Crittografia, Firma Digitale e PEC

(Una vechia guida dimenticata del 2006 ma ancora molto attuale)

Augusto Scatolini (webmaster@comunecampagnano.it)
Ver. 1.0 Giugno 2010

- -

CRITTOGRAFIA, FIRMA DIGITALE
e PEC (Posta Elettronica Certificata)

(¯`·._.·´¯`·._ Parte 1° _.·´¯`·._.·´¯)

(¯`·._.·´¯`·._ Parte 2° _.·´¯`·._.·´¯)

(¯`·._.·´¯`·._ Parte 3° _.·´¯`·._.·´¯)

(¯`·._.·´¯`·._ ° _.·´¯`·._.·´¯`·._.·´¯`·._ ° _.·´¯`·._.·´¯`·._.·´¯`·._ ° _.·´¯`·._.·´¯`·._.·´¯`·._ ° _.·´¯`·._.·´¯)

Premessa Back

"La norma è incerta", così si usa dire quando di una legge non si capisce niente! Parliamo della posta elettronica certificata. L'introduzione di questa meraviglia dovrebbe rendere possibile un esempio di questo tipo: "*Un cittadino, o un'azienda, dalla postazione informatica della propria abitazione chiede ad una pubblica amministrazione, tramite posta elettronica certificata, un documento elettronico firmato digitalmente dal Responsabile del procedimento e chiede di riceverlo con lo stesso mezzo, possibilmente crittografato*." Ora è un suo diritto!
Tralasciando il fatto che per tentare di usare una casella di posta elettronica certificata si deve comunque essere in possesso di un personal computer, di una connessione ad internet, e saper sopravvivere tra virus, cavalli di troia, spie, dialer, vermi, hacker, cracker, patch, hot fix e altre simpatiche diavolerie;
Ma cos'è una casella di posta certificata? Dove si prende? Quanto costa? Come si usa?
La firma digitale è forse la propria firma passata sotto uno scanner?
Che differenza c'è tra firma elettronica, digitale, debole, forte, certificata, avanzata, qualificata?
Cos'è la chiave privata, la chiave pubblica, il certificato digitale, chi me lo da?
Firmo elettronicamente il mio documento con la mia chiave privata?
Crittografo il mio documento elettronico con la chiave pubblica del destinatario?
E' meglio la crittografia simmetrica a chiave unica o quella asimmetrica a doppia chiave?
E' vero che i cinesi hanno già "craccato" la firma digitale che ancora non riesce a prendere il via?
"La norma è incerta" ma qui anche la materia è incerta.
Questo scritto, ripreso come un collage da più fonti, è un mite tentativo di fare un po' di chiarezza, almeno sui termini. Partendo dalla crittografia che è la base della firma elettronica per arrivare alla posta elettronica certificata che appunto usa firme e certificati elettronici.

Crittografia Back

Echelon e' un nome in codice che si riferisce ad una rete informatica, segreta fino al 1997, capace di controllare l'intero globo e di intercettare, selezionare e registrare ogni forma di comunicazione elettronica. E' composta da satelliti artificiali, super computer (definiti *dizionari*) e un certo numero di stazioni a terra in grado di ricevere informazioni dai satelliti artificiali presenti in orbita. Dopo un'inchiesta della BBC, e la voce di alcuni parlamentari del Governo australiano, e di un giudice romano, c'è la conferma che Echelon esiste. Echelon è stato progettato da USA, Gran Bretagna, Canada, Australia, Nuova Zelanda con il compito di monitorare le comunicazioni. Nel 1997 anche l'Unione Europea diede l'allarme. Ed i Paesi coinvolti non hanno voluto dare nessuna spiegazione al riguardo.
Storicamente, nel 1947 gli Stati Uniti e la Gran Bretagna hanno stipulato un accordo segreto per proseguire la loro collaborazione nell'attività di spionaggio gia' iniziata durante la guerra, volta ad intercettare principalmente comunicazioni radio sovietiche. Tale accordo e' noto come patto UKUSA, al quale successivamente si sono aggiunti, come parti secondarie, il Canada, la Nuova Zelanda e l'Australia.
Letteralmente il termine Echelon vuol dire "gradino". Secondo quanto scritto dalla ricercatrice freelance e giornalista investigativa Susan Bryce : "UKUSA e' un accordo *a gradini,* la NSA e' chiamata *primo partito...* rispetto agli altri paesi dell'accordo, si assume l'impegno di numerose operazioni clandestine. Fu allestita senza alcuna legislazione ufficiale e non c'è nulla, legalmente, che non possa fare.
La crittografia, dal greco "crypto" (nascondere) e "graphein" (scrivere), è l'arte di progettare algoritmi (cifrari) per crittografare un messaggio rendendolo incomprensibile a tutti tranne al suo destinatario che con un algoritmo simile deve essere in grado di codificarlo, attraverso un parametro segreto detto chiave, usata in precedenza anche dal mittente per la cifratura. La sicurezza di un sistema di crittografia risiede solo ed esclusivamente nella segretezza della chiave e non dell'algoritmo che è opportuno far conoscere alla pubblica analisi, in modo che se ne possano scoprire eventuali punti deboli in tempo. Questo principio, noto come principio di Kerckhoffs, che lo enunciò nel 1883, dice in sostanza che il metodo è più sicuro quanto è più difficile scoprire la chiave segreta conoscendo l'algoritmo che l'ha generata.

Tecniche di crittografia Back

I vari cifrari e gli algoritmi di crittografia usano varie tecniche, applicate singolarmente o in combinazione fra loro. Fra le altre tecniche:

* Trasposizione consiste nel rimescolare i caratteri del testo in chiaro secondo una regola prestabilita. Un esempio di questo metodo è lo Scitala lacedemonica.
* Monoalfabetico sono classificabili in questo metodo, la Cifratura di Cesare, Rot-13, Atbash.
* Polialfabetico con questo metodo la cifratura di più gruppi di segni assume più significati. I cifrari di questa categoria sono: codice Vigenere, disco cifrante Alberti, dispositivo di Jefferson, macchina Enigma, cifrario Vernam.
* Poligrafico è un metodo in cui i caratteri in chiaro sono sostituiti a gruppi di due o più caratteri. I cifrari sono: Scacchiera di Polibio, Playfair, Delastelle.
* Composti i cifrari composti fanno uso di varie tecniche in successione. Oppure sono applicati vari metodi di criptazione sullo stesso blocco di testo. Questo metodo rappresenta gli algoritmi moderni, applicabili anche grazie ai sistemi informatici. Tra questi: DES, IDEA.
* Chiave pubblica come per il metodo precedente, è un cifrario moderno. Ad esempio il codice RSA.

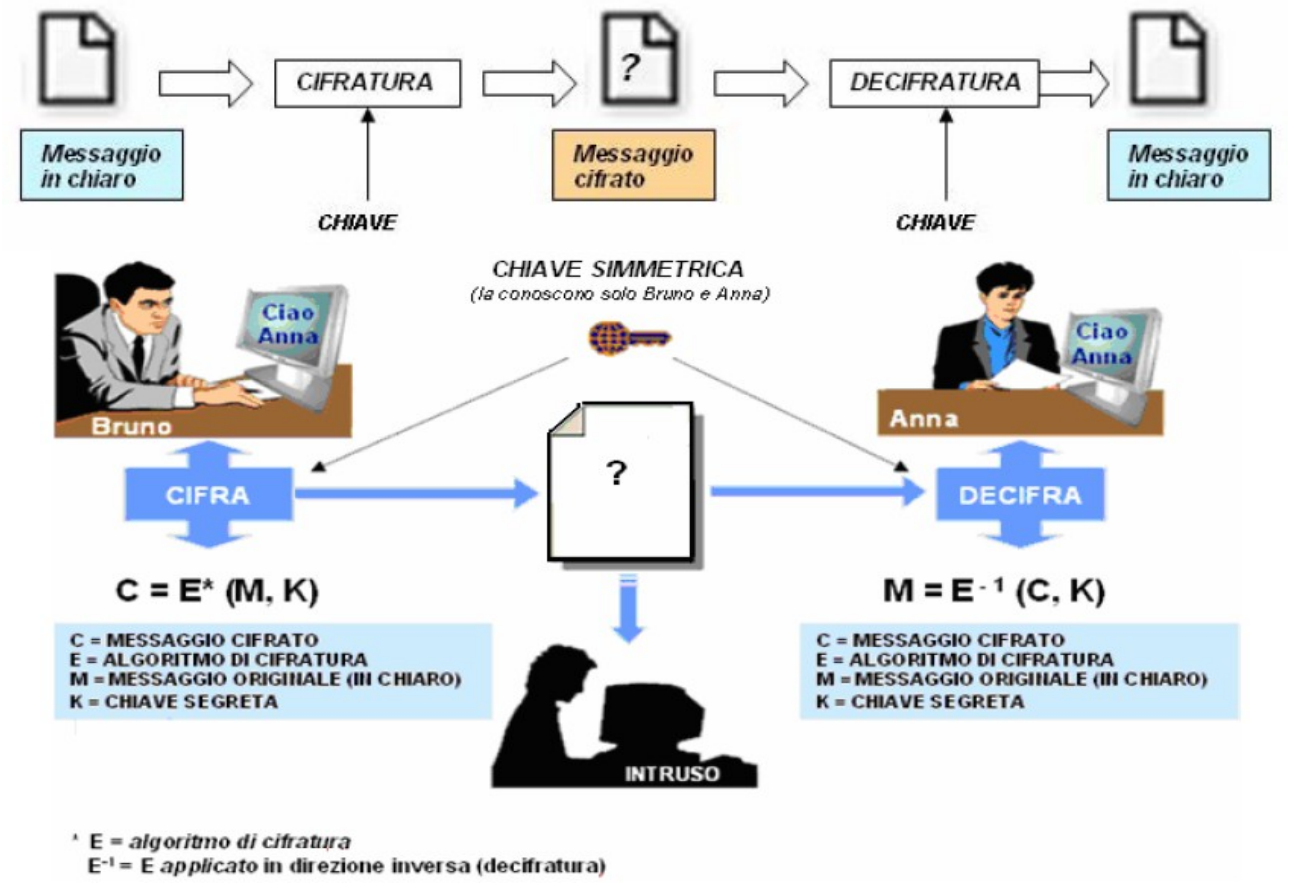
Crittografia a chiave simmetrica (o privata) e Crittografia a chiave asimmetrica (o pubblica) Back

