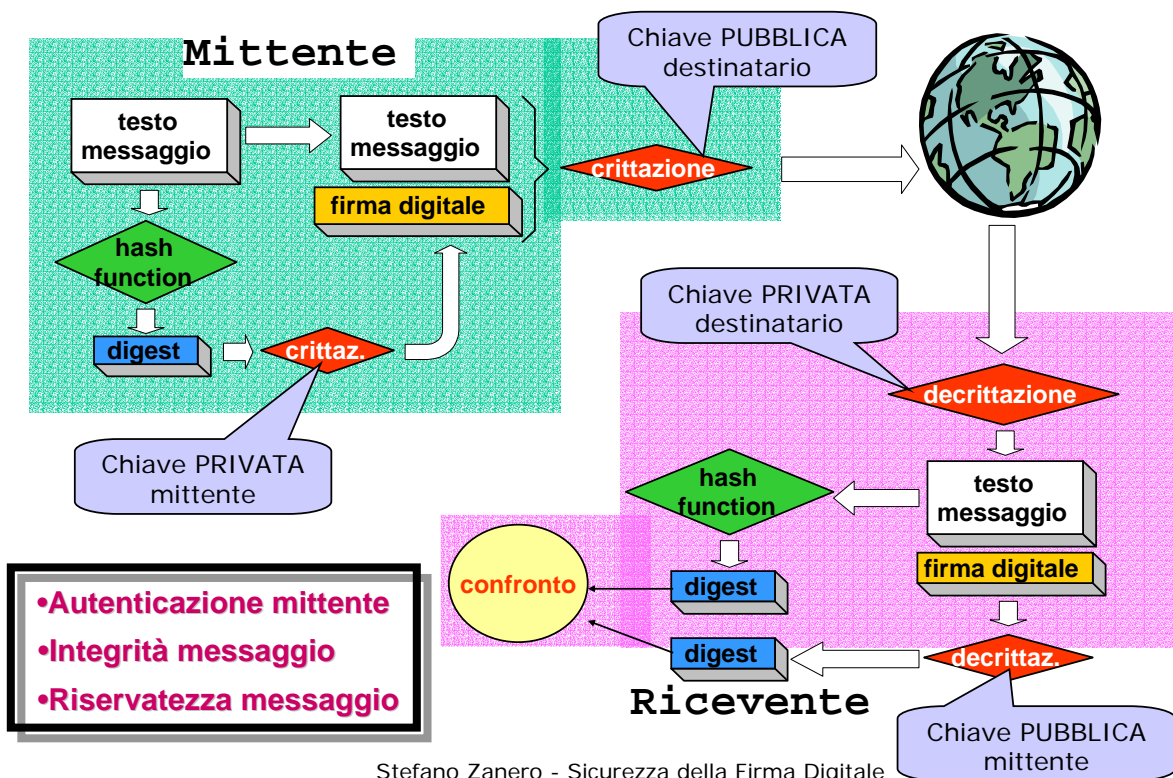
Sicurezza della Firma Digitale



Architettura e vulnerabilità della firma digitale italiana a valore legale

**Ing. Stefano Zanero
Politecnico di Milano
Dip. di Elettronica ed Informazione**

Crittografia asimmetrica: i concetti



Problema dell'identità


- L'utilizzo dell'algoritmo di firma digitale garantisce che un documento sia stato firmato con una determinata chiave privata
- Questo non dice nulla sull'AUTORE della firma, se non si è a conoscenza in modo certo della chiave pubblica di una persona
- Non c'è un modo sicuro di scambiarsi le chiavi pubbliche, se non out-of-band (di persona e mediante dischetto, per esempio)
- Lo scopo di una PKI (Public Key Infrastructure) è di garantire l'associazione chiave pubblica-mittente su una scala più vasta

Come funziona una PKI

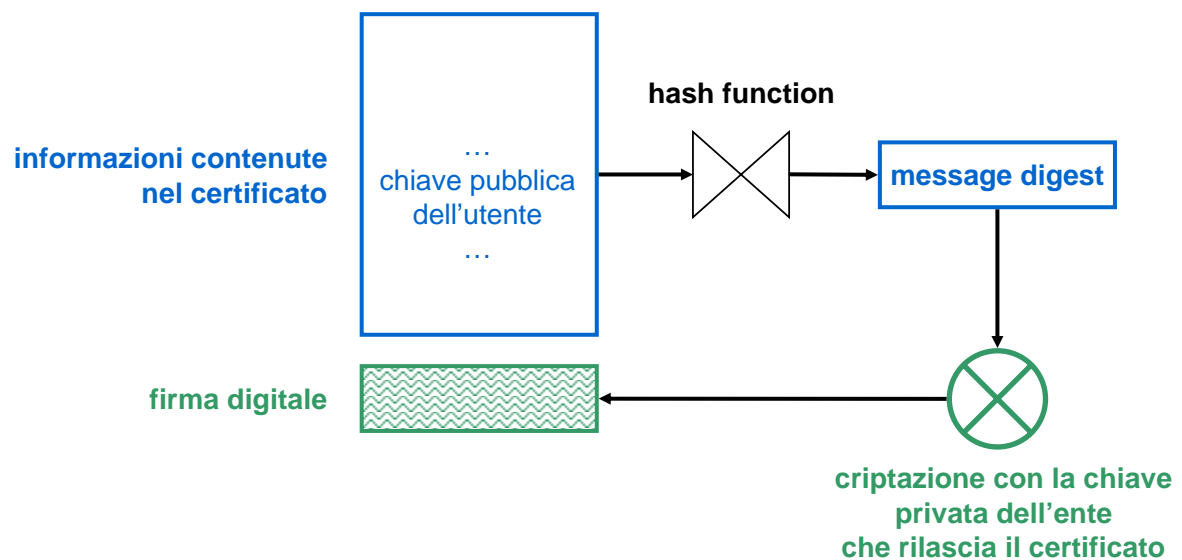
- Per poter garantire l'associazione tra un soggetto e una determinata chiave pubblica è necessario utilizzare una terza parte fidata che autentichi la chiavi pubblica
- Questa terza parte viene chiamata **certification authority (CA)**
- La CA rilascia un **certificato digitale** che contiene alcune informazioni sull'utente che l'ha richiesto, tra cui la chiave pubblica dell'utente
- Il certificato è firmato digitalmente dalla CA
- In questo modo, pur di ottenere in maniera sicura la chiave pubblica della CA, possiamo ottenere garanzie su una molteplicità di soggetti

