

FIRME DIGITALI: COSA SONO E A COSA SERVONO

Giancarlo
Mauri
e
Alberto
Leporati

La diffusione degli strumenti informatici e la parallela crescita della comunicazione attraverso le reti di calcolatori hanno posto con pressante urgenza il problema della sostituzione del tradizionale documento cartaceo con un equivalente strumento informatico. Il meccanismo universalmente adottato per costruire tale strumento è la cosiddetta firma digitale, basata sulla crittografia a chiave pubblica.

La firma digitale si è ormai affermata come principale strumento in grado, allo stato attuale della tecnologia, di assicurare l'integrità e la provenienza dei documenti informatici, e quindi di svolgere per questi la funzione che nei documenti tradizionali è assolta dalla firma autografa.

La principale differenza tra firma autografa e firma digitale sta nel fatto che la prima è direttamente riconducibile all'identità di colui che la appone, poiché la calligrafia è un elemento identificativo della persona, mentre la seconda non possiede questa proprietà. Per coprire questa deficienza si ricorre all'autorità di certificazione, il cui compito è quello di stabilire, garantire e pubblicare l'associazione tra firma digitale e soggetto sottoscrittore.

Per contro, mentre l'associazione tra testo di un documento e firma autografa è ottenuta esclusivamente attraverso il supporto cartaceo, tanto che i due oggetti possono essere fisicamente separati, la firma digitale è intrinsecamente legata al testo a cui è apposta, tanto che a testi diversi corrispondono firme diverse; quindi, nonostante la sua perfetta replicabilità, è impossibile trasferire la firma digitale da un documento ad un altro.

Solitamente, il crittosistema a chiave pubblica utilizzato per cifrare e decifrare i messaggi e per implementare le firme digitali è il ben noto RSA. Tuttavia, non è l'unico ad essere utilizzato; ad esempio, il Digital Signature Algorithm (DSA) è una specifica di un processo che crea firme a partire dal contenuto del messaggio. Il vantaggio di DSA rispetto ad

RSA è che DSA utilizza tecnologia liberamente esportabile al di fuori degli Stati Uniti mentre RSA contiene codice brevettato, ed è inoltre assoggettato alle regole di esportazione per la cosiddetta "crittografia forte". Lo svantaggio di DSA rispetto ad RSA è che DSA può essere utilizzato unicamente per produrre firme digitali, mentre RSA è un crittosistema a chiave pubblica completo, utilizzabile per cifrare e decifrare qualunque messaggio. Ulteriori informazioni sul DSA possono essere trovate alla pagina Web:<http://Mw.nist.gov/>

Le applicazioni pratiche delle firme digitali sono le seguenti:

- autenticazione di utenti remoti per l'accesso ad informazioni riservate;
- sistemi di pagamento elettronico basati su carte di credito o carte di debito;
- sistemi di commercio elettronico;
- sistemi di sicurezza in applicazioni di rete.

Standard per le firme digitali

Sotto la spinta delle applicazioni commerciali, ed in particolare di quelle bancarie, sono stati sviluppati numerosi standard, tanto de iure che de facto, relativi all'uso delle tecniche crittografiche, che possono trovare applicazione per la sottoscrizione digitale.

Nell'ambito della standardizzazione ufficiale, un ruolo determinante è ovviamente giocato dall'International Standard Organization (ISO), che costituisce l'ente normatore primario a livello internazionale. Tale organismo ha emanato numerose norme in campo crittografico, destinate principalmente al settore bancario ed a quello della tecnologia dell'informazione. Si tenga presente che, per la normazione in campo informatico, l'ISO opera in congiunzione con l'International Electrical Commission (IEC), con la quale ha costituito un apposito comitato tecnico congiunto, il Joint Technical Committee n. 1 (JTC1).

Accanto all'ISO, ed in modo coordinato con esso, opera l'International Telecommunication Union (ITU), che ha sostituito lo storico CCITT ed emette "raccomandazioni" che hanno valore di norme primarie nei settori delle telecomunicazioni (ITU-T) e della radiodiffusione (ITU-R). Da esso provengono le raccomandazioni X.400 ed X.500 che hanno un'importanza fondamentale per i sistemi di messaggistica elettronica. In particolare alla famiglia X.500 appartiene la raccomandazione X.509 verso cui stanno convergendo tutti i sistemi di autenticazione e firma digitale quale standard per i certificati. Il coordinamento tra ITU ed ISO è, almeno per le questioni che hanno riflessi sulla firma digitale, molto stretto. Infatti l'intera famiglia X.500 è emanata in modo congiunto, ossia a ciascuna "raccomandazione" ITU-T corrisponde uno "standard internazionale" ISO tali che il testo di entrambi è esattamente lo stesso.