Un algoritmo di crittografia riceve un testo da codificare (detto testo in chiaro o Plain-text) e lo trasforma, attraverso la chiave, in un testo cifrato (Cipher-text) apparentemente incomprensibile. I passaggi di cifratura e decifratura del testo vengono solitamente indicati in questo modo:

cifratura: M = Ck(Mc)

decifratura: Dk(Ck(M)) = M

dove M è il messaggio da cifrare, C è l'algoritmo di codifica, D quello di decodifica e k la chiave per i due algoritmi. I metodi di crittografia di questo tipo, cioè che utilizzano la stessa chiave per la codifica e la decodifica sono detti a chiave segreta (o simmetrici). Altri metodi che utilizzano due chiavi diverse per la codifica e la decodifica vengono detti a chiave pubblica (o asimmetrici).



* E = *algoritmo di cifratura*
E^{-1} = E *applicato* in direzione inversa (decifratura)

Algoritmi Back

Gli algoritmi simmetrici usano un sistema per cifrare che può essere a flusso o a blocchi. Se a flusso, il codice cripta un bit, byte o una parola alla volta. Se a blocchi, viene applicato ad un gruppo di bit, byte o parole. A seconda dell'applicazione utilizzata viene usato l'uno o l'altro. Il sistema di maggiore utilizzo è quello a blocchi. Sull'algoritmo simmetrico c'è poco da dire: l'utente A cifra il documento mediante una chiave k, ed il destinatario usa sempre questa chiave k per decifrare il messaggio. Se la chiave scelta viene consegnata di persona al proprio interlocutore allora un minimo di sicurezza esiste. Ma se le persone sono distanti? Come fare a scambiarsi la chiave mediante un canale sicuro? Perché internet non è un canale sicuro. La soluzione a questo problema consiste nell'utilizzare un sistema a doppia chiave, un algoritmo asimmetrico.

Gli algoritmi simmetrici a blocchi Back

- BLOWFISH algoritmo creato da Bruce Schneier. L'autore ha implementato nel cifrario varie tecniche, fra cui Feistel network, S-box dipendenti da chiavi, funzioni non invertibili ed altro ancora. In sostanza è uno dei più sicuri.
- CAST sviluppato da Carlisle Adams e Stafford Taveres, utilizza un sistema di permutazioni-sostituzioni, nonché altre tecniche. David Wagner, John Kelsey e Bruce Schneier hanno scoperto un attacco su una chiave di 64 bit, comunque l'attacco non è efficace al 100%. Sono state sviluppate versioni successive del CAST ed attualmente non è stato ancora violato (in particolare il CAST5). L'algoritmo è registrato dalla Entrust Technologies, ed è disponibile il codice sorgente.
- CMEA progettato dalla Telecommunications Industry Association, per l'utilizzo nella telefonia cellulare, fa uso di chiavi a 64 bit con lunghezza del blocco variabile. E' usato nella cifratura dei canali di controllo dei cellulari. E' stato brillantemente attaccato da David Wagner, John Kelsey e Bruce Schneier della Counterpane Systems.
- DES Il DES (Data Encryption Standard) è un cifrario composto, sviluppato dall'IBM, modificato dalla National Security Agency (NSA) e adottato dal governo statunitense nel 1977 ufficialmente per la protezione di dati riservati ma non classificati come “segreti militari” o di “stato”. Il 17 luglio 1998 la Electronic Frontier Foundation (EFF) diffonde un comunicato stampa con il quale annuncia la definitiva sconfitta del DES. Per dimostrare i gravi rischi di sicurezza a cui si sottopone chi utilizza il DES, la EFF costruisce il primo apparecchio hardware non coperto dal segreto di stato per decodificare i messaggi crittografati utilizzando il Data Encryption Standard. In meno di un anno viene costruito un calcolatore costato 250.000 dollari che in meno di sessanta ore era capace di forzare un messaggio cifrato con DES.
- FEAL acronimo di Fast Data Encipherment Algorithm, creato dalla Nippon Telephone & Telegraph, il cui scopo era riuscire a rimpiazzare il DES, ma si è rilevato una buca, poiché è molto insicuro.
- GOST cifrario creato ed utilizzato in Russia, anche questo con lo scopo di rimpiazzare il DES. Usa 32 cicli per l'operazione di criptazione con chiavi di 256 bit. E' molto più sicuro del precedente, comunque è stato violato nel 1996 da John Kelsey.
- IDEA **IDEA** (*International Data Encryption Algorithm*) è nato nel 1991 sotto il nome di **IPES** (*Improved Proposed Encryption Standard*), ed è stato progettato da due famosi ricercatori dello **Swiss Federal Institute of Technology: Xuejia Lai** e **James L. Massey**. Come il *DES*, è un codice cifrato a blocchi di 64 bit, la differenza sta nel fatto che questa volta però la chiave è di 128 bit, che dovrebbe eliminare qualsiasi possibilità di riuscita di ricerca della chiave procedendo per tentativi (attacco *brute force*): le possibili combinazioni sono infatti *2^128*. Fino a questo momento ha resistito agli attacchi di numerosi crittoanalisti mondiali. *IDEA* è al momento il cifrario a chiave segreta più utilizzato per quanto riguarda i software commerciali di crittografia vista la sua velocità di codifica e decodifica nonché la sua elevata sicurezza.
- LOKI studiato come rimpiazzo per il DES, utilizza chiavi di 64 bit su blocchi della stessa lunghezza. Alcuni test di crittoanalisi hanno dimostrato che è insicuro.
- LUCIFER è stato sviluppato nel 1960 dall'IBM, dal ricercatore Horst Feistel. La crittoanalisi ha dimostrato la sua insicurezza.
- MACGUFFIN cifrario sviluppato da Matt Blaze e Bruce Schneier come esperimento. Esso divide i blocchi di 64 bit in due parti, rispettivamente di 16 e 48 bit. E' stato trovato un attacco di crittoanalisi.
- MARS è un altro cifrario progettato dall'IBM, adopera blocchi di 128 bit per la cifratura, e supporta chiavi di lunghezza tra 128 e 1248 bit. E' unico perché utilizza tutte le tecniche di cifratura/decifratura conosciute: addizioni, sottrazioni, rotazioni a virgola fissa e mobile, prodotti, trasposizioni e tutto il resto.
- MISTY dopo la violazione del DES, molti fanno a gara per trovare un degno rimpiazzo. Fra questi la Mitsubishi Electric, che crea questo sistema di crittografia in grado di resistere alla crittoanalisi lineare e differenziale. E' ancora in fase di test.
- MMB il progetto aveva lo scopo di rimpiazzare il cifrario IDEA, ma non è riuscito poiché sono stati portati a termine molti attacchi nei suoi confronti.
- NEWDES sviluppato come alternativa al DES da Robert Scott, è stato violato quasi subito.