Certificato digitale

proprietario del certificato
validità del certificato
chiave pubblica dell'utente
ente che ha rilasciato il certificato
firma digitale dell'ente che
ha rilasciato il certificato

Mario Rossi
dal 1/1/2000 all'1/1/2001
QH76H9H5GJ0J2JHAW
...
CA


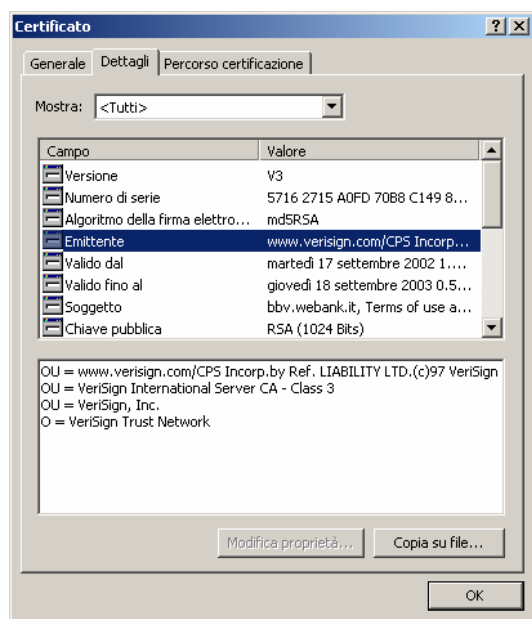
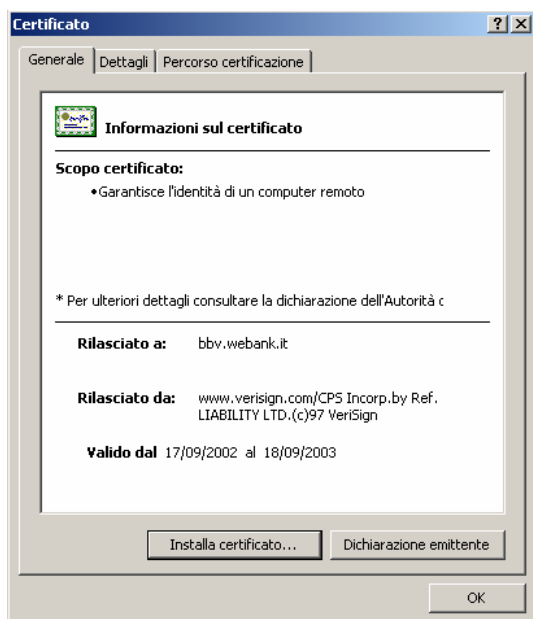
Certificato digitale (2)



Certificati digitali: standard X.509

- Lo standard associa un DN (*distinguished name*) ad una chiave pubblica
- La struttura di un certificato X.509 è
 - numero di versione del certificato
 - *serial number* del certificato
 - un numero diverso da quello di tutti gli altri certificati
 - chiave pubblica
 - DN della certification authority che ha rilasciato il certificato
 - periodo di validità
 - DN del proprietario del certificato
 - tipo di certificato
 - client, server, email
 - firma digitale della CA

Esempio di Certificato digitale X.509



Esempio di certificato X.509

Certificate:
Data:
Version: v3 (0x2)
Serial Number: 3 (0x3)
Signature Algorithm: PKCS #1 MD5 With RSA Encryption
Issuer: OU=Ace Certificate Authority, O=Ace Industry, C=US
Validity:
Not Before: Fri Oct 17 18:36:25 1997
Not After: Sun Oct 17 18:36:25 1999
Subject Public Key Info:
Algorithm: PKCS #1 RSA Encryption
Public Key:
Modulus:
00:ca:fa:79:98:8f:19:f8:d7:de:e4:49:80:48:e6:2a:2a:86:
43:7d:45:6d:71:4e:17:3d:f0:36:4b:5b:7f:a8:51:a3:a1:00:
Public Exponent: 65537 (0x10001)
Extensions:
Identifier: Certificate Type
Certified Usage: SSL Client
Identifier: Authority Key Identifier
Critical: no
Key Identifier: f2:f2:06:59:90:18:47:51:f5:89:33:5a:31:7a:e6:5c:fb:36:
Signature:
Algorithm: PKCS #1 MD5 With RSA Encryption
Signature:
6d:23:af:f3:d3:b6:7a:df:90:df:cd:7e:18:6c:01:69:8e:54:65:fc:06:
4a:e5:26:38:ff:32:78:a1:38:f1:ed:dc:0d:31:d1:b0:6d:67:e9:46:a8:

Esempio di certificato X.509 (2)

-----BEGIN CERTIFICATE-----

```
MIICKzCCAZSgAwIBAgIBAzANBgkqhkiG9w0BAQQFADA3MQswCQYDVQQGEwJVUzER
MA8GA1UEChMITmV0c2NhcGUxFTATBgNVBAsTDFN1cHJpeWEncyBDQTAeFw05NzEw
MTgwMTM2MjVaFw05OTEwMTgwMTM2MjVaMEgxCzAJBgNVBAYTAlVTMREwDwYDVQQK
EwhOZXRzY2FwZTENMASGA1UECxEUHViczEXMBUGA1UEAxMOU3Vwcm15YSB0aGV0
dHkwZ8wDQYJKoZIhvcNAQEFBQADgY0AMIGJAoGBAMr6eZiPGfjX3uRJgEjmKiqG
7SdATYazBcABulAVyd7chrkiQ31FbXFOGD3wNktbf6hRo6EAmM5/R1AskzZ8AW7L
iQZBcrXpc0k4du+2Q6xJu2MPm/8WKuMonTuvzpo+SGXelmHVChEqooCwfdiZywyZ
NMmrJgaoMa2MS6pUkfQVAgMBAAGjNjA0MBEGCWCsSAGG+EIBAQQEAWIAGDAfBgNV
HSMEGDAWgBTy8gZZkHhUfWJM1oxeuZc+zYmyTANBgkqhkiG9w0BAQQFAAOBgQBt
I6/z07Z635DfzX4XbAfpj1Rl/AYwQzTSYx8GfcNAqCqCwaSDKvsuj/vwbf91o3j3
UkdGYpcd2cYRCgKi4MwqdWyLtpuHAH18hHZ5uvi00mJYw8W2wUOsY0RC/a/IDy84
hW3WWehBUqVK5SY4/zJ4oTjx7dwNMdGwbWfpRqjd1A==
```

-----END CERTIFICATE-----

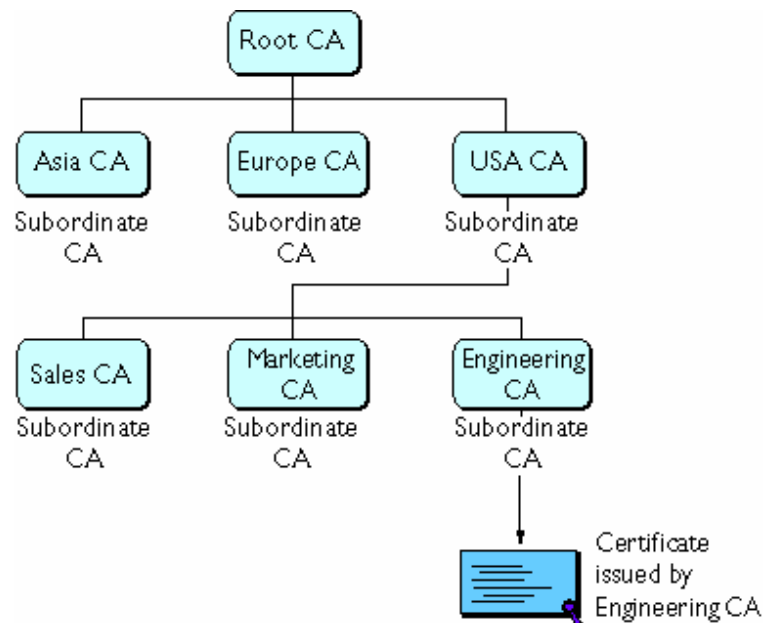
Rilascio di un certificato

- L'utente prova la propria identità alla CA (ad esempio mostrando un documento)
- L'utente crea una coppia di chiavi (pubblica e privata) e conferisce la pubblica alla CA in modo sicuro; a volte per generare e contenere la chiave privata viene utilizzata una smart card
- La CA crea un certificato digitale, che contiene la chiave pubblica dell'utente ed i dati identificativi
- Il certificato digitale è firmato elettronicamente con la chiave privata della CA
- In questa sequenza di operazioni, ovviamente, il punto debole della catena è il primo...