Non si può poi ignorare il ruolo delle maggiori organizzazioni di standardizzazione americane, in particolare il National Institute of Standards and Technology (NIST), che ha definito il Digital Signature Standard (DSS), e lo American National Standards Institute (ANSI), che ha emesso numerose norme per il settore finanziario tra cui vale la pena ricordare la X9.30.1, che definisce il Digital Signature Algorithm (DSA), e la X9.30.2, che specifica il Secure Hash Algorithm (SHA-1) recepito anche dall'ISO nella norma ISO/IEC CD 10118-3 [JTC196] (si rimanda alla pagina Web <http://www.ansi.org/> per maggiori informazioni sull'ANSI e sugli standard FIPS).

Deve essere infine menzionato lo Institute of Electrical and Electronics Engineers (IEEE), al quale si deve tra l'altro la standardizzazione di Ethernet, che sta compiendo un notevole sforzo per sviluppare uno standard unico ed integrato comprendente tutti gli algoritmi asimmetrici attualmente disponibili, da quelli basati sulla fattorizzazione degli interi, a quelli che sfruttano il problema del logaritmo discreto, a quelli che usano le proprietà delle curve ellittiche. Tale progetto di standard viene indicato con la sigla P1363.

Parallelamente agli standard ufficiali, e per alcuni versi in anticipo rispetto a questi, sono stati sviluppati e si sono affermati alcuni standard di fatto che non possono essere trascurati, soprattutto perchè possono vantare un numero di implementazioni ed una quantità di utenti superiore a quella degli stan-

dard de iure. In tale ambito deve essere ricordato in primo luogo Pretty Good Privacy (PGP), cui deve essere riconosciuto il merito di aver diffuso la crittografia a chiavi pubbliche, sia pure più con lo scopo di proteggere la riservatezza della comunicazione che per l'autenticazione dei documenti.

Per la diffusione nei prodotti commerciali deve essere infine considerato il Public Key Crypto System (PKCS), un insieme di specifiche tecniche pubblicate dalla RSA Inc. con lo scopo di fornire uno strumento atto a garantire l'interoperabilità dei prodotti utilizzando il cifrario di Rivest, Shamir e Adleman.

In definitiva gli standard attinenti la firma digitale maggiormente rilevanti a livello europeo possono essere inquadrati in quattro filoni principali:

1. standard bancari;
2. norme ISO per la tecnologia dell'informazione;
3. PGP;
4. PKCS.

Gli standard utilizzati nel settore bancario rivestono particolare importanza poichè sono quelli maggiormente consolidati e collaudati; d'altra parte essi si presentano in realtà come una molteplicità di norme eterogenee e sostanzialmente incompatibili tra loro, sviluppate sotto la spinta di specifiche applicazioni, quali il trasferimento di ordinativi, l'effettuazione di transazioni con carta di credito e cosæ via. L'integrazione dei servizi e dei vari circuiti bancari ha comunque portato allo sviluppo di strumenti di interoperabilità e alla progressiva convergenza verso le norme di maggiore generalità.

L'eterogeneità presente nel settore si manifesta in modo eclatante nella sostanziale incompatibilità tra norme emanate dalla stessa organizzazione, come accade nel caso degli standard internazionali emanati dall'ISO per il settore bancario da un lato e per quello della tecnologia dell'informazione dall'altro. Questi ultimi, pi` recenti, costituiscono la base su cui costruire sistemi interoperabili e durevoli nel tempo. Un fatto che conforta questa prospettiva è la progressiva convergenza, nel settore più maturo della tecnologia, quello dei certificati, verso lo X.509 come standard di base unico, eventualmente esteso in modo diverso secondo le particolari necessità, ma comunque universalmente supportato nelle caratteristiche essenziali.

In effetti fino ad oggi le tecniche crittografiche, anche a chiavi pubbliche, sono state utilizzate

essenzialmente per assicurare la riservatezza della comunicazione e quindi la compatibilità e l'interoperabilità erano considerate caratteristiche di secondaria importanza, se non addirittura potenzialmente pericolose. Il ribaltamento della prospettiva introdotto dalla firma digitale, che deve garantire l'autenticità di un documento di fronte a chiunque e non solo per il diretto destinatario, porterà, come è successo nei protocolli di comunicazione, ad una rapida convergenza verso gli standard maggiormente efficaci.

Criteri generali di sicurezza per le smart card

L'uso sempre più frequente delle smartcard per la fruizione controllata di beni e servizi, o come meccanismi di autenticazione per l'accesso a dati e a luoghi riservati, e il prevedibile uso massiccio come supporto per sistemi di firma digitale, pone in evidenza il problema della sicurezza di tali dispositivi. L'utente di una smartcard desidera che solo lui (ed eventualmente chi sia stato autorizzato da lui) sia in grado di usare la carta, soprattutto in caso di smarrimento o furto della stessa; inoltre, solo con la sua autorizzazione deve essere possibile accedere ai dati contenuti all'interno della smartcard, in modo da evitare che vengano resi pubblici dati sensibili quali lo stato di salute, la religione, le abitudini sessuali, ecc. Infine, tali richieste di base di sicurezza devono valere anche nel caso in cui la carta venga inserita in un lettore contraffatto.

La realizzazione di questi criteri generali di sicurezza può essere suddivisa in più livelli, partendo dal livello fisico della smartcard (specificando quindi le tecniche costruttive in grado di resistere ad attacchi fisici e/o elettromagnetici), passando per il meccanismo di memorizzazione dei dati all'interno della memoria (specifica del Sistema Operativo e delle primitive crittografiche) fino alla sicurezza legata ai protocolli utilizzati nella comunicazione tra la smartcard e il lettore, così che non sia possibile spacciarsi per il proprietario di una smartcard quando ciò non sia vero, oppure falsificare i messaggi scambiati tra il lettore e la smartcard in modo da trarne vantaggio.

Già molto è stato fatto per elaborare criteri di valutazione della sicurezza delle tecnologie dell'informazione, pur con obiettivi lievemente diversi, secondo le esigenze specifiche dei singoli paesi od organismi. Per questo, sono stati elaborati insiemi di criteri che coprono tutti i livelli; qui sotto sono presentati i principali.





TCSEC

L'insieme di criteri più importante, e che per molti versi ha aperto la strada ad ulteriori sviluppi, noto come Trusted Computer System Evaluation Criteria, o più semplicemente TCSEC od Orange Book, è stato elaborato ed utilizzato, per la valutazione dei prodotti, dal Dipartimento della Difesa degli Stati Uniti. Anche altri paesi, per lo più Europei, vantano una notevole esperienza nella valutazione della sicurezza delle tecnologie dell'informazione e hanno elaborato, in merito, propri criteri di sicurezza. Nel Regno Unito, ad esempio, è il caso del CESG (Communication Electronics Security Group) Memorandum Number 3, elaborato ad uso del governo, e delle proposte del Dipartimento dell'Industria e Commercio, denominate Green Book, per i prodotti di sicurezza IT per uso commerciale. In Germania, l'ente per la sicurezza dell'informazione ha pubblicato, nel 1989, una prima versione dei propri criteri; allo stesso tempo, in Francia, sono stati elaborati criteri denominati Livre bleu-blanc-rouge.

ITSEC

I criteri ITSEC costituiscono il risultato degli sforzi di armonizzazione compiuti in ambito europeo nell'area della valutazione della sicurezza nell'Information Technology e, nonostante siano in atto a livello internazionale numerose attività per la definizione di nuovi criteri, rappresentano ad oggi un costante punto di riferimento. In particolare, l'Unione Europea ha espresso l'intenzione di sostenere i criteri ITSEC tramite una raccomandazione del 1995 nella quale si chiede che tali criteri siano applicati per la valutazione e la certificazione di prodotti, servizi e sistemi IT. Tale raccomandazione, inoltre, richiede che sia negoziato dagli Stati membri il riconoscimento reciproco a livello europeo e possibilmente internazionale dei certificati di valutazione della sicurezza.

Uno dei motivi dell'elaborazione di questi criteri armonizzati a livello internazionale è la volontà di costituire una base comune per l'attività di certificazione svolta dagli organismi nazionali dei quattro paesi che vi cooperano (Regno Unito, Germania, Francia e Paesi Bassi), con l'obiettivo finale di consentire il mutuo riconoscimento dei risultati delle valutazioni.

I criteri TCSEC classificano i sistemi secondo una gerarchia nella quale per ciascuna classe sono speci-

ficati sia requisiti di funzionalità che di assurance; i criteri ITSEC permettono, invece, la scelta di arbitrarie funzioni di sicurezza e definiscono sette livelli (E0, E1, ..., E6) di valutazione dell'assurance che rappresentano una crescente fiducia nella capacità del sistema di soddisfare le sue specifiche di sicurezza. La principale innovazione di questo approccio è costituita dalla netta separazione tra i requisiti di funzionalità e quelli di assurance.

Segue il sommario dei livelli di sicurezza definiti da ITSEC:

EO. Sicurezza inadeguata.

E1. Bisogna definire un target di sicurezza (TOE) e produrre uno schema informale dell'architettura. La documentazione per gli utenti e per l'amministratore daranno le direttive sulla sicurezza del TOE. Le funzioni di sicurezza da seguire sono testate dai valutatori e dagli sviluppatori. Vanno utilizzati metodi di distribuzione sicuri.

E2. Vanno prodotti sia uno schema informale ma dettagliato dell'architettura sia la documentazione dei test. L'architettura dovrà mostrare la separazione del TOE dagli altri componenti. Sono valutati i controlli sulla configurazione e sulla sicurezza di sviluppo. È richiesta una traccia di output (Audit) durante l'avvio e di tutte le operazioni eseguite.