- RC2, RC4 cifrari segreti di cui David Wagner, John Kelsey e Bruce Schneier hanno scoperto un attacco.
- RC5 è un gruppo di algoritmi sviluppati da Ron Rivest della RSA Data Security Inc., che lavorano su blocchi di dati, chiavi e numeri casuali di lunghezza variabile. Con chiavi a 32 bit l'RC5 lavora su blocchi di 64 bit. David Wagner, John Kelsey e Bruce Schneier hanno scoperto punti deboli dell'ordine fra 2 e 10r, con r che rappresenta il numero di tentativi. Se il numero di tentativi è maggiore di 10 non ci sono problemi di sicurezza. Un attacco di crittoanalisi differenziale è stato trovato.
- RC6 creato su richiesta della Ronald Rivest's AES, opera su blocchi di 128 bit ed accetta chiavi di lunghezza variabile. Fa uso di prodotti per il calcolo delle rotazioni.
- REDOC è un cifrario considerato sicuro. Ne esistono attualmente due versioni, di cui una insicura. Utilizza chiavi di 160 bit su blocchi di 80 bit.
- RIJNDAEL sistema di crittografia sviluppato dai matematici belgi Joan Daemen e Vincent Rijmen su richiesta della Advanced Encryption Standard (AES), fa uso di chiavi di lunghezza variabile (128, 182 e 256 bit). Viene nominato come standard AES, in sostituzione del DES. E' implementato via software in molti linguaggi: C/C++, Java, Lisp, Phyton ed anche in Perl e Javascript.
- SAFER creato da Robert Massey per la Cylink Corporation. Le chiavi possono essere di 40, 64 e 128 bit. Ha resistiti ad alcuni attacchi fatta dalla crittoanalisi lineare e differenziale.
- SERPENT algoritmo progettato da Ross Anderson, Eli Biham e Lars Knudsen, su richiesta della AES. Il Serpent adopera chiavi di 256 bit su blocchi di 128 bit, ed ha resistito alla crittoanalisi lineare e differenziale. Contiene delle permutazioni iniziali e finali, così come il DES.
- SQUARE cifrario a blocchi iterativi di 128 bit su chiavi anch'esse di 128 bit. La funzione di arrotondamento di questo algoritmo consiste in una trasformazione lineare, una trasformazione non-lineare, una permutazione sui byte, ed un'addizione sui bit con la chiave. Anch'esso è stato progettato per resistere alla crittoanalisi lineare e differenziale.
- SKIPJACK è stato rilasciato dalla National Security Agency (NSA), utilizza chiavi di 80 bit. Eli Biham e Adi Shamir hanno pubblicato i primi risultati di crittoanalisi, tuttavia ancora non si può dire se è sicuro oppure no.
- TEA acronimo di Tiny Encryption Algorithm, il cui scopo è quello di ottimizzare la velocità e lo spazio di memoria occupato. Questa ottimizzazione ha portato però il cifrario ad essere insicuro.
- TWOFISH è stato sviluppato dal team della Counterpane Systems' AES (Bruce Schneier, John Kelsey, Doug Whiting, David Wagner, Chris Hall e Niels Ferguson) e dichiarato sicuro dopo averlo analizzato. Fa uso di chiavi da 256 bit.

Gli algoritmi simmetrici a flusso Back

- ORYX come il CMEA, è usato per criptare i dati delle comunicazioni dei cellulari. David Wagner, John Kelsey e Bruce Schneier sono riusciti ad attaccare il cifrario, basandosi sulla conoscenza di 24 byte di un testo cifrato con circa 216 parametri iniziali.
- RC4 algoritmo della RSA Data Security Inc. E' usato in vari tipi di applicazioni ed al momento non ci sono attacchi conosciuti. La versione a 40 bit in passato era stata violata.
- SEAL acronimo di Software Encryption ALgorithm, sviluppato da Don Coppersmith della IBM, è uno dei più veloci.

Algoritmi asimmetrici Back

- Curve ellittiche basato sui numeri di una curva ellittica definita su un campo finito. Si dice che abbia un livello di sicurezza superiore a quello basato sulla fattorizzazione intera o sul calcolo dei logaritmi discreti (Diffie-Hellman, RSA, ElGamal).
- DSA acronimo di Digital Signature Algorithm inglobato nel Digital Signature Standard (DSS), è un cifrario usato per generare le firme digitali, più debole rispetto ad esempio all'RSA. Il software GnuPG lo usa con ELGAMAL per la creazione delle coppia di chiavi pubblica e privata. Non adatto per la crittografia dei dati.
- ELGAMAL sistema crittografico inventato da Taher Elgamal nel 1985 è basato sul problema dei logaritmi discreti. Questo algoritmo è simile a Diffie-Hellman ma un po' più lento, ed il sistema di criptazione che implementa è diverso. E' usato per la creazione della chiave privata, nonché per cifrare i dati. Ne fa uso il programma GnuPG.
- RSA descrizione più avanti.

Algoritmi per il calcolo dell'hashing di un documento Back

- MD4 algoritmo di hash considerato sicuro ed alla base delle funzioni Hash. Il messaggio viene suddiviso in blocchi di 512 bit, poi tramite una struttura iterativa il blocco viene elaborato da una funzione di compressione sui blocchi di 512 bit per la generazione del valore hash. L'output ha una lunghezza di 128 bit. Hans Dobbertin ha sviluppato un attacco a questo algoritmo, in grado di generare collisioni in un minuto di tempo di calcolo su un normale computer.

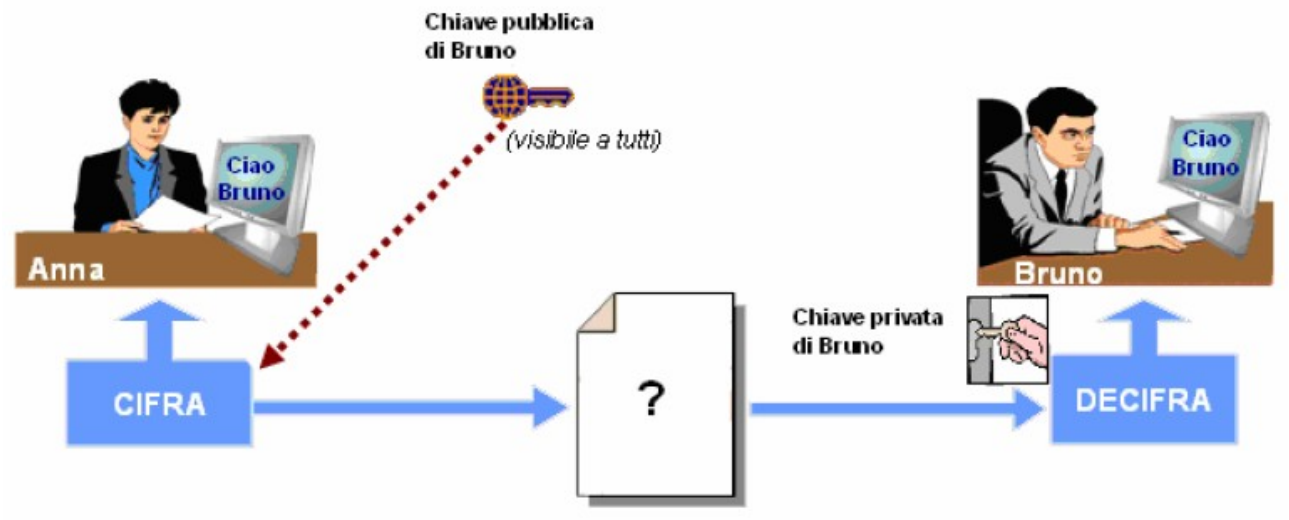
- MD5 questo algoritmo è stato concepito in modo da essere più sicuro rispetto a MD4. Sempre Hans Dobbertin, ha dimostrato che occorrono almeno 10 ore di calcolo per trovare collisioni.
- RIPE-MD sono stati sviluppati dal progetto European RIPE, i cui autori hanno scoperto collisioni per una sua versione, in due casi. L'algoritmo originale è stato successivamente migliorato nel RIPE-MD/160, che utilizza output di 160, 256 o 320 bit.
- SHA-1 acronimo di Secure Hash Algorithm-1, sviluppato dal NSA su richiesta del National Institute of Standard and Technology (NIST), è simile all'algoritmo MD4. L'originale progetto del 1994 aveva il nome di SHA, poi modificato nel codice dal NSA. Produce output di 160 bit. Attualmente è uno dei più sicuri, usato anche dai programmi PGP e GPG per firmare un documento.
- SHA-2, Secure Hash Algorithm-2, versione successiva a SHA-1, genera impronte di documenti da 256, 384 e 512 bit.
- SNEFRU funzione di hash sviluppata da Ralph Merkle. La versione denominata 2-round, è stata violata da Eli Biham. Attualmente esiste SNEFRU 4-round. Produce output di 128 o 256 bit.
- TIGER è un nuovo algoritmo sviluppato da Ross Anderson ed Eli Biham. A differenza di MD4, non usa istruzioni di rotazione per generare il valore di hash. Consente l'output di 128, 160 e 192 bit.