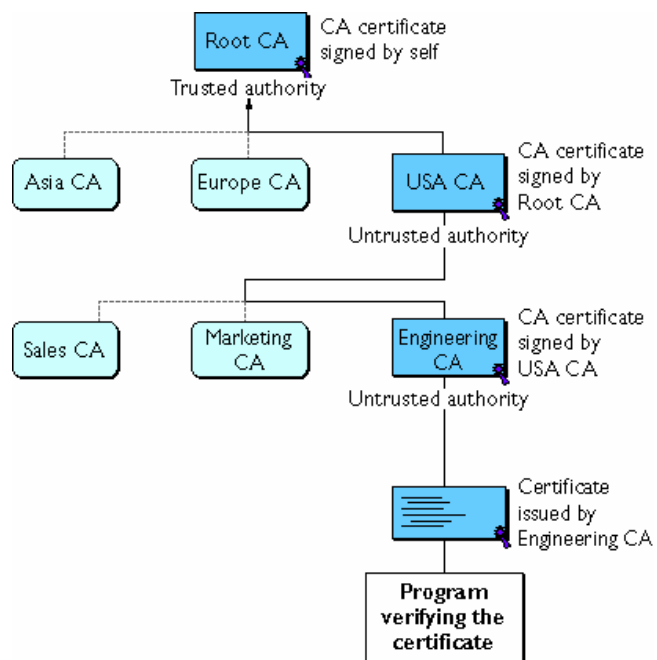
Catene e reti di certificazioni

- *Quis custodiebit custodes?*
- I certificati rilasciati da un'autorità possono essere garantiti soltanto da un'autorità di livello superiore, ma la catena va fermata...
 - autorità "pubbliche" alla sommità della catena
 - web-of-trust di PGP
 - Società specializzate i cui certificati sono "già presenti" nei maggiori browser (de facto)
- La CA di "top level" usa un certificato "self-signed"
 - Come distribuirlo, se non presente nel browser ?
- Problemi di prestazioni e di gestione delle revoche (CRL, Certificate Revocation Lists)

Esempio di gerarchia di Certification Authorities



Esempio di catena di certificazione



Procedura di verifica

- La firma sul documento corrisponde al documento?
 - Verifica dell'hash come spiegato in precedenza
- La chiave pubblica usata è quella del certificato?
 - Semplice confronto automatizzato
- Il certificato corrisponde alla persona?
 - Verifica del nome e altri dati (possibili problemi di omonimia, p.es.)
- La firma che convalida il certificato corrisponde al certificato?
 - Il certificato viene "validato" con lo stesso meccanismo di un documento, eventualmente risalendo la catena di autorità.
- La firma sul certificato è quella di un certificatore valido?
 - Bisogna che l'utente sia in qualche modo in possesso del certificato root a cui siamo giunti. Come?
- Il certificato non compare nella CRL del certificatore?
 - La lista è indicata nel certificato della CA. Ma se non possiamo raggiungerla, p.es. perché non siamo connessi ?
- **OMETTERE UNO DI QUESTI PUNTI CONDUCE A POSSIBILI ATTACCHI NELLO SCHEMA !**

Esempi di Certification Authorities

- **Provider commerciali internazionali**
 - **Verisign** (www.verisign.com)
- **CA riconosciute da AIPA (firma digitale a valore legale)**
 - Elenco completo su www.aipa.it
- **CA dipartimentali**
 - Per una singola azienda, p.es. il CED del Politecnico per i suoi dipendenti

Firma digitale a valor legale (fino ad oggi)

- Normata dal D.P.R. 513/97 e successive modificazioni;
- Basata sull'uso di certificati X.509 (come da DPCM 8/02/99) a bordo di strumenti di firma hardware modificabili solo all'origine (al momento smart card, ma non necessariamente)
- Rilasciata da certificatori abilitati iscritti nell'elenco AIPA e dotati di particolari requisiti (a livello di struttura societaria e di procedure)
- **Ha lo stesso valore di una firma su documento cartaceo, ma non può essere "disconosciuta" se non "a querela di parte"**
- Dico "fino ad oggi" perchè una nuova normativa è in via di elaborazione... ne parleremo

Utilità e inutilità della f.d.

- Cosa si può fare con la firma digitale:
 - firmare un contratto ("scrittura privata")
 - firmare documenti destinati alla P.A.
 - applicare una marca temporale a un documento
- Cosa non si può fare:
 - comprare una casa (l'atto notarile richiede la presenza): potete però usare la smart card presso il notaio!
 - firmare un referendum (dovete essere identificati da un pubblico ufficiale): potreste però usare la smart card al "banchetto"
- Per cosa non è utile una firma a valore legale
 - per il commercio online: avete mai firmato un contratto per comprare un oggetto al supermercato ?
 - per identificarsi verso un server remoto SSL: non avrebbe comunque valore legale !

I requisiti dei certificatori

- Forma di SpA e capitale sociale non inferiore a quello necessario ai fini dell'autorizzazione all'attività bancaria, se soggetti privati.
 - "legge bancaria", D. Lgs 1. settembre 1993, n. 385, art. 14, comma 1: "b) il capitale versato sia di ammontare non inferiore a quello determinato dalla Banca d'Italia". Dalle "Istruzioni" pubblicate sulla Gazzetta Ufficiale 21 febbraio 1994, n. 42 si tratta di 12.500.000.000 in lire.
- Competenza ed esperienza dei responsabili tecnici e del personale addetto siano sufficienti per rispettare le norme tecniche
- Qualità dei processi informatici e dei relativi prodotti, sulla base di standard riconosciuti a livello internazionale.

