IL FUTURO DELLA FIRMA DIGITALE

Giovanni Manca

Negli ultimi anni, la firma digitale è stata oggetto di interesse sia giuridico che tecnologico soprattutto perché è possibile, tramite essa, garantire l'autore di un documento informatico e verificare che tale documento non abbia subito modifiche dopo la sottoscrizione. Nel presente articolo, viene descritta l'evoluzione a cui i meccanismi della sottoscrizione digitale saranno soggetti per poter rispondere nell'immediato futuro, alle esigenze di efficienza e sicurezza che lo scambio in rete di documenti informatici rende indispensabile.

1. PREMESSA

A partire dal 1997, in Italia, una serie di provvedimenti legislativi hanno conferito valore giuridico al documento informatico e alla firma digitale. La pubblicazione della Direttiva Europea 1999/93/CE[1], nel gennaio del 2000, ha dato ulteriori impulsi al processo legislativo, imponendo un quadro comune agli stati dell'Unione Europea. Il processo legislativo ha anche fornito delle indicazioni sulle tecnologie da impiegare per ottenere delle firme digitali che possano ritenersi equivalenti a quelle autografe. Le tecnologie coinvolte in questo processo, ancora oggi, si stanno evolvendo per seguire esigenze sempre più complesse nella sottoscrizione digitale, nello scambio in rete e nella successiva conservazione dei documenti informatici. In questo articolo viene descritto quanto sta accadendo a livello di standardizzazione e di disponibilità di prodotti di mercato, sia a livello nazionale che europeo. Allo stato attuale, è possibile sottoscrivere digitalmente un documento informatico e, purché ci si attenga alle norme vigenti, ottenere per esso piena validità legale. Per poter rispondere alle nuove esigenze, non indipendenti, di armonizzazione con le leggi europee e di rispondenza all'evoluzione degli standard, è stato necessario realizzare nuove funzioni. Si analizza, inoltre, sinteticamente come è possibile sottoscrivere, digitalmente, un documento informatico (Paragrafo 2); come si sono evoluti i sistemi per la collocazione certa nel tempo (marcature temporali) di un documento informatico sottoscritto digitalmente (Paragrafo 3) e in che modo sono stati definiti specifici meccanismi per collegare un documento informatico al suo riferimento temporale e per garantirne la verifica anche dopo molti anni (Paragrafo 4). Si descrivono, successivamente, le liste di revoca e sospensione (Paragrafo 5) indispensabili per la verifica; il modo mediante cui i certificati

[1] Directive 1999/93/EC of the European Parliament and of the Council on a common framework for electronic signatures.

digitali, già ampiamente utilizzati, sono stati ridefiniti come qualificati dalla già citata Direttiva e come, di conseguenza, si è rivelato necessario definire il formato delle nuove informazioni che devono contenere: di esse, occorre sottolineare, soprattutto, il ruolo del sottoscrittore, molto importante se la firma deve essere contestuale all'attività e quindi all'attribuzione degli incarichi del firmatario (Paragrafo 6). Si prende in esame anche la necessità che tutti questi nuovi formati e strutture dei dati possano ricorrere all'utilizzo evoluto di buste crittografiche (Paragrafo 7) e di nuove tecnologie come il linguaggio XML (*eXtensible Markup Language*) (Paragrafo 8). Infine, per gli scambi dei documenti in rete verrà analizzato il problema dell'interoperabilità cioè del riconoscimento del sottoscrittore, della validità della sottoscrizione e della presenza dei requisiti legali che rendono la sottoscrizione pienamente equivalente a quella autografa. Nell'ultima parte (Paragrafo 9), è possibile osservare che tutte le novità descritte si applicano al modello operativo già adottato.

2. LE BASI TECNICHE DELLA FIRMA DIGITALE

Prima di affrontare i vari temi illustrati nella premessa, è opportuno richiamare i concetti tecnici che sono alla base della firma digitale. Per prima cosa, si deve chiarire che l'espressione *firma digitale* si riferisce a meccanismi di sicurezza che permettono di garantire una serie di servizi come l'autenticazione del mittente, l'integrità dei dati inviati e le possibili contestazioni sul fatto di non aver eseguito la sottoscrizione su di essi.