Comunicazione sicura Back

- Secure Socket Layer (SSL), Secure Shell (SSH) e Transport Layer Security (TLS), protocolli per la comunicazione client/server attraverso un canale criptato.
- HTTP over Secure (HTTPS) e Secure FTP (SFTP), protocolli per il trasferimento di documenti ipertestuali attraverso un canale cifrato. Sono basati su SSL e sui certificati digitali.
- Virtual Private Networks (VPN) gruppo di macchine collegate in rete tramite un protocollo cifrato denominato IPSec. Ogni macchina dispone delle chiavi pubblica e privata necessarie per cifrare/decifrare i dati in transito e per identificarsi.
- S/MIME, PGP/MIME (adesso chiamato OpenPGP), standard di comunicazione criptata per la posta elettronica.

Crittografia a chiave asimmetrica (o pubblica) Back

Diffie ed Hellman pensarono ad un sistema asimmetrico, chiamato **algoritmo Diffie-Hellman**, basato su l'uso di due chiavi generate in modo che sia impossibile ricavarne una dall'altra. Le due chiavi vengono chiamate pubblica e privata: la prima serve per cifrare e la seconda per decifrare. Una persona che deve comunicare con un'altra persona non deve far altro che cifrare il messaggio con la chiave pubblica del destinatario, il quale a sua volta, ricevuto il messaggio non dovrà fare altro che decifrarlo con la chiave segreta personale. Ogni persona con questo sistema possiede quindi una coppia di chiavi: quella pubblica può essere tranquillamente distribuita e resa di pubblico dominio perché consente solo di cifrare il messaggio, mentre quella privata deve essere conosciuta solo da una persona. In questo modo lo scambio di chiavi è assolutamente sicuro. Fino a questo punto sembrava andare tutto bene, ma bisognava trovare il modo di implementare matematicamente questo sistema, riuscire cioè a creare due chiavi per cui non fosse possibile dedurre quella privata conoscendo quella pubblica.



RSA Back

Il primo modello di chiave pubblica e privata, fu sviluppato nel 1978 da tre professori: Ronald Rivest, Adi Shamir e Leonard Adleman, che realizzarono una procedura di calcoli matematici che prenderà il nome di “algoritmo RSA”, dalle iniziali dei suoi inventori. I tre ricercatori del MIT si basarono sul modello di Diffie-Hellman includendo anche la crittazione dei dati, a differenza del primo.

Quando ci si rese conto dell'efficacia di questo algoritmo, ritenuto ancora oggi inattaccabile, il governo americano decise che i programmi basati su questo algoritmo potevano essere utilizzati liberamente negli Stati Uniti, ma la loro esportazione costituiva reato. Un altro ostacolo all'immediato sviluppo di questo algoritmo era dovuto al fatto che i tre inventori del sistema RSA decisero, nel 1982, di brevettare il loro algoritmo e fondare la RSA Data Security Inc., una compagnia nata per lo sfruttamento commerciale del loro sistema di crittografia.

Nonostante le restrizioni statunitensi all'utilizzo dell'RSA, al di fuori degli USA, dove il governo americano non ha potere e gli algoritmi non sono coperti da brevetto, iniziano a diffondersi

numerosi programmi ispirati molto da vicino alla tecnica di Rivest, Shamir e Adleman.
Comunque nel 2000 l'agoritmo RSA diviene pubblico.

Chiavi miste Back

L'introduzione dei metodi a chiave pubblica come RSA hanno risolto brillantemente il grosso problema dello scambio della chiave. La crittografia a doppia chiave è stata una brillante intuizione ma le funzioni matematiche che generano il codice cifrato e quelle inverse per decifrarlo, fanno si che questo tipo di crittografia sia uno dei più lenti in assoluto: si dice che sia da 100 a 1000 volte più lento dei sistemi a chiave segreta.
Per questo sono nati sistemi di crittografia misti, che combinano le due tecniche in modo da fonderne i vantaggi. In pratica, si utilizza la chiave pubblica soltanto per comunicare la chiave segreta (che in questi casi viene chiamata chiave di sessione) che poi verrà usata per una normale comunicazione basata su cifrati a chiave segreta. In questo modo quindi è ampiamente risolto il problema della sicurezza nello scambio della chiave e la velocità di cifratura/decifratura rimane molto alta e non penalizza la comunicazione.
In pratica avviene questo: se A e B devono comunicare in modo sicuro e veloce,
A utilizza la chiave pubblica di B per inviare la chiave di sessione, B decifra la chiave di sessione con la propria chiave segreta, A e B possono comunicare utilizzando la chiave di sessione.

Funzioni di HASH Back

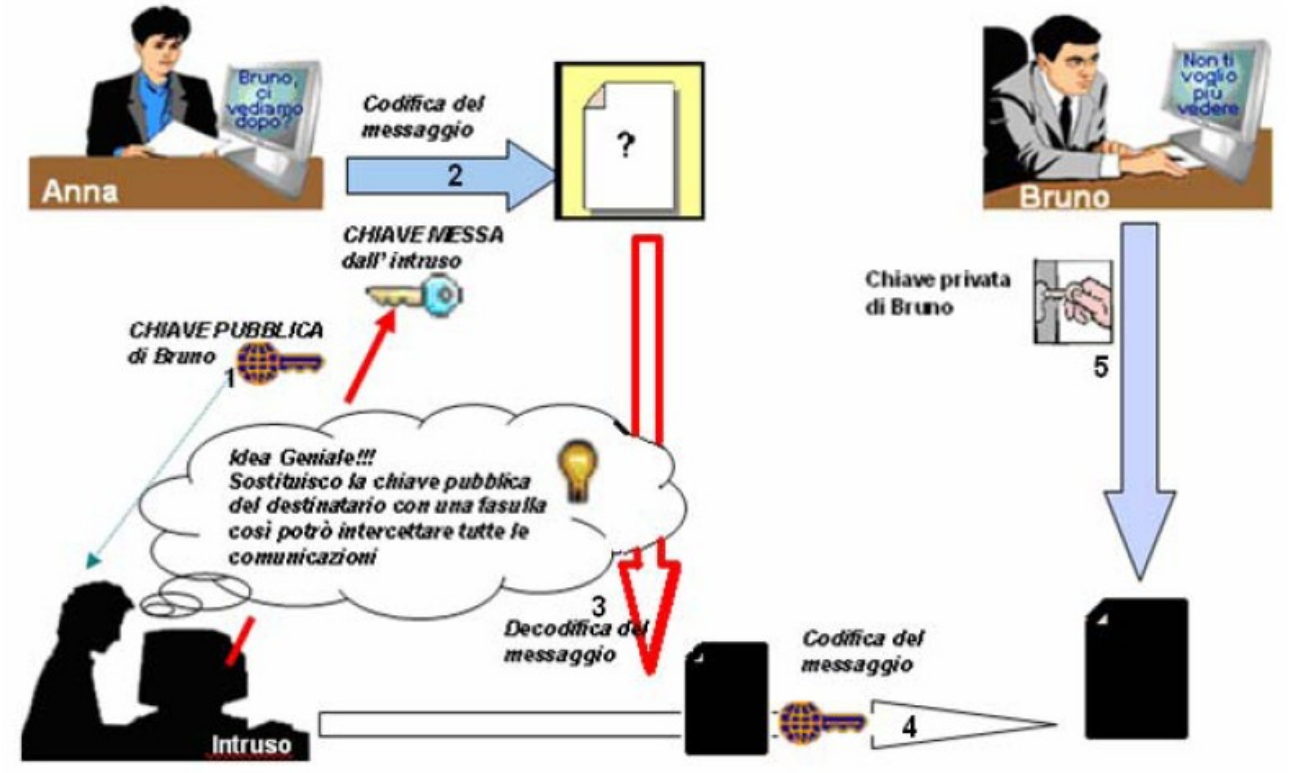
Una funzione di hash, detta anche one way hash, trasforma un testo normale di lunghezza arbitraria in una stringa di lunghezza relativamente limitata (in genere 128 o 160 bit). Questa stringa rappresenta una sintesi del messaggio (message digest) è consiste in una vera e propria impronta digitale unica che viene definita valore di hash (oppure checksum) e che gode di tre importanti proprietà:

- dato un messaggio si può facilmente calcolare il suo valore di hash
- dato il valore di hash è impossibile risalire al messaggio (per questo one way hash)
- non si possono generare due messaggi che abbiano la stessa sintesi

Quest'ultima proprietà non è impossibile ma in genere si intende che la probabilità di collisione (due messaggi con la stessa sintesi) deve essere molto bassa. Solitamente per le impronte vengono utilizzati 128 bit, ma il valore può essere qualsiasi, tenendo conto che più basso è e più alta è la probabilità di collisione. PGP e GPG utilizzano la crittografia unita all'algoritmo di Hash SHA-1 per firmare il documento.