I requisiti dei certificatori

- Possesso da parte dei rappresentanti legali e dei soggetti preposti all'amministrazione, dei "requisiti di onorabilità" richiesti ai soggetti che svolgono funzioni di amministrazione, direzione e controllo presso banche (d. min. Tesoro, 18 marzo 1998, nr. 161, art. 5 e 6)
 - Non devono essere interdetti, inabilitati, falliti, o condannati all'interdizione, anche temporanea, dai pubblici uffici, o l'incapacità ad esercitare uffici direttivi, ex art. 2382 c.c.
 - Non devono essere stati sottoposti a misure di prevenzione e custodia cautelare
 - Non devono essere stati condannati con sentenza irrevocabile a pena detentiva:
 - Qualsiasi, per uno dei reati previsti dalle norme che disciplinano l'attività bancaria, assicurativa, etc.
 - Non inferiore a un anno per un delitto contro la p.a., contro la fede pubblica, contro il patrimonio, contro l'ordine pubblico, contro l'economia pubblica, o in materia tributaria;
 - Non inferiore a due anni per un qualunque delitto non colposo.
 - Idem dicasi per pene applicate "su richiesta delle parti"
 - Costituiscono cause di sospensione dalle funzioni di amministratore, sindaco e direttore generale le sentenze non definitive per quanto sopra, o l'applicazione provvisoria di una misura cautelare di tipo personale.

I certificatori accreditati

- **Certificatori attivi**

- Actalis S.p.A.
- BNL Multiservizi S.p.A.
- Cedacrinord S.p.A.
- Centro Tecnico per la RUPA
- Consiglio Nazionale del Notariato
- ENEL.IT S.p.A.
- Finital S.p.A.
- Infocamere SC.p.A.
- In.Te.S.A. S.p.A.
- I.T. Telecom S.p.A.
- Postecom S.p.A.
- Saritel S.p.A. (Società fusa per incorporazione nella I.T. Telecom S.p.A.)
- Seceti S.p.A.
- Trust Italia S.p.A.

- **Certificatori che hanno cessato l'attività**

- S.I.A. S.p.A. (dal 01/01/2003 - Certificatore sostitutivo Actalis S.p.A.)
- SSB S.p.A. (dal 01/01/2003 - Certificatore sostitutivo Actalis S.p.A.)

Alcuni punti fermi...

- Una firma "digitale" è persino più forte di una firma "reale"
 - Il documento firmato realmente può essere modificato, mentre una sequenza di bit firmata digitalmente, a meno di perdita della chiave privata o di vulnerabilità dell'algoritmo, non è modificabile
 - La firma reale è sempre uguale e può essere riprodotta, la firma digitale varia a seconda dei bit di informazione firmati
- Gli algoritmi di crittografia asimmetrica utilizzati per la firma digitale italiana sono fondamentalmente sicuri
 - La crittografia asimmetrica si basa, lo ricordiamo, sulla "sostanziale impossibilità" di invertire un'operazione matematica. Per ora tale presupposto non è stato compromesso da nessuno
- Tuttavia, alcuni problemi sono emersi...

Campi di cavoli amari...

- Bug scoperto il 9 settembre 2002
- Il software di firma di vari certificatori (originariamente rilevato su DiKe di Infocamere) consente di firmare documenti in formato Word contenenti campi dinamici
- In questi documenti il contenuto non cambia, ma ciò che viene mostrato all'utente sì !
- Il software non riesce a rilevare alcuna alterazione, e **non** informa di nulla l'utente...
- Info: www.elet.polimi.it/upload/zanero , sezione "bug e advisory"

Risultati ?

The image shows two overlapping windows. The left window is Microsoft Word, titled 'provaDiKe.doc - Microsoft Word'. The right window is DiKe, titled 'DiKe'. Both windows display the same text, but the DiKe window shows the results of a digital signature verification.

Microsoft Word Content:

Questo è un documento di prova scritto con MS Word 2000.
Nelle righe seguenti sono inseriti campi variabili tra asterischi:

Data e ora *17/09/2002 08.48.53*
I dati inseriti sono 17/09/2002 08.48.53

Data e ora *17/09/2002 08.48.53* (Questa non dovrebbe modificarsi)
I dati inseriti sono 17/09/2002 08.48.53

Nome del documento *provaDiKe.doc*
Dato inserito provaDiKe.doc

Nome autore *Manlio Cammarata*
Dato inserito Manlio Cammarata

Nome utente *Manlio Cammarata*
Dato inserito Manlio Cammarata

Ora il file sarà firmato digitalmente con DiKe e dovremo controllare se la verifica va a buon fine anche dopo l'aggiornamento dei campi.

DiKe Content:

Nr. Firmatari: 1
Firmatario: 1 CAMMARATA MANLIO;Cod. Fiscale:CMMMNL47P04L424H;Identificativo:200111111812
Stato:IT;Organizzazione:Non Dichiarato;Unità Organizzativa:RA=NFOCAMERE S.C.p.A.
[verifica completata correttamente](#)

Documento: d:\test\provaDiKe18.doc.p7m Dimensioni: 21944 Data: 18/09/2002 14.20.44

Questo è un documento di prova scritto con MS Word 2000.
Nelle righe seguenti sono inseriti campi variabili tra asterischi:

Data e ora *18/09/2002 14.28.15*
I dati inseriti sono 17/09/2002 08.48.53

Data e ora *17/09/2002 08.48.53* (Questa non dovrebbe modificarsi)
I dati inseriti sono 17/09/2002 08.48.53

Nome del documento *provaDiKe.doc*
Dato inserito provaDiKe.doc

Nome autore *Manlio Cammarata*
Dato inserito Manlio Cammarata

Nome utente *Manlio Cammarata*
Dato inserito Manlio Cammarata

Ora il file sarà firmato digitalmente con DiKe e dovremo controllare se la verifica va a buon fine anche dopo l'aggiornamento dei campi.

