ingenium

La rivista di scritti monografici del Gruppo Engineering

Sponsor di questo numero
INFOCAMERE

LA FIRMA DIGITALE

Dal documento informatico i nuovi scenari delle comunicazioni in rete

STRATEGIE D'IMPRESA E TECNOLOGIE DELL'INFORMAZIONE E DELLE COMUNICAZIONI

Numero 23 Mag[illegible] P. [illegible] tt. B art. [illegible] 23/12/96 n. 662 [illegible] L. 8.000

Firme digitali e Autorità di Certificazione
Le garanzie di validità degli atti elettronici

A. Michael Froomkin*
Professore Associato
di Internet Law
Università di Miami
Usa

La tecnologia della firma digitale garantisce la sicurezza delle comunicazioni su rete, ma non la reale identità degli interlocutori coinvolti. Occorre una Terza Parte Fidata. Le Autorità di Certificazione sono chiamate a garantire reciprocamente i soggetti della transazione elettronica.

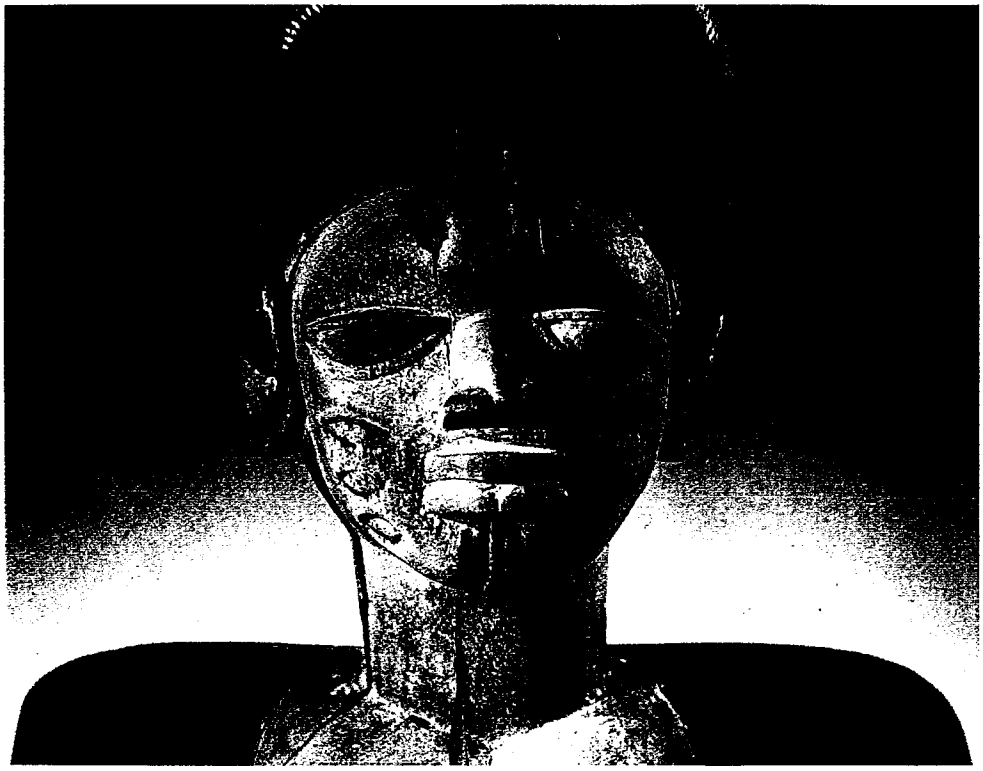
La firma digitale a chiave pubblica: garanzie e limiti dell'identificazione