Si può manomettere una chiave pubblica? Back

Purtroppo si.
Vediamo in pratica cosa può accadere:



Un intruso sostituisce la chiave pubblica di Bruno con la sua.
Anna cifra il messaggio utilizzando la chiave pubblica di Bruno (in realtà è la chiave dell'intruso).
L'intruso è in grado, quindi, di decifrare il messaggio. Prepara quindi un nuovo messaggio (messaggio alterato) da inviare.
L'intruso invia il nuovo messaggio a Bruno, cifrandolo utilizzando la "vera" chiave pubblica di Bruno.
Bruno decodifica il messaggio utilizzando la sua chiave privata.
Né Bruno né Anna scopriranno mai niente di quanto è successo.
Per risolvere questo problema è necessario trovare un modo per LEGARE una chiave pubblica al suo proprietario. Ovvero con il CERTIFICATO DIGITALE

Certificati digitali: chiave PGP/GPG e X.509 Back

Il certificato digitale, è un po' come avere la patente, il codice fiscale. Non ce ne possono essere uguali, altrimenti è un documento falso. Esso include:

- una chiave pubblica
- informazioni sull'identità del proprietario
- una o più firme digitali

Una chiave pubblica può essere firmata così come un documento cartaceo. Firmando un certificato si attesta che la veridicità è confermata dai firmatari della chiave.
Il certificato contiene la chiave pubblica, più un'etichetta con una o più prove che la corrispondenza è esatta. In un gruppo di amici, o in una sede aziendale, non è difficile scambiarsi la chiave pubblica fra gli utenti, basta per esempio un floppy disk. Se il discorso è esteso ad un vasto gruppo di utenti, quindi esterni al gruppo di amici o esterni ai dipendenti di una certa azienda, lo scambio può avvenire tramite un server di certificati, o altrimenti detti Public Key Infrastructure. Questi server, o meglio, questi keyserver permettono di depositare e prelevare i certificati di chiave pubblica.
Queste strutture sono nate perché i software crittografici (PGP, GnuPG) ovviamente non sanno se il

nome, l'e-mail che si stanno inserendo appartengono effettivamente a chi inserisce i dati.
Un intruso potrebbe effettuare un attacco di tipo Man-in-the-middle e generare dati falsi per l'occasione. Se invece esiste un'entità di cui si ha totale fiducia, e questa stessa entità ha firmato la chiave pubblica del nostro interlocutore, allora ci si potrà fidare di quella chiave pubblica.
Un certificato digitale può avere diversi formati. I più diffusi sono:

- chiavi PGP/GPG
- certificati X.509

Una chiave PGP/GPG include:

- versione di PGP/GPG numero che identifica la versione del software per creare la chiave associata al certificato.
- chiave pubblica
- informazioni sul proprietario quali ad esempio il nome, indirizzo di posta elettronica, la fotografia, ecc.
- firma digitale o certificato del proprietario cioè una firma elettronica creata utilizzando la chiave privata che corrisponde alla chiave pubblica associata al certificato.
- validità del certificato data-ora di creazione della coppia di chiavi.
- algoritmo simmetrico è l'algoritmo utilizzato per creare la chiave, a preferenza di chi crea il certificato. Gli algoritmi sono: AES, CAST5, IDEA, Triple-DES, Twofish.

Un certificato X.509 contiene:

- versione X.509 indica quale versione dello standard X.509 è stata applicata al certificato.
- Numero di serie l'entità che ha creato il certificato, deve assegnare un ID unico all'emissione.
- Algoritmo della firma elettronica ad esempio MD5.
- Rilasciato da (oppure Emittente), l'autorità che ha rilasciato il certificato.
- Valido dal data di inizio validità del certificato.
- Valido fino al data di scadenza.
- Soggetto il corrispondente proprietario del certificato.
- Chiave pubblica
- Algoritmo identificazione personale ad esempio SHA-1.

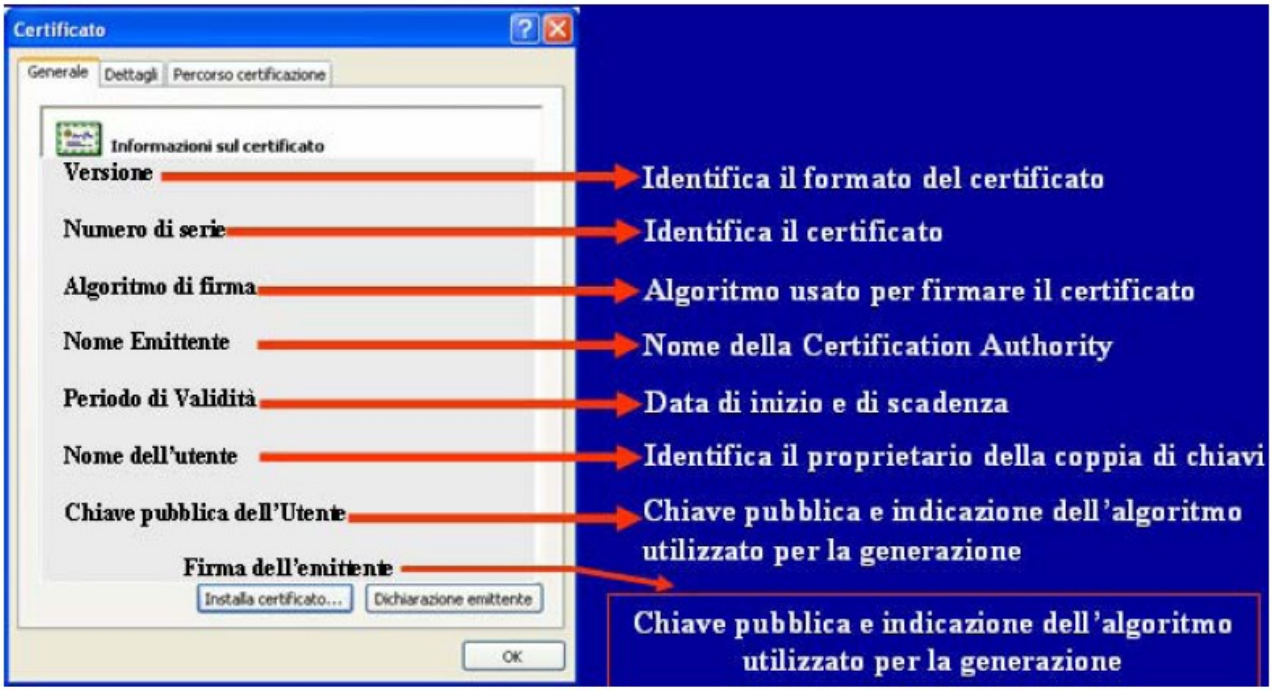
E poi altre informazioni.
Quali sono le differenze fra un certificato PGP/GPG ed uno di tipo X.509? Sono queste:

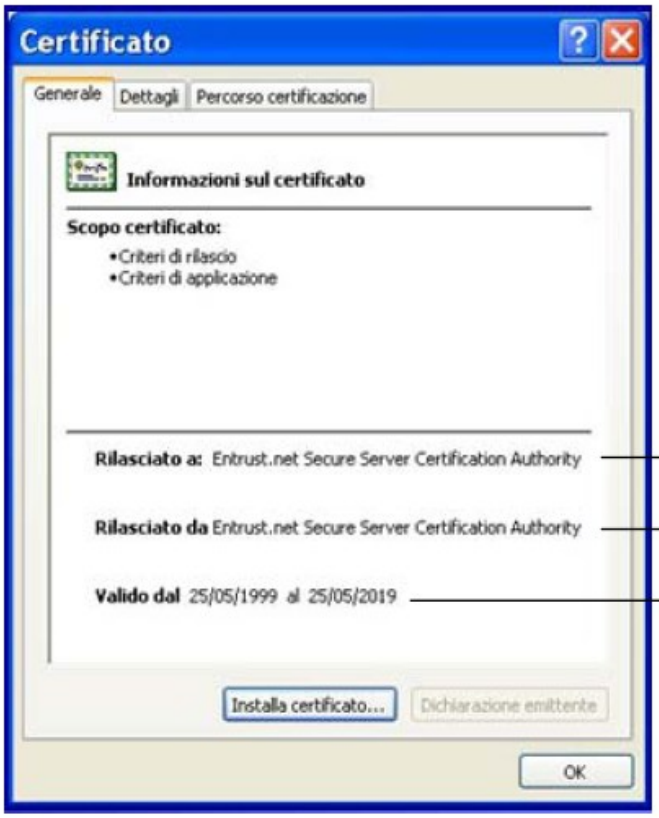
- è possibile creare il proprio certificato PGP/GPG in modo autonomo ed in pochissimi istanti, mentre per X.509 è necessario rivolgersi ad un ente addetto allo scopo.
- il certificato X.509 consente di avere un singolo nome per il proprietario della chiave.
- il certificato X.509 possiede solo un id numerico per far fede alla validità della chiave.

Nei certificati digitali di tipo X.509 rivestono un ruolo importante:

- Certification Authority (CA), Autorità di Certificazione
- Registration Authority (RA), Autorità di Registrazione

La CA crea i certificati e li firma elettronicamente utilizzando la propria chiave privata. Controllando la chiave pubblica della CA, chiunque può verificare sia l'autenticità che l'integrità del certificato attraverso la firma digitale della CA.
Una CA può delegare anche ad altri il compito di validare i certificati, da qui nasce il modello di fiducia gerarchico. In questo caso la CA alla base è detta CA root.
La CA inoltre, crea o gestisce il software che viene utilizzato per emettere i certificati dei suoi utenti (che possono essere privati, aziende, enti governativi). Esistono autorità di certificazione che sono protetti a livello amministrativo e persino militare.
La RA controlla i processi e gli strumenti utilizzati dalla CA.



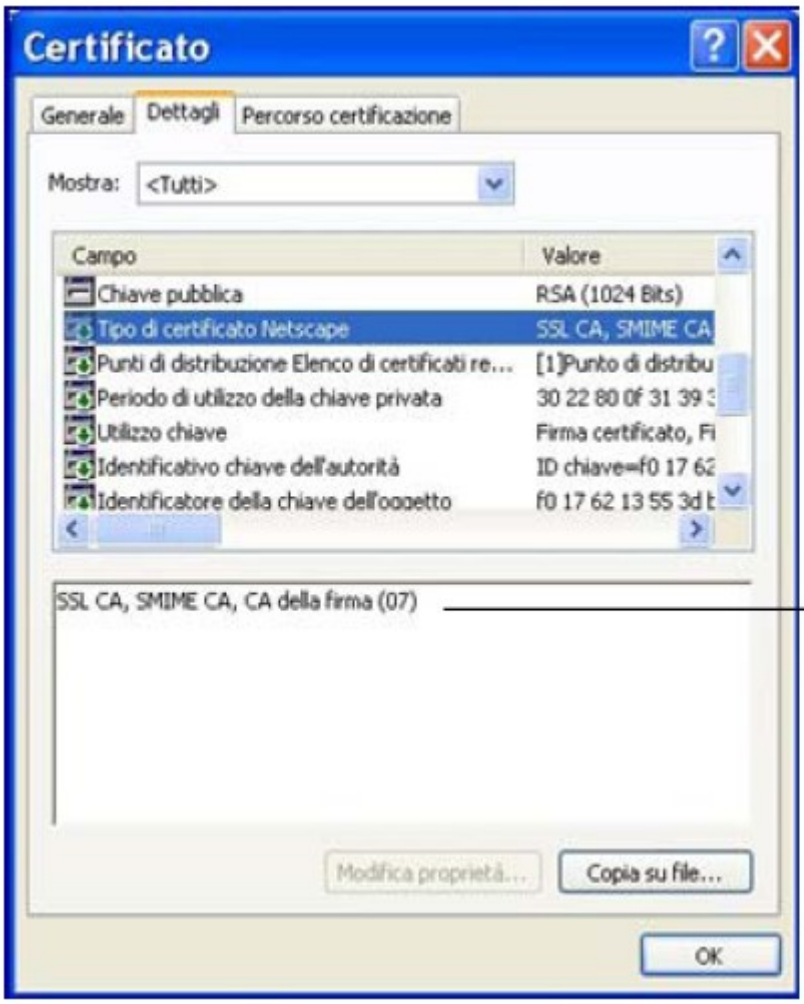


Di chi è il certificato

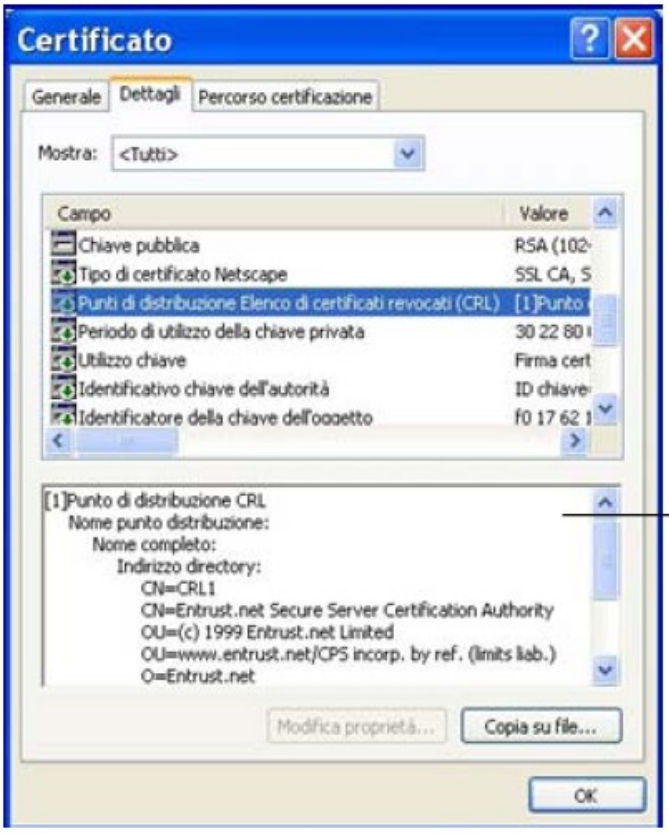
CA che ha rilasciato il certificato

Periodo di validità del certificato.
Per motivi di sicurezza la validità di un certificato non può essere superiore a 3 anni.