La risposta del certificatore

- P. Sacconi di InfoCamere, in vari interventi, sostiene che:
 - Il difetto è di **scarso rilievo**, perché i documenti Word con campi dinamici non possono essere usati nella pubblica amministrazione. L'art. 4 della del. AlPA 51/2000 richiede per i formati dei documenti della P.A. "almeno [...] b) la non alterabilità del documento durante le fasi di accesso e conservazione; [...] d) l'immutabilità nel tempo del contenuto e della sua struttura. A tale fine i documenti informatici non devono contenere macroistruzioni o codice eseguibile, tali da attivare funzionalità che possano modificarne la struttura o il contenuto".
 - DiKe, come qualsiasi altro software di firma digitale, nel momento in cui provvede all'apposizione della firma ed alla successiva verifica non fa altro che firmare (e verificare) il **contenuto di un documento** (o meglio ad estrarre un hash del suo contenuto ed a firmare e verificare la firma apposta sullo stesso).
 - **Non è possibile** disattivare le macro di Office dall'esterno
 - La variazione dei valori contenuti nella macro non comporta alcuna alterazione del documento. DiKe, quindi, **si comporta correttamente** fornendo un esito positivo della verifica di firma in quanto non vi è stata alcuna rottura dell'integrità del **documento**.
 - "Ci aspettiamo una soluzione normativa a questi problemi", dice Sacconi: il bug, secondo InfoCamere, sta nella **normativa**. Ma è così?

Il programma o le norme ?

- Il programma esegue correttamente la verifica crittografica: la stringa di bit non è cambiata. Su questo Sacconi ha ragione
- Tuttavia, il programma aderisce alla norma sulla firma digitale ?
- Art. 1, T.U. sulla doc. amministrativa: il documento informatico è "*la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti*". Rappresentazione: ciò che si vede, non il mezzo.
- La firma digitale va applicata non al **file** che è un mero accidente, ma al **documento**. Se il software verifica l'integrità non del **documento** in senso **giuridico**, ma solo quella del file ("evidenza informatica", dicono le norme tecniche) sul quale è stato calcolato l'hash e quindi generata la firma stessa, esso verifica l'integrità dell'**evidenza informatica**, che non ha alcun valore legale!
- Un notaio firmerebbe un *documento* scritto a matita ?
- DPCM 8 febbraio 1999 art. 10 c. 1: "Gli strumenti e le procedure utilizzate per la generazione, l'apposizione e la verifica delle firme digitali debbono presentare al sottoscrittore, **chiaramente e senza ambiguità**, i dati a cui la firma si riferisce". Di nuovo, la tesi di InfoCamere viene smentita.

Possibili soluzioni

- Si potrebbero “squalificare” a priori i formati modificabili, conservando p.es. solo il formato pdf, testo, e i formati immagine: questo è operativamente poco efficiente
- L'applicazione di firma potrebbe mostrare una copia in pdf del documento al momento della firma, e firmare quest'ultima. Ciò creerebbe sicuramente problemi di compatibilità e di “royalty” per i certificatori
- Microsoft, il 30 gennaio 2003, ha completato una patch per Office per consentire la disabilitazione dei campi dall'esterno
- Lo stesso DiKe nella nuova versione mostra una finestra di avvertimento... quindi forse non avevo tutti i torti ;-)
- Andrebbero “validati” i sistemi di decodifica per tutti i formati complessi... impensabile
- Uso di XML/SIG ? Potrebbe essere il futuro!

Il secondo baco: Firma&Cifra

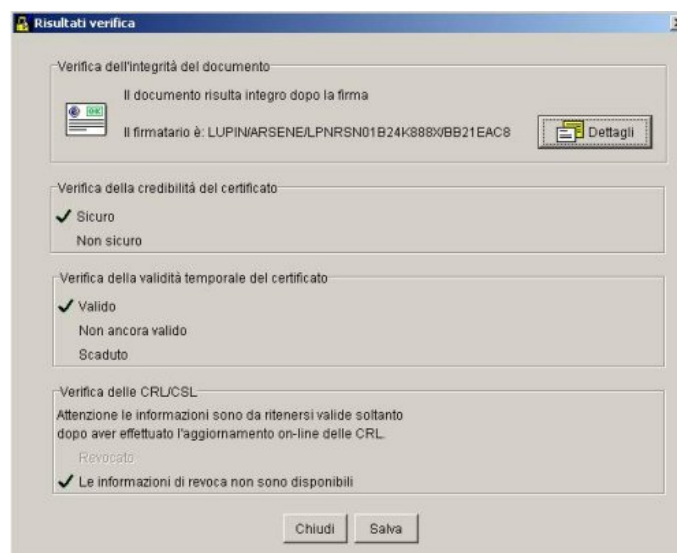
- Firma&Cifra è l'applicativo di PostECom per la firma digitale
- Baco segnalato da anonimo il 20 marzo 2003
<http://www.interlex.it/docdigit/sikur159.htm>
- Risultato del bug: possibilità di creare qualsiasi certificato falso e di far verificare una firma apposta con tale certificato a Firma&Cifra
- Anche in questo caso, il problema non sono gli algoritmi crittografici...