E3. Va prodotto uno schema del codice sorgente e dell'hardware. Vanno evidenziate dettagliatamente le corrispondenze tra il codice sorgente e tale schema. Vanno utilizzate procedure di accettazione. I linguaggi implementativi devono essere standard. Bisogna rieseguire il test dopo la correzione degli errori.

E4. Vanno prodotti: modelli della sicurezza, specifiche semi-formali dell'applicazione delle funzioni di sicurezza, schemi dettagliati dell'architettura. Bisogna mostrare la validità dei test. Il TOE e i tools sono sotto il controllo della configurazione con audit dei cambiamenti.

E5. I disegni dell'architettura mostrano le relazioni reciproche tra i componenti atti a rinforzare la sicurezza. Vanno prodotte le informazioni riguardanti l'integrazione tra processi e librerie di runtime.

E6. Vanno prodotte descrizioni formali dell'architettura e delle funzioni atte a rafforzare la sicurezza e vanno mostrate le corrispondenze tra le specifiche formali delle funzioni di sicurezza attraverso il codice sorgente e i test. Differenti configurazioni di TOE vanno definite in termini di schemi architeturali formali. Tutti i tools sono soggetti a controlli di configurazione.

Common Criteria o ISO 15408

Per concludere la panoramica sui criteri di sicurezza è necessario citare l'attività di standardizzazione condotta dal gruppo di lavoro WG3 (Evaluation Criteria for IT Security) dell'ISO/IEC/JTC1/SC27 [ISO1, ISO2, ISO3], avviata nel 1990 con l'obiettivo di giungere alla definizione di criteri standard internazionali.

Dal 1993 le attività del WG3 sono risultate notevolmente condizionate da quelle di un altro gruppo, denominato CCEB (Common Criteria Editorial Board), nato per iniziativa della Comunità Europea e costituito da esperti europei, statunitensi e canadesi. L'obiettivo del CCEB è stato quello di armonizzare i criteri europei ITSEC, i nuovi criteri federali statunitensi e i criteri canadesi CTCPEC attraverso la definizione di una nuova raccolta di criteri denominata Common Criteria (CC). Ciò per consentire il riconoscimento reciproco, a livello internazionale,



dei risultati delle valutazioni, ottenendo pertanto una notevole semplificazione della distribuzione (e quindi dell'acquisizione) di prodotti valutati attraverso l'eliminazione dei costi che altrimenti dovrebbero essere sostenuti per effettuare le valutazioni necessarie nelle diverse nazioni. Inoltre i CC sono compatibili con i criteri di valutazione suddetti, consentendo ai produttori di salvaguardare eventuali investimenti già effettuati per la valutazione della sicurezza dei prodotti.

ISO/IEG ha ottenuto dalle Common Criteria Project Sponsoring Organizations una "non-exclusive license" per utilizzare i Common Criteria 2.0 come standard internazionale ISO/IEC 15408. L'8 giugno 1999 tali criteri sono stati approvati, accettati e codificati come ISO 15408-1, -2, -3.

I criteri di sicurezza Common Criteria sono organizzati in livelli chiamati EAL (Evaluation Assurance Levels). EAL1 è il livello minimo di sicurezza.

I primi quattro livelli possono essere generalmente applicati anche a prodotti e sistemi già esistenti. Oltre EAL4 è richiesta l'applicazione di tecniche di sicurezza specializzate. Il TOE che deve soddisfare questi livelli di sicurezza deve essere progettato e sviluppato con il preciso intento di soddisfare tali criteri. Al massimo livello (EAL7) ci sono limitazioni significative con un notevole impatto sia sul

costo di sviluppo sia su quello di valutazione. Segue l'elenco dei livelli di sicurezza definiti dai Common Criteria:

- EAL1: Testato funzionalmente.
- EAL2: Testato strutturalmente.
- EAL3: Testato e controllato metodicamente.
- EAL4: Progettato, testato e rivisto metodicamente.
- EAL5: Progettato e testato semiformalmente.
- EAL6: Schema verificato e testato semiformalmente.
- EAL7: Schema verificato e testato formalmente.

Come già accennato gli EAL dei Common Criteria sono stati sviluppati con l'obiettivo di preservare le garanzie e i risultati delle precedenti valutazioni. La seguente tabella può essere utilizzata per aiutare a fare una comparazione con gli standard precedenti.

Common Criteria	US TCSEC	ITSEC Europei
EAL1	D	E0
EAL2		E1
EAL3	C1	E2
EAL4	C2	E3
EAL5	B1	E4
EAL6	B2	E5
EAL7	A1	E6

Tabella 1: Corrispondenze tra i criteri di sicurezza.