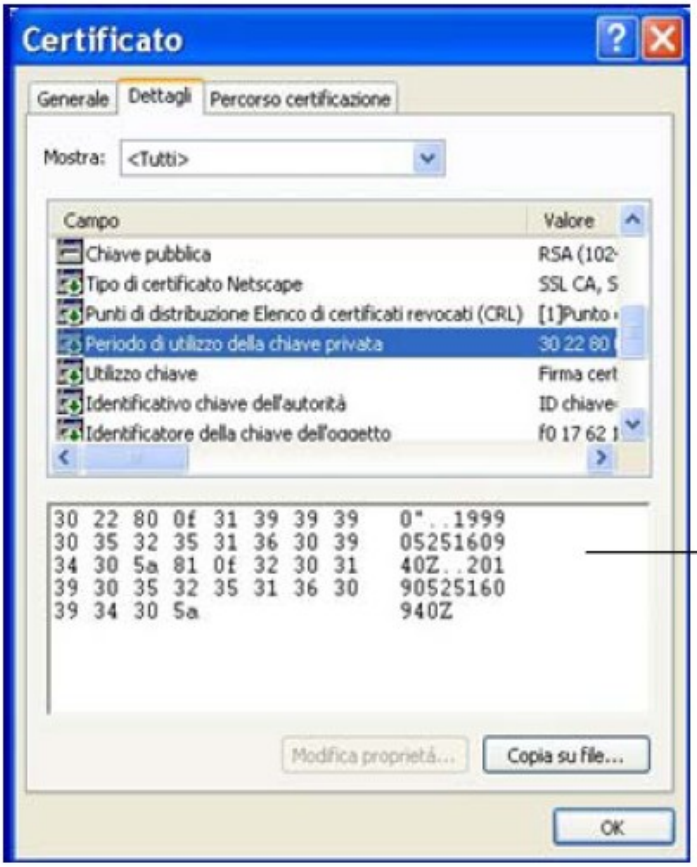
Chiave pubblica



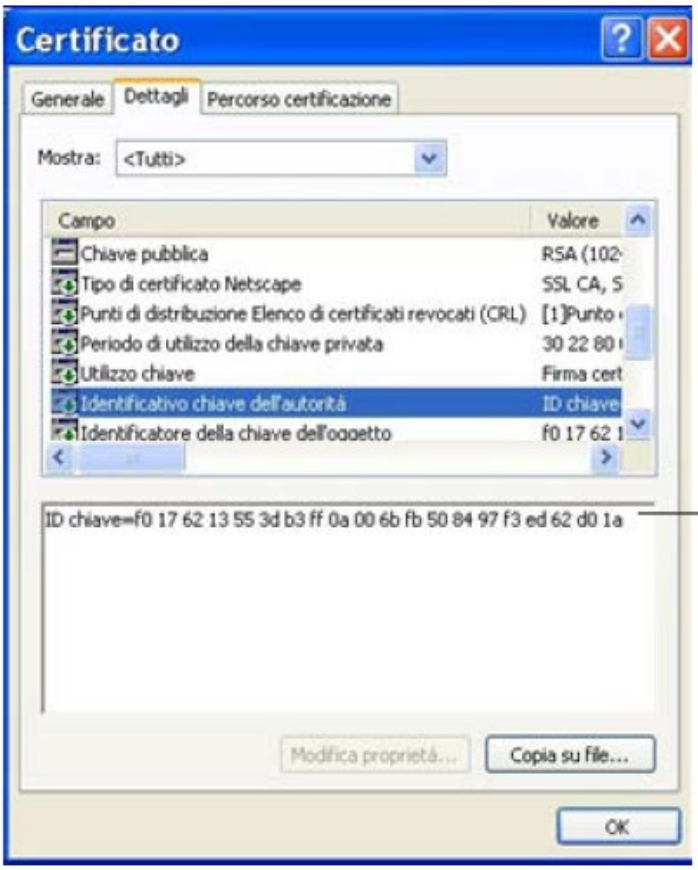
Tipo di certificato



Punti di distribuzione Elenco dei certificati revocati (CRL)



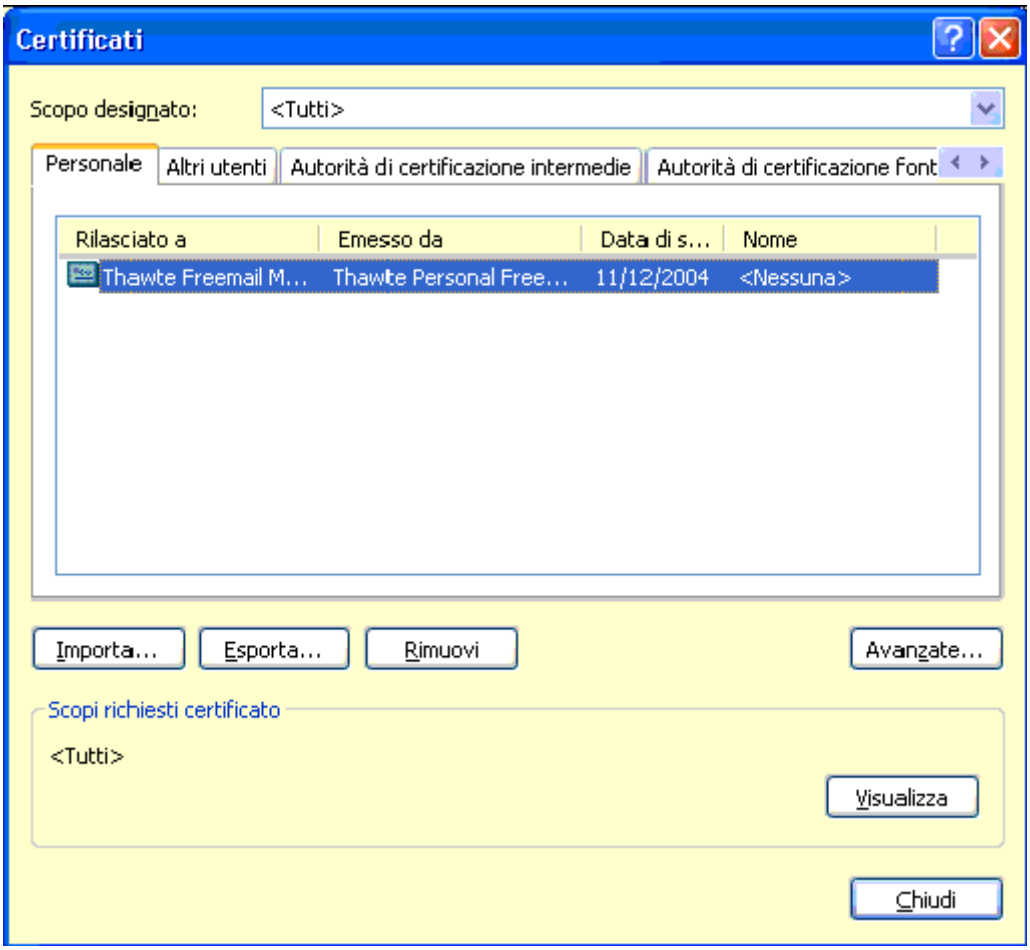
Periodo di utilizzo della chiave privata



Identificativo della chiave della CA

Esempio Back

L'utente A firma digitalmente un documento, calcolando l'impronta mediante un procedimento matematico (funzione di Hash). Cripta quest'impronta con la propria chiave privata ed allega questa firma al documento. L'utente B, il destinatario del documento firmato, per verificare la firma del suo corrisponde effettivo, innanzitutto deve possedere la chiave pubblica della CA così da verificare la firma digitale dell'autorità del certificato dell'utente A.
Poi applica il procedimento matematico per calcolare l'impronta, decriptando quest'impronta con la chiave pubblica del mittente, e se la risultante sequenza di bit è uguale all'impronta ottenuta dalla firma di A, allora il documento è stato realmente mandato da quel mittente e non è stato modificato da nessuno. Per concludere, per essere certi di comunicare effettivamente con una certa persona (azienda, ente), c'è bisogno di un'autorità al di sopra delle parti che garantisca l'identità del proprio interlocutore, nel caso di certificato X.509.
Fra queste autorità, faccio presente la Thawte (http://thawte.ascia.net oppure http://www.thawteitalia.com), VeriSign (http://www.verisign.com) e il progetto EuroPKI Italian Certification Authority (http://www.europki.org/ca/it/it_index.html). La prima e la terza autorità rilasciano i certificati digitali in modo del tutto gratuito (naturalmente dopo aver verificato i dati personali).
Per vedere i certificati memorizzati sul proprio computer (con sistema operativo Windows), cliccare su Pannello di controllo>Opzioni internet>clic sul tab Contenuto>clic sul pulsante Certificati.
Apparirà una lista con i certificati memorizzati sul computer. La finestra è simile alla seguente:



I tab che ci interessano di più sono: “Personale” e “Altri utenti”. Il primo tab, come indica il nome, contiene i propri certificati digitali personali, mentre il secondo contiene quelli dei propri corrispondenti. Tenere presente che ad ogni certificato digitale può corrispondere un solo indirizzo e-mail. Analizziamo ora alcuni passi da compiere per mettere al sicuro i certificati, perché se si perdono bisognerà richiederli nuovamente.

Firma digitale / Firma elettronica forte o pesante Back

(principio giuridico) è quella che il legislatore definisce firma digitale. Essa è basata su un sistema a chiavi crittografiche asimmetriche, utilizza un certificato digitale con particolari caratteristiche, rilasciato da un soggetto con specifiche capacità professionali garantite dallo Stato e viene creata mediante un dispositivo con elevate caratteristiche di sicurezza che in genere è una smart card. La firma digitale può ritenersi equivalenti a quella autografa. Quando si ha la necessità di una sottoscrizione equivalente a quella autografa è indispensabile utilizzare la firma digitale. La firma digitale è utile nel momento in cui è necessario sottoscrivere una dichiarazione ottenendo la garanzia di integrità dei dati oggetto della sottoscrizione e di autenticità delle informazioni relative al sottoscrittore.
Quindi, alla sottoscrizione con firma digitale "forte" (quella che possiede le seguenti caratteristiche:
1- è una firma elettronica avanzata,
2- è basata su un certificato qualificato,
3- è generata per mezzo di un dispositivo sicuro per la generazione delle firme)
viene data la medesima validità giuridica di una firma autografa autenticata da un pubblico ufficiale.