Il meccanismo del bug

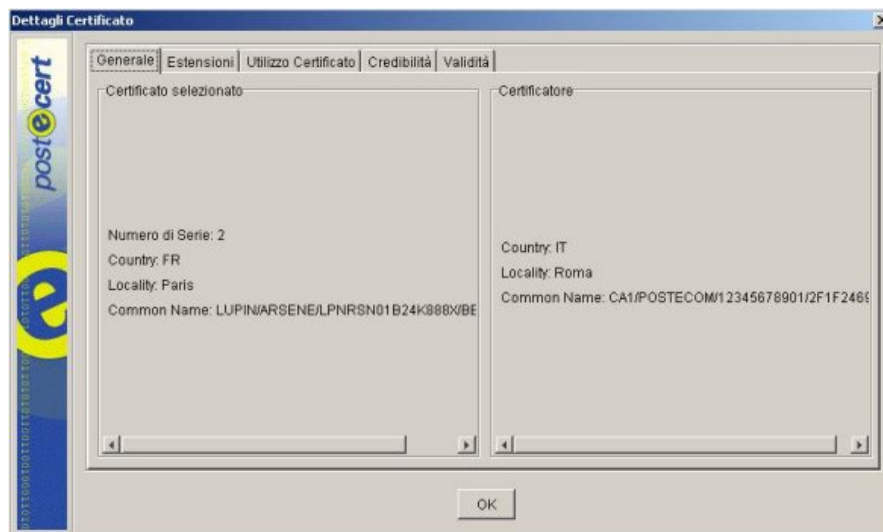
- Per verificare una firma bisogna disporre del certificato che l'ha generata
 - Teoricamente esso potrebbe essere recuperato online da un server, ma questo "sovraccaricherebbe" il repository
 - Per rimediare, nella firma in formato PKCS#7 della norma italiana viene allegato il certificato utente usato per firmare, che viene poi validato
- Normalmente, per verificare un certificato, si controlla la firma apposta dal certificatore, usando un certificato di root
 - I certificati di root sono disponibili sul sito dell'AIPA, ma vengono "preinstallati" in maniera sicura con il software di verifica
 - L'archivio dei certificati di root è quindi un'area di sicurezza critica per il software
- Firma&Cifra commette un errore fatale: se nella struttura PKCS#7 non si include soltanto il certificato utente, ma anche il certificato root utilizzato per firmare il certificato utente, **il software non va a cercare quello ufficiale**, ma si "accontenta" di quello fornito e decreta che la firma è autentica!

La firma di Arsène Lupin

- Generiamo un falso certificato root inserendo una denominazione uguale a quella di uno dei certificatori dell'elenco pubblico (nel nostro esempio PosteCom)
- Usiamo questo certificato per firmare un falso certificato intestato al soggetto che si vuole impersonare (nell'esempio Arsène Lupin)
- Usiamo il falso certificato di Arsène Lupin per firmare il documento
- Aggiungiamo al documento firmato il falso certificato di Postecom



Sempre Arsène Lupin...



- Roberto Palombo (PosteCom), nella sua "risposta" ad InterLex, arriva a sostenere che questo comportamento è "by design", e che si limiteranno a rilasciare un aggiornamento che richieda "una più esplicita volontà dell'utente nell'importare un certificato di root."

Le soluzioni...

Il comportamento di un altro software:

✓	Stato della firma:	Valido
✗	Stato del certificato:	Verifica fallita
i	Errore:	Error # 43, "Non trovato nel database un valido certificato del certificatore"

- La "soluzione" è quanto mai semplice: implementare correttamente il software
- Spacciare quella di Firma&Cifra per una "lieve" svista è quantomeno riduttivo e fuorviante

Bug o non bug?

- 13 maggio 2003, varie testate, online e cartacee, annunciano: "Il Laboratorio di Sicurezza e Reti del Dipartimento di informatica e comunicazione dell'Università degli Studi di Milano ha condotto la prima realizzazione pratica a livello mondiale di attacco riuscito a un dispositivo di firma digitale..."
- Abbiamo dimostrato, nelle "slide" precedenti, come non si tratta della prima realizzazione pratica nemmeno a livello italiano...
- Inoltre, a quanto è dato capire, non si tratta nemmeno di un bug o di un attacco al dispositivo di firma, in quanto il team dell'università di Milano ha utilizzato un trojan per "firmare" documenti all'insaputa dell'utente.
- È del tutto chiaro che su una macchina compromessa l'uso di **qualsiasi** tipo di software non può essere in alcun modo garantito !
- Su questo argomento non è stata pubblicata una advisory. Non sono stati descritti i dettagli. Non ci sono state pubblicazioni scientifiche. Restano dei dubbi su quale sia l'elemento veramente nuovo.
- È però reale problema di **garantire la sicurezza della piattaforma di firma**, che è difficile se pensiamo di dotare degli strumenti di firma digitale l'utente "qualunque"