Pur essendo stata introdotta con standard che non facevano riferimento ad una particolare tecnologia, sino ad oggi, la firma digitale è stata realizzata con meccanismi di crittografia asimmetrica accompagnati da particolari **funzioni** denominate ***hash***.

Le **funzioni hash** sono funzioni matematiche che generano, a partire da una generica sequenza di simboli binari, una ulteriore sequenza di lunghezza predefinita e determinata dalla funzione prescelta. Tale sequenza viene comunemente definita *impronta*. Quest'ultima, viene calcolata in modo tale che risulti, di fatto, impossibile determinare una sequenza di simboli binari che la generi e, inoltre, risulti impossibile determinare una coppia di sequenze di simboli binari per le quali la funzione generi impronte uguali.

La citata Direttiva europea 1999/93/CE, relativa ad un quadro comunitario per le firme elettroniche, ha introdotto concetti differenti. Quello che maggiormente interessa, in questo contesto, è appunto quello di firma elettronica, definita dalla Direttiva come "dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici ed utilizzati come metodo di autenticazione". Inoltre, poiché il firmatario è definito come *persona*, le relazioni con le sottoscrizioni autografe sono evidenti. Naturalmente, la firma elettronica non può essere essa stessa equivalente ad una autografa, ma è indispensabile che siano soddisfatte una serie di ulteriori condizioni. L'insieme di tali condizioni (vedi la Direttiva per le definizioni di *firma elettronica avanzata, certificato qualificato* e *dispositivo per la creazione di una firma sicura*) portano a considerare nuovamente la firma digitale definita nella legislazione italiana (D.P.R. 445 del 28 dicembre 2000), come unico strumento per ottenere l'equivalenza legale con la firma autografa.

Descritte le principali premesse giuridiche, si analizza, sinteticamente, in che modo è possibile effettuare una firma digitale.

Tutto si basa su una cosiddetta infrastruttura a chiave pubblica. Ogni utente dispone di due chiavi crittografiche, ovvero due particolari codici numerici. Uno di essi viene reso pubblico, mentre il secondo deve rimanere assolutamente segreto (chiave privata). Queste coppie di chiavi devono la loro efficacia alle caratteristiche delle funzioni matematiche alle quali sono associate. In particolare, i dati crittografati con l'una possono essere decifrati solo con l'altra e viceversa.

La sottoscrizione digitale prevede che il documento da sottoscrivere sia sottoposto a una elaborazione capace di estrarre, da esso, un riassunto univoco che è associabile ad una impronta del documento stesso. Le funzioni matematiche, denominate funzioni di hash, coinvolte in tale elaborazione sono tali da garantire che a documenti di-

Una coppia di **chiavi asimmetriche** è costituita da due numeri che, rappresentati in binario, hanno generalmente, nell'utilizzo industriale corrente, la lunghezza di 1024 bit. La caratteristica peculiare di queste chiavi è che i dati cifrati con la chiave pubblica possono essere decifrati solo con l'uso della corrispondente chiave privata e viceversa. Ciò rende possibile la diffusione della chiave pubblica all'esterno (da cui il nome), mentre la chiave privata è nota a una sola persona e nelle applicazioni con elevati requisiti di sicurezza (come la firma digitale) viene protetta all'interno di dispositivi che ne impediscono l'estrazione come le *smart card*. La chiave privata ovviamente non è deducibile dalla conoscenza della chiave pubblica. Il più famoso algoritmo asimmetrico è l'RSA (Rivest-Shamir-Adleman dal nome dei suoi autori).