La tecnologia della firma digitale crittografata a chiave pubblica consente di gestire in modo relativamente semplice una comunicazione sicura su una linea insicura. Infatti solo chi possiede una determinata chiave privata può generare un messaggio criptato che può essere letto dalla chiave pubblica corrispondente. Analogamente, un messaggio criptato con una chiave pubblica può essere letto solo da chi possiede la chiave privata corrispondente.
Se la comunicazione deve avvenire tra due parti (che possiamo chiamare Alice e Bob), tuttavia occorre essere certi che chi possiede l'altra chiave privata sia effettivamente il soggetto con cui si vuole entrare in comunicazione. Infatti nulla vieta che un terzo si spacci ad esempio per Bob e comunichi ad Alice la "propria" chiave pubblica, asserendo che si tratta di quella di Bob. In assenza di contenuti del messaggio già noti all'altra parte e che possano perciò costituire prova certa dell'identità del mittente, la tecnologia di criptazione a chiave pubblica garantisce solo la sicurezza del messaggio, non ancora l'identità degli interlocutori coinvolti.
Una possibile soluzione potrebbe essere la pubblicazione delle chiavi pubbliche, ad esempio su di un registro tenuto on-line da un terzo.
Tuttavia, se il gestore del registro si limita a pubblicare tutto ciò che riceve senza effettuare alcuna verifica, di nuovo viene meno ogni garanzia di sicurezza. Infatti nulla vieta che un terzo comunichi al registro la propria chiave pubblica e la propria casella di posta elettronica, ma con il nome di qualcun altro che vuole impersonare.

La necessità di una Terza Parte Fidata: le Autorità di Certificazione e i loro compiti

Per garantire un adeguato livello di sicurezza e di fiducia tra due soggetti che intendono comunicare per via telematica, e che non si conoscono, occorre che sia assicurata la corrispondenza tra l'identità di ciascuno e la sua chiave pubblica. Questo compito potrà essere svolto da qualunque Terza Parte che ispiri fiducia: un amico comune, un ufficio della Pubblica Amministrazione, un'impresa che offre servizi come Autorità di Certificazione (CA).
Infatti una CA è un organismo che soddisfa il bisogno di servizi di Terza Parte Fidata nel commercio o nella comunicazione elettronica, attraverso l'emissione di certificati che attestano determinati fatti rispetto ai soggetti cui i certificati si riferiscono. Affinché gli utenti possano aver fiducia in una Terza

* e-mail: froomkin@law.tm
http: //www.law.tm



Parte, occorre che questa soddisfi requisiti di sicurezza rispetto all'hardware e software che utilizza, alle procedure di verifica che mette in atto, e inoltre che sia garantita la corrispondenza con la sua chiave pubblica.
Di fatto questo significa che deve essere a sua volta riconosciuta come CA da qualche altro soggetto fidato. E' possibile sia un mutuo riconoscimento tra diverse CA, sia la certificazione di ciascuna di esse da parte di un'Autorità esterna o centrale, ad esempio appartenente alla Pubblica Amministrazione.
Al momento, le poche CA che stanno operando hanno affrontato il problema autocertificandosi e pubblicando la propria chiave pubblica sul Web o da altra parte. Alcuni esperti prevedono che il modello che si realizzerà sarà quello di una struttura piatta in cui ciascuna CA è certificata da almeno un'altra e in cui gli utenti si rivolgono per i propri certificati a organizzazioni note, siano i loro fornitori, le Poste, le Camere di Commercio o i notai.

I diversi livelli di intervento di una Autorità di Certificazione

Certificati di identificazione

Un certificato di identificazione lega il nome di un soggetto titolare di una chiave pubblica digitale a una persona o ente presente nel mondo reale. Un'identificazione accurata non è un compito banale e comporta, a seconda del tipo di certificato, accertamenti sempre più approfonditi. L'accettazione o meno della validità dei certificati emessi da una CA dipende anche da quanto l'utente consideri affidabili queste procedure. Naturalmente, per una comunicazione digitale il nome presente sul certificato non deve essere necessariamente un nome univocamente individuabile e neppure un nome reale. Il certificato può essere riferito a "Black Death X", oppure a "John Smith", oppure a "John Smith 1000 Main Street Eugene Oregon - Social Security Number 123-45-6789".