Le nuove direttive

- Non è possibile essere “chiari” perché i testi in sé sono nebulosi e contraddittori. Proviamo ad esaminare qualche definizione dal testo del decreto:
- **“Firma elettronica”**: l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di autenticazione informatica
 - La firma elettronica non è la firma digitale?
 - Una firma non è solo un metodo di autenticazione, ma di controllo di integrità!
 - La definizione è quanto mai fallace
- **“Firma elettronica avanzata”**: la firma elettronica ottenuta attraverso una procedura informatica che garantisce la connessione univoca al firmatario e la sua univoca identificazione, creata con mezzi sui quali il firmatario può conservare un controllo esclusivo e collegata ai dati ai quali si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati;
 - Invece la firma elettronica non è collegata ai dati?
- **“firma elettronica qualificata”**: una firma avanzata creata con un certificato qualificato (vedi slide seguenti)
- **“firma digitale”**: una firma qualificata creata usando uno schema a chiavi asimmetriche (?!)

Le nuove direttive (2)

- **"certificatori"**: coloro che prestano servizi di certificazione delle firme elettroniche o che forniscono altri servizi connessi alle firme elettroniche;
 - Un certificatore non certifica le firme, ma i certificati, come dice il nome
 - I servizi del certificatore non c'entrano, necessariamente, con la firma
 - **L'attività dei certificatori è libera**: questa sarebbe la grande novità del provvedimento, ma è esattamente la situazione precedente, con l'orribile differenza che i certificati prodotti da certificatori qualsiasi assumono un valore sproporzionato
- **"certificatori accreditati"**: i certificatori accreditati in Italia ovvero in altri Stati membri dell'Unione europea, ai sensi dell'articolo 3, paragrafo 2, della direttiva 1999/93/CE;
 - Sarebbero l'equivalente dei certificatori iscritti nell'elenco AIPA

Le nuove direttive (3)

- **"certificati elettronici"**: gli attestati elettronici che collegano i dati utilizzati per verificare le firme elettroniche ai titolari e confermano l'identità dei titolari stessi;
 - Miracolosamente, questa definizione pare quasi giusta
- **"certificati qualificati"**: i certificati elettronici conformi ai requisiti di cui all'allegato I della direttiva 1999/93/CE, rilasciati da certificatori che rispondono ai requisiti fissati dall'allegato II della medesima direttiva;
- **"accreditamento facoltativo"**: il riconoscimento del possesso, da parte del certificatore che lo richieda, dei requisiti del livello più elevato, in termini di qualità e di sicurezza.

Una sintesi dei problemi

- Il testo modifica catastroficamente il quadro normativo esistente, attribuendo validità e un forte valore probatorio ad un documento sottoscritto con firma "leggera"
- Questa estensione va oltre la previsione comunitaria, che impone solo che a tale documento non sia negato il valore probatorio.
- Si introduce una "carta nazionale dei servizi", non prevista dalla legge delega. Si ammette la presentazione di atti e istanze alla pubblica amministrazione con la semplice identificazione del mittente attraverso la carta d'identità elettronica, senza alcuna garanzia per eventuali alterazioni del contenuto (i.e. uso del certificato per l'identificazione)

Una sintesi dei problemi

- Le definizioni sono confuse, quando non giuridicamente sbagliate ("autenticazione" invece di "validazione" della firma) e in totale disarmonia con quelle della normativa in vigore. Si parla di firma elettronica, digitale, debole, forte, sicura, in un carosello infinito di confusione
- **Il testo esce plurimamente dai limiti della legge delega per il recepimento**, intervenendo su tutto tranne che sull'unica norma da emendare per l'attuazione della direttiva: l'art. 15, comma 2, della legge 59/97 (che andava emendata aggiungendo la precisazione della necessità della firma "sicura" e aggiungendo una disposizione sul divieto di negare valore probatorio a una firma per il solo fatto che è in forma elettronica o non sicura).
- Eccezione di costituzionalità ?

Per ridere un po'

Da un comunicato del Ministro per l'Innovazione e le Tecnologie, agosto 2002:

"... La firma digitale è un **software contenuto in una smart card** - una sorta di carta bancomat - che, inserita in un apposito lettore collegato al computer, consente di firmare qualsiasi tipo di documento elettronico...

Il provvedimento approvato oggi introduce due novità sostanziali rispetto alla normativa precedente: la **liberalizzazione del settore dei servizi di certificazione, che elimina così la necessità di una preventiva autorizzazione** per l'esercizio di questa attività, e l'introduzione di due categorie di firma digitale. Sarà disponibile una **firma leggera - utile per l'identificazione personale** e l'accesso ai servizi della Pubblica amministrazione - e **una firma pesante, con la massima sicurezza per la sottoscrizione di documenti più rilevanti.**

Col nuovo Regolamento, potrà essere conferito valore legale ai documenti elettronici, garantendo al contempo l'autenticità della firma e del soggetto da cui proviene e, insieme, l'integrità del documento stesso."

Riferimenti web

- Mailing list italiane sulla sicurezza:
www.sikurezza.org
- Legislazione di Internet:
www.interlex.it
- Portale sulla sicurezza informatica:
www.securityfocus.com

Questions ? :-)

Grazie per l'attenzione !

Stefano Zanero

zanero@elet.polimi.it

www.elet.polimi.it/upload/zanero