versi, anche per un solo *bit*, corrispondano, con elevata probabilità, impronte digitali diverse. Esiste, tuttavia, la possibilità, che, a documenti differenti, corrispondano impronte uguali. Mediante la chiave privata del mittente si cifra l'impronta del documento da inviare al destinatario. Ogni volta che si vuole verificare la firma, ovvero controllare l'autenticità di un documento in relazione alla firma apposta in modo digitale, è sufficiente calcolare l'impronta del documento mediante la stessa funzione di hash utilizzata dal mittente; poi, grazie alle proprietà della **coppia di chiavi** asimmetriche, utilizzando la chiave pubblica del mittente è possibile effettuare la decodifica della firma, ottenendo l'impronta calcolata in precedenza. In caso di coincidenza dell'impronta originale con quella calcolata su quanto ricevuto, si verifica che la firma è attribuibile al possessore della chiave privata associata alla chiave pubblica utilizzata per decodificare la firma (Figura 1). Per garantire che la verifica della firma digitale sia affidabile, l'operazione di verifica è ovviamente di elevata criticità: essa avviene utilizzando la chiave pubblica del firmatario. Chi riceve il documento deve essere certo che la firma corrisponda alla chiave privata e che l'autenticità dei dati personali associati alla chiave pubblica sia assicurata da una terza parte fidata, ovvero il certificatore[2].
La principale attività del certificatore è quella di verificare e registrare l'identità dell'utente, associandola poi al cosiddetto certificato di chiave pubblica. Tale particolare documento informatico, firmato dal certificatore al fine di garantirne l'integrità del contenuto e l'autenticità dell'origine, contiene i dati identificativi

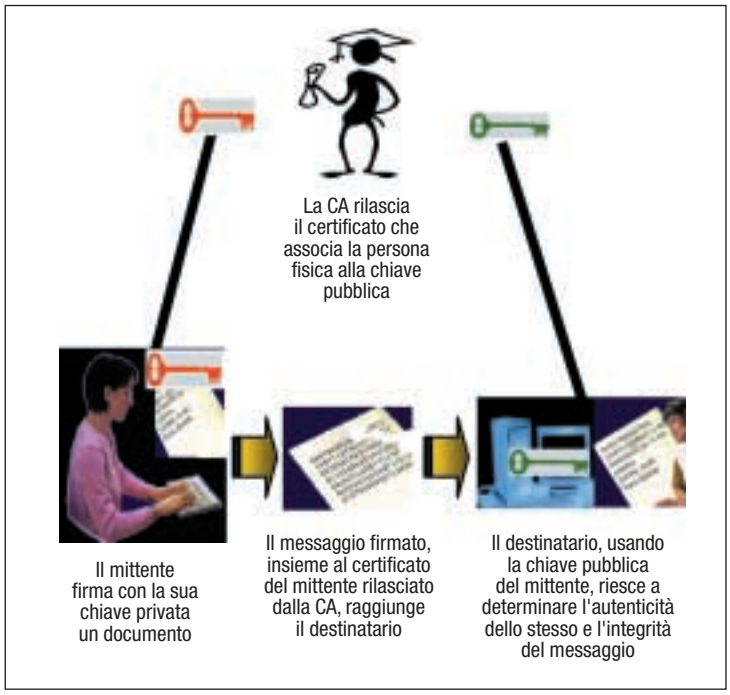

FIGURA 1
Il processo di firma

e la chiave pubblica del titolare. I destinatari verificheranno i documenti ricevuti e sottoscritti digitalmente, semplicemente utilizzando il certificato allegato al documento: essi possono, per maggior sicurezza, consultare le liste di sospensione e revoca per assicurarsi che il certificato non sia stato revocato. Il tema della consultazione delle liste di revoca sarà affrontato in seguito.
Oltre alla certificazione, un altro procedimento importante è il riferimento temporale, argomento che sarà trattato nel prossimo paragrafo in cui si vedrà come sia necessario disporre di questa informazione per ottenere un processo di verifica veramente completo.

3. IL RIFERIMENTO TEMPORALE

Come già precedentemente accennato, la firma digitale si basa su particolari funzioni matematiche e su meccanismi crittografi-

2 Attualmente, in Italia, ci sono 14 certificatori e il loro elenco (completo dei link ai loro siti Internet) è consultabile sul sito www.aipa.it.

ci, i quali, però, possono essere forzati con i cosiddetti "attacchi di forza bruta". Tali attacchi utilizzano insiemi di chiavi e tentano di forzare la crittografia semplicemente provandole tutte. È in quest'ottica che i certificati di chiave pubblica hanno tra le loro caratteristiche un periodo di validità. Allo stato attuale, il periodo di validità di un certificato è determinato anche da esigenze commerciali. I certificatori, infatti, anche se non esiste alcun rischio apprezzabile, raramente emettono certificati con validità superiore all'anno. In questo modo, possono beneficiare degli introiti dei rinnovi dei certificati di chiave pubblica talvolta applicando tali rinnovi alla stessa chiave pubblica "in scadenza". Quanto descritto, evidenzia che esiste un legame tra le firme digitali e il tempo.

4. LA VERIFICA DELLA FIRMA E IL TEMPO

Se si suppone, per esempio, di ricevere un documento informatico sottoscritto digitalmente e di doverlo conservare per un periodo di tempo superiore a quello della validità del certificato di chiave pubblica del firmatario del documento, appare evidente che, una volta superato tale periodo di validità, non risulta scontato dimostrare che la sottoscrizione digitale di un documento con la coppia di chiavi, la cui parte pubblica è contenuta nel certificato scaduto, è avvenuta prima di tale scadenza. Al fine di poter dimostrare che tale operazione è stata realizzata nell'intervallo tra l'emissione del certificato e la sua scadenza, è necessario associare al documento una marca temporale. Il processo di generazione di una marca temporale è mostrato in figura 2.
Tale processo inizia con il calcolo dell'impronta del documento tramite una funzione di hash. Tale impronta viene inviata all'interno di una richiesta di marca temporale alla *Time Stamp Authority* (TSA). Questa struttura elabora la richiesta di marcatura e associa, mediante una busta crittografica, data e ora esatte all'impronta del documento. Il tutto, poi, è "sigillato" mediante la firma della TSA . L'operazione di firma garantisce che il legame tra il documento (in forma

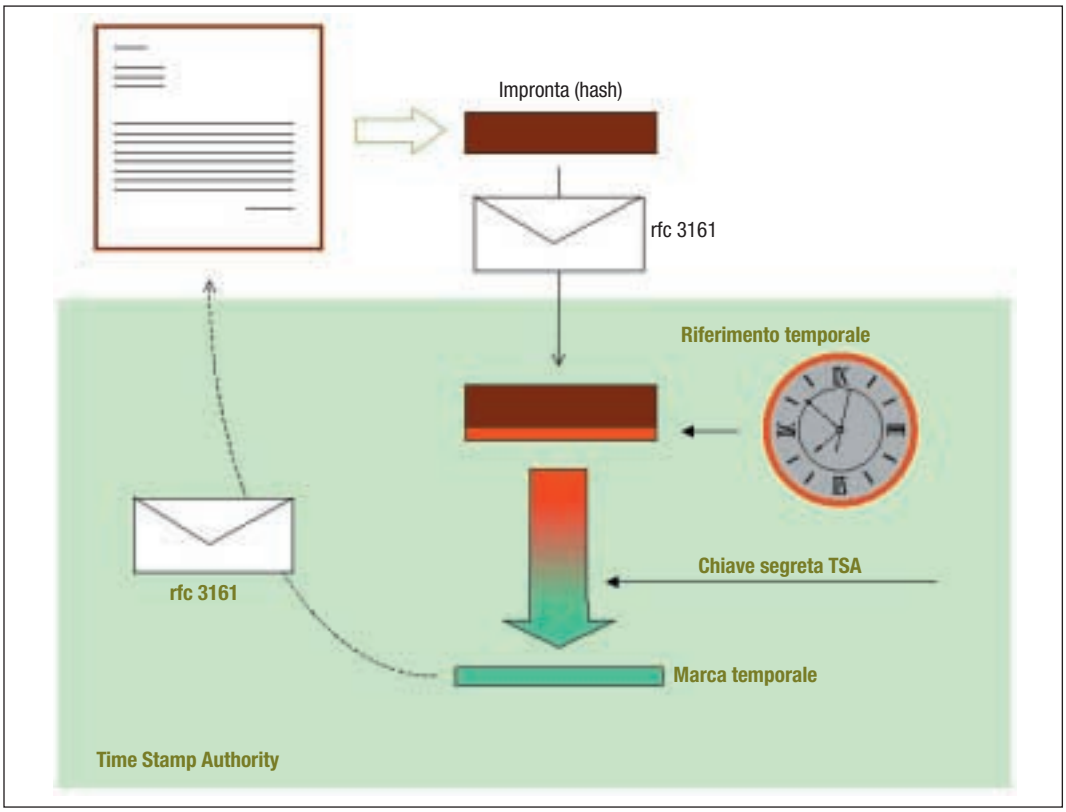

FIGURA 2
Generazione di una marca temporale

La **marcatura temporale** è l'attribuzione a un documento della certezza circa il momento in cui questo è stato redatto e, ma non necessariamente, firmato digitalmente. Consiste nella generazione promossa da una terza parte fidata, in generale, il certificatore, di un ulteriore sottoscrizione digitale che si va ad aggiungere a quella eventualmente apposta al documento informatico. L'operazione di marcatura aggiunge, alla solita impronta del documento, data e ora, ottenuti da una fonte certa. Questo insieme di dati, unito ad altre informazioni di servizio, viene firmato con una chiave privata del certificatore, dedicata a questo scopo, divenendo "marca temporale". La marca temporale viene poi inviata al richiedente che la associa al relativo documento.

di impronta) e il tempo non può essere più alterato. Lo standard che determina i formati delle strutture e dei dati nel processo di **marcatura temporale** è l'RFC (*Request For Comment*) 3161 [4], pubblicato nell'agosto del 2001, che garantisce un unico formato di marca temporale e quindi costituisce la base indispensabile per la totale interoperabilità tra le marche temporali. L'assenza di uno standard di riferimento, infatti, aveva reso sino ad ora praticamente inutilizzabile la marcatura temporale; ciò a causa dell'impossibilità di garantire l'interoperabilità tra realizzazioni differenti.
Avere a disposizione questo standard non è sufficiente, però, per risolvere il problema del collocamento certo nel tempo del documento informatico. Rimane infatti da risolvere il legame tra il documento e il riferimento temporale. Un modo per risolvere tale problema è stato proposto dall'ETSI (*European Telecommunication Standard Institute*) all'interno dello standard TS 101 733 [4], per il quale vale la pena effettuare un minimo di approfondimento, essendo molto importante per il trattamento di un documento informatico per un lungo periodo di tempo. Nello standard viene introdotto il legame tra documento informatico (anche non sottoscritto) e il riferimento temporale: quest'ultimo può essere una marca temporale come definita nell'RFC 3161, integrato con lo standard europeo ETSI TS 101 861 [6]. Questo legame non è logicamente difforme da quanto descritto in precedenza, ma introduce la ripetizione periodica della marcatura temporale su un documento. Quest'ultimo infatti dovendo essere conservato per parecchi anni, non può garantire, in fase di verifica, tutti gli elementi di fiducia necessari per il fatto che il certificato è scaduto; ciò avviene perché la chiave del certificatore è risultata compromessa, ovvero perché gli algoritmi utilizzati per il calcolo dell'impronta potrebbero dar luogo nel tempo e con l'incremento dei documenti elaborati, a possibili collisioni. A tutto ciò va aggiunto il fatto che anche la marca temporale scade e quindi deve essere rinnovata. Il modello citato garantisce in tal senso. Ogni volta che il contesto lo richiede, mediante buste crittografiche standard (Paragrafo 7), si imbustano nuovamente, in una nuova busta marcata temporalmente, le informazioni che stanno per diventare non più collocabili con certezza nel tempo.
Anche la marcatura temporale è critica e deve essere ottenuta mediante una richiesta sulla rete, inviando a colui che emette le marche temporali (oggi, il certificatore), l'impronta del documento coinvolto. Il processo funziona, ma, su grossi volumi di dati, potrebbe risultare non efficiente. Per tali motivi, attualmente, la marcatura temporale è considerata un ostacolo alla piena diffusione della firma digitale: dove è possibile si cerca di utilizzare collocazioni temporali alternative. Validi esempi, in tal senso, sono il protocollo informatico, la conservazione ottica e, ove applicabile, un riferimento temporale della transazione all'interno del sistema informativo.

5. LE LISTE DI REVOCA

La verifica di una firma digitale richiede un controllo sul certificato per verificare se è scaduto o se è stato revocato. La scadenza viene subito messa in evidenza dalle informazioni *not before* e *not after* presenti nel certificato, firmato dal certificatore e quindi non alterabile. Tali informazioni indicano l'intervallo di validità del certificato.
Per le informazioni di revoca si ricorre alle *Certificate Revocation List* (CRL), che sono liste di certificati con relativa data di revoca. Sono in grado di rappresentare altre informazioni come il motivo della revoca, la data e