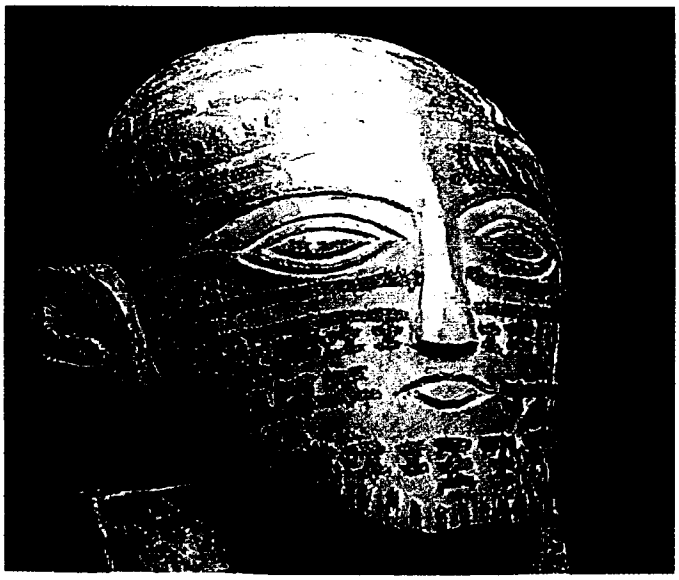
Il certificato è firmato dalla CA con la propria chiave privata, consegnato al titolare, reso pubblico o accessibile al pubblico per verificarne la validità.
Un certificato valido non è tuttavia una prova assoluta di identità. Per esempio, è possibile che nel corso del tempo la password di accesso alla firma digitale venga conosciuta da altri, che quindi potrebbero firmare al posto del titolare. Un modo per ridurre il rischio che un certificato non sia più valido è quello di inserirvi la data di emissione e quella di scadenza. Questo tuttavia non elimina il rischio che la chiave privata sia resa nota accidentalmente nello stesso momento in cui il certificato viene emesso. Per questo può essere opportuno verificare l'elenco dei certificati revocati, che ogni seria CA mette a disposizione degli utenti. Poiché questa operazione può avere un costo, anche minimo, si può decidere di effettuarla nel caso in cui il certificato sia stato emesso da oltre 30 giorni, o al limite da oltre 30 ore o anche 30 secondi. In assenza di prassi consolidate è l'utente che deciderà volta per volta cosa fare, definendo contemporaneamente il margine di rischio che si vuole assumere.

Certificati di qualificazione

I certificati di identità saranno il tipo di garanzia più diffuso nel breve termine, mentre nel medio diventeranno importanti certificati relativi ad altre caratteristiche del soggetto. Un certificato digitale potrà anche confermare l'età del soggetto o il possesso di determinati titoli o requisiti, come ad esempio l'appartenenza a un ordine professionale, la sua autorizzazione come utente di un software particolare, il suo potere di firma all'interno di un'organizzazione, o l'iscrizione alla Camera di Commercio.
Un certificato di questo tipo può contenere il nome del soggetto titolare, ma questo non è sempre necessario. Se Mario Rossi è Direttore Generale della MR srl, il certificato può attestare questa qualità, senza bisogno di rivelare il nome del soggetto. Questo può consentire forme sofisticate di commercio elettronico, ad esempio per l'accesso a un conto numerato in una banca svizzera o per l'acquisto di materiale vendibile solo ad adulti, garantendo la privacy.

Certificati che attestano una transazione

Un'Autorità di Certificazione può anche attestare fatti relativi ad una transazione elettronica. Un certificato di questo tipo non è emesso per essere riutilizzato, ma attesta semplicemente che la Terza Parte è stata testimone di un avvenimento. Per esempio, un notaio può testimoniare, firmando con la propria chiave privata un contratto già firmato con un'altra chiave privata, che la firma è stata apposta in sua presenza.
Questo tipo di certificati ha interessanti implicazioni di carattere legale. Primo, l'Associazione dei Procuratori Legali Americani (American Bar Association) e la Camera di Commercio Internazionale stanno esplorando la possibilità di creare la figura del CyberNotary. La speranza è che atti legali sottoscritti negli Usa e certificati da un CyberNotary siano legalmente validi negli Stati di "civil law", quali ad esempio l'Italia, mentre l'assistenza di un normale avvocato o notaio statunitense non sarebbe sufficiente. Casi possibili sono il trasferimento di quote azionarie o l'assegnazione di un incarico di rappresentanza legale. Secondo, un certificato di questo tipo incorpora informazioni sulle verifiche espletate dalla CA nell'occasione specifica, mentre una normale firma digitale attesta solo verifiche eseguite al momento del rilascio. Inoltre la CA può aggiungere ulteriori informazioni, ad esempio la data in cui l'evento si è verificato o i destinatari di un determinato messaggio.



Certificati che attestano la data di un evento

In certi casi può essere di notevole importanza conoscere il momento esatto in cui un documento è stato validato. Un "time-stamp" è una sorta di bollo digitale, reso non falsificabile attraverso un sistema di crittografia a chiave pubblica, che attesta che un documento esisteva in un momento particolare. Per avere validità universale, deve far riferimento a un tempo preciso di riferimento, ma questo è solo un dettaglio tecnico. Infatti qualsiasi data inserita da un computer, come quella inserita automaticamente su un documento al momento della stampa, può essere facilmente manipolata. L'unico modo di definire con certezza il momento di un evento è pertanto quello di collocarlo tra due eventi esterni, non manipolabili.

Se un documento cita un fatto noto al momento della creazione, dimostra di essere posteriore a questo. Ma questo non è sufficiente per definire il momento esatto in cui un evento si è verificato, e quindi la sua eventuale priorità rispetto ad altri eventi. Il documento infatti potrebbe essere stato creato in qualsiasi momento successivo al fatto citato. L'unico modo di provare con certezza che un documento sia stato prodotto prima di un certo tempo è quello di generare un altro evento basato sul documento che possa essere osservato da altri. Ad esempio, il documento potrebbe essere pubblicato su un giornale. Ma la cosa è costosa e rende pubbliche informazioni che magari si vuol tenere riservate. Una possibile soluzione è quella di calcolare un valore digitale, un'impronta del documento stesso ("hash value"), praticamente non falsificabile e attraverso la quale non è possibile ricostruire il documento originale, e di rendere pubblica solo questa. La funzione di pubblicità può essere svolta da una CA che, al ricevimento dell'impronta digitale, restituisce una ricevuta costituita dall'impronta più la data, firmata con la sua chiave privata. Tuttavia, nulla vieta che, per errore o per dolo, il "time-stamp" apposto dalla CA sia errato. Un sistema più sicuro è quello in cui la CA restituisce non solo l'impronta da validare, ma le ultime impronte ricevute da altri soggetti, con il relativo indirizzo di posta elettronica. In questo modo un'eventuale frode dovrebbe coinvolgere molti soggetti.

Un sistema flessibile di garanzie per il commercio elettronico

In una transazione elettronica non sempre i servizi forniti da una CA sono necessari.

Nel caso in cui un prodotto o un servizio sia scambiato con denaro, può essere sufficiente una carta di credito o denaro elettronico, con la società emittente che svolge il ruolo di Terza Parte. Di fatto la transazione è molto simile a quelle che possono avvenire in un negozio o via telefono o per posta. Il venditore è abbastanza sicuro dell'incasso, il compratore si basa sulla notorietà e sulla reputazione del primo. Nel commercio elettronico può tuttavia essere più difficile reperire il venditore in caso di reclami, ma se si paga con carta di credito è sempre possibile bloccare il pagamento. L'esigenza di certificati è quindi probabilmente limitata alle transazioni di maggiore importo.

Si prevede che il denaro elettronico verrà usato per pagamenti di così piccolo importo da rendere eccessivamente onerosa la verifica immediata con la banca emittente.

Al contrario, se gli effetti della transazione sono durevoli (come la presentazione di documenti dovuti a una Pubblica Amministrazione, un servizio di home banking o un ordine per una commessa di importo elevato), le parti hanno un interesse molto maggiore a identificarsi reciprocamente con sicurezza.

Nessun fornitore accetterebbe ordini con pagamento successivo alla consegna, nemmeno da un cliente abituale, senza essere sicuro che la chiave usata per firmare appartenga a una persona autorizzata a piazzare l'ordine.

In questo caso è importante sia che il certificato attesti l'identità della persona, ed eventualmente la sua autorizzazione a firmare l'importo dell'acquisto, sia che la persona non abbia lasciato l'incarico e che la segretezza della chiave non sia stata violata.

Ovviamente, questo può essere verificato attraverso l'elenco delle chiavi revocate. L'uso di certificati nel mondo reale delle transazioni elettroniche sarà pertanto proporzionato al rischio implicito nella transazione e al rapporto tra costo sostenuto e benefici acquisiti in termini di sicurezza.

I servizi e le tecnologie di un'infrastruttura di certificazione

Lo scopo di un'infrastruttura di servizio a chiave pubblica (PKI) è fornire una piattaforma affidabile per la gestione, da parte di un'Autorità di Certificazione (CA), dei servizi di firma digitale e di crittografia. Ciò è essenziale soprattutto per i servizi di supporto a transazioni di commercio elettronico, dalla semplice messaggistica ai servizi di certificazione più sofisticati.

Gestione dei certificati

I certificati sono i documenti su cui si fonda l'affidabilità dei servizi erogati. Le funzioni chiave per una loro gestione adeguata sono:

• Certificazione e Registrazione

La certificazione e registrazione di un utente può avvenire direttamente on-line. Tutti i fornitori di tecnologia offrono questa funzionalità (sostanzialmente è uno scambio di messaggi via posta elettronica). Per quanto rapida ed economica, tuttavia, questa modalità offre un livello di affidabilità molto debole sulla reale identità dell'utente. Ben più sicura è la registrazione tramite presentazione diretta dell'utente agli sportelli del certificatore, eventualmente corroborata da qualche documento di identità. Questa procedura è di particolare importanza, se la firma dell'utente ha anche potere di rappresentanza di un ente.

• Sospensione/Revoca dei certificati

Ogni PKI deve garantire contromisure efficaci per gli usi fraudolenti o scorretti di un certificato o di un servizio. La revoca di un certificato può avvenire per svariate ragioni (ad es. una nuova posizione professionale, un cambio di residenza o nazionalità, ecc.). E' essenziale quindi la creazione di una Certificate Revocation List (CRL) per garantire che i certificati non più validi siano revocati tempestivamente. L'atto di revoca deve essere tempestivo e deve recare la data e l'ora esatta in cui è diventato operativo. Tutte le CA serie offriranno questo servizio, che in alcuni Paesi è anche un obbligo di legge.

• Accesso agli elenchi di certificati rilasciati o revocati

Gli utenti hanno il diritto di accedere alle liste dei certificati rilasciati o revocati, per accertarsi l'un l'altro. Per consentire a tutti semplicità di accesso a queste liste, quasi tutti i fornitori di tecnologia offrono una directory su standard X.500.

Gestione delle chiavi crittografiche

Ricordiamo che una firma digitale si basa essenzialmente su una coppia di chiavi asimmetriche (chiave pubblica e chiave segreta).

• Lunghezza delle chiavi

Il numero di bit che compone una chiave ha una relazione fondamentale con la possibilità di rompere il codice segreto. E' ormai abituale l'utilizzo di codici di 1.024 bit per le chiavi di firma digitale. Alcune CA addirittura utilizzano chiavi a 2.048 bit. Oggi, codici di simili dimensioni sono praticamente inviolabili.

Ovviamente, l'esigenza di codici ancora più lunghi crescerà propor-

zionalmente all'aumento della potenza di calcolo degli elaboratori.

• Copia e recupero delle chiavi

Dal momento che solo il legittimo intestatario deve essere in grado di usare la propria firma, la tendenza generale è di non duplicare le chiavi private per la firma. Ma il problema con le chiavi per la codifica dei messaggi è sensibilmente diverso. Se si smarrisce una chiave segreta, l'accesso ai dati codificati in precedenza diventa virtualmente impossibile. Possono anche sussistere norme legali per il deposito in garanzia di chiavi o per datori di lavoro che devono gestire chiavi di protezione di informazioni societarie. Un metodo per la gestione degli accessi alle chiavi è una componente necessaria di una PKI. Se si possa certificare la veridicità di atti avvenuti in precedenza, nel caso che le chiavi siano smarrite o compromesse, è una questione dibattuta.

Accesso all'infrastruttura

• Pacchetti software per gli utenti

Si richiedono metodi di accesso degli utenti all'infrastruttura tecnologica, che siano semplici da integrare e da sviluppare. Generalmente queste vie di accesso sono consentite da plug-in dei browser Web.

Garanzie verso terzi

L'atto di registrazione di un utente è una forma di contratto che implica doveri e responsabilità. E' importante quindi che il certificato di registrazione rilasciato da una CA specifichi, anche di fronte a terzi, le procedure di accertamento e le condizioni in base alle quali il certificato è stato rilasciato.

• Dichiarazione sulle regole contrattuali dei certificati

Per agevolare questo compito, alcuni

sistemi supportano modelli di documenti che consentono di rendere disponibile anche on-line le specifiche contrattuali di un certificato (Certificate Practice Statement), al momento stesso della registrazione. Queste misure rendono più agevole la procedura di registrazione e riducono i rischi di errore o di incomprensione tra i contraenti. La dichiarazione spesso include anche i metodi e la disponibilità del gestore a una certificazione incrociata con altri gestori.

• Registrazioni per verifiche legali

Nel caso di una disputa sulla validità legale o sulle implicazioni di una firma digitale, il certificatore sarà chiamato in causa per esibire prove sulla veridicità di certi eventi avvenuti anche a distanza di tempo. Per garantire questa possibilità, un gestore di servizi di certificazione sarà tenuto per legge a mantenere registrazione delle transazioni per tutti i servizi che offre. Tutti i certificatori useranno quantomeno un motore database su standard SQL per estrarre questo tipo di informazioni.

Interoperabilità e certificazione incrociata con altre CA

Può capitare di frequente il caso di una comunicazione o di una transazione tra utenti certificati da diverse CA. Per garantire la massima libertà di interscambio globale, è dunque essenziale la possibilità di certificazione incrociata tra diverse CA, sia sotto il profilo politico che tecnologico.

• Struttura di certificati standard

Il rispetto di specifiche standard nell'implementazione dei certificati consente tecnicamente la reciproca certificazione di atti tra infrastrutture di gestori diversi. L'accordo sullo standard PKIX renderà molto più agevole questa possibilità.

Servizi ulteriori

Si può prevedere che le future PKI includeranno anche le seguenti caratteristiche:

• Time-Stamping (timbro digitale di data e ora)

Oggi la funzione time-stamping è usata solo dalle Autorità di Certificazione quando siglano o revocano i loro certificati.

Tuttavia, il time-stamping è un'utile funzione che andrebbe offerta anche agli utenti per la loro messaggistica.

• Certificati di autorizzazione

Specificano l'appartenenza, i diritti e le cariche di un individuo e consentono diversi tipi e livelli di autenticazione o autorizzazione.