Firma elettronica debole o leggera Back

è tutto ciò che non risponde anche in minima parte a quanto appena descritto, ma è compatibile con la definizione giuridica di firma elettronica. Quando non si ha la necessità di una sottoscrizione equivalente a quella autografa è sufficiente utilizzare la firma digitale debole o leggera.

Firma elettronica (generica) Back

può essere realizzata con qualsiasi strumento (password, PIN, digitalizzazione della firma autografa, tecniche biometriche, ecc.) in grado di conferire un certo livello di autenticazione a dati elettronici.

Firma elettronica avanzata Back

più sofisticata, consente di identificare in modo univoco il firmatario garantendo anche l'evidenza di modifiche all'oggetto firmato, apportate dopo la sottoscrizione.

I Certificatori Back

garantiscono la veridicità e la correttezza delle informazioni riportate nel certificato (dati anagrafici del titolare). I certificatori che intendono rilasciare certificati digitali validi per le sottoscrizioni di istanze e dichiarazioni inviate per via telematica alla pubblica amministrazione stessa, possono dimostrare di possedere particolari e comunque superiori caratteristiche di qualità e sicurezza e ottenere quindi la qualifica di "certificatore accreditato". Tale qualifica è sotto il controllo ed è garantita, in Italia, dallo Stato.

Non ripudio Back

La firma digitale ha caratteristiche tali da non consentire al sottoscrittore di disconoscere la propria firma digitale (fatta salva la possibilità di querela di falso). Infatti Il documento informatico, quando è sottoscritto con firma digitale o con un altro tipo di firma elettronica avanzata, e la firma è basata su di un certificato qualificato ed è generata mediante un dispositivo per la creazione di una firma sicura, fa inoltre piena prova, fino a querela di falso, della provenienza delle dichiarazioni da chi l'ha sottoscritto.

Kit di firma digitale ed i costi Back

Per poter generare firme digitali è necessario essere dotati di un dispositivo sicuro per la generazione delle firme (costituito da una smartcard o da un token USB), un lettore di smartcard (nel caso in cui non si utilizzi il token USB), un software in grado di interagire con il dispositivo per la generazione di firme digitali e per la gestione del dispositivo stesso (es. per il cambio del PIN che

ne consente l'uso).
I costi del kit completo è variabile da certificatore a certificatore; a titolo orientativo è comunque possibile ottenere il kit completo ad un prezzo di circa 100,00 €. Il certificato ha una scadenza, e deve essere quindi rinnovato periodicamente. In genere hanno una validità di uno o due anni, il rinnovo ha un costo orientativo di 10,00/15,00 € per anno.

Dove e come dotarsi di firma digitale forte Back

L'elenco pubblico dei certificatori è disponibile via Internet per la consultazione (1), dove sono anche disponibili i link ai siti web degli stessi sui quali sono indicate le modalità operative da seguire.

Dove e come dotarsi di firma digitale (debole) gratis Back

Prima di avventurarsi a contattare un certificatore accreditato per il rilascio di una firma digitale forte, prendere un appuntamento, pagare circa 100,00 Euro, e poi magari scoprire che nel frattempo le "norme" si sono accorte che la firma digitale forte non è poi così forte, ci si può dotare gratuitamente di una firma digitale cosiddetta debole e iniziare a firmare e crittografare e-mail e documenti.
Quello che segue è l'indirizzo internet di una società di Terni che mette a disposizione gratuitamente i propri certificati S/MIME (certificati per la posta elettronica certificata) per uso personale! https://www.globaltrust.it/products_buy/gcorpsecmail_24.aspx
Quello che segue invece è l'indirizzo della branca italiana di Thawte, recentemente acquisitaaa dalla più grande e potente VeriSign, leader del settore, la quale rilascia certificati digitali in maniera del tutto gratuita. http://thawte.ascia.net/guideweb/registrazione/frameset.php

Procedura di firma digitale Back

Dopo aver reso disponibile il dispositivo, inserendo quindi la smartcard nell'apposito lettore o aver inserito il Token USB nella porta specifica, l'applicazione di firma provvederà a richiedere l'inserimento del PIN di protezione, visualizzerà e richiederà di scegliere quale certificato si intende usare e procederà infine alla generazione della firma. In base alla legislazione vigente sull'interoperabilità della firma digitale il file sottoscritto conserva il suo nome originale, al quale viene aggiunta l'estensione ".p7m". Ne risulta che il file pippo.pdf, dopo la sottoscrizione, diverrà pippo.pdf.p7m e come tale sarà fruito da altre applicazioni.

Procedura di verifica Back

La procedura di verifica della firma digitale apposta ad un documento informatico consiste sostanzialmente nel verificare che:
1. il documento non sia stato modificato dopo la firma;
2. il certificato del sottoscrittore sia garantito da una Autorità di Certificazione (CA) inclusa nell'Elenco Pubblico dei Certificatori;
3. il certificato del sottoscrittore non sia scaduto;
4. il certificato del sottoscrittore non sia stato sospeso o revocato.

Per eseguire queste verifiche, oltre che per rendere leggibile il contenuto del documento, sono utilizzati specifici software. Detti software sono forniti dai certificatori ai titolari dei certificati; coloro che non sono dotati di un kit di firma digitale possono altresì utilizzare dei software disponibili per uso personale a titolo gratuito.

NORME DI RIFERIMENTO Back

Art. 15, comma 2, della legge 15/3/1997, n. 59;
DPR 10 novembre 1997, n. 513;
DPCM 8 febbraio 1999;
Direttiva europea 1999/93/CE sulle firme elettroniche:
Circolare AIPA CR/24 del 19 giugno 2000;
Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445:
Circolare n. 3529/C del 30-10-2001 del Ministero delle Attività Produttive;
Circolare n. 3532/C del 15-11-2001 del Ministero delle Attività Produttive;
Circolare n. 3553/C del 29/11/2002 del Ministero delle Attività Produttive;
Decreto legislativo 23 gennaio 2002, n. 10;
Decreto del Presidente della Repubblica 7 aprile 2003, n. 137;
Decreto del Presidente del Consiglio dei Ministri 13 gennaio 2004;
DPCM 13 gennaio 2004;
D.Lgs. 15 marzo 2006

Fonti e Bibliografia Back

http://www.cli.di.unipi.it/~guidi/echelon/tesi.html
http://www.cnipa.gov.it
http://www.gxware.org/
http://www.interlex.it/attualit/amonti49.htm
http://www.repubblica.it/online/tecnologie/echelon/echelon2/echelon2.html
http://news.bbc.co.uk/1/hi/world/europe/1357264.stm

Per approfondire (links) Back

http://www.card.infocamere.it/
http://www.interlex.it/docdigit/indice.htm
http://www.interlex.it/docdigit/intro/intro1.htm
http://www.mininnovazione.it/ita/egovernment/infrastrutture/firma_digitale.shtml
http://www.mininnovazione.it/ita/normativa/normativa_firmadigitale.shtml
http://www.poste.it/online/postecert/cosef.shtml
http://www.cnipa.gov.it/site/it-IT/Aree_operative/Regolazione_e_Formazione/Firma_digitale/
http://www.cnipa.gov.it/site/it-IT/In_primo_piano/Posta_Elettronica_Certificata__(PEC)/
http://www.governo.it/governoinforma/dossier/firma_digitale/index.html
https://firmadigitale.trustitalia.it/
http://it.wikipedia.org/wiki/Firma_digitale
http://it.wikipedia.org/wiki/Certificato_digitale
http://punto-informatico.it/p.asp?i=57917
http://opensignature.sourceforge.net/
http://www.macworld.it/showPage.php?template=notizie&id=5849
http://www.ictlex.net/?p=296
http://www.urp.it/Sezione.jsp?idSezione=807&idSezioneRif=39
http://www.re-set.it/documenti/1000/1800/1810/1817/15giugno_firmadigitale.htm
http://thawte.ascia.net/guideweb/richiesta/index.php
http://www.trustitalia.it/decode.php?id=2kcU8E002914
http://www.gnomixland.com/mod-subjects-viewpage-pageid-428.html
http://www.kpromos.com/sicurezza-informatica/40/sha1-violato.html
http://www.osservatoriofinanziario.it/of/newslarge.asp?id=6
http://www.globaltrust.it/seclaw/italia/postaCert/index.aspx
http://thawte.ascia.net/index.php
http://www.interlex.it/docdigit/dallariva1.htm

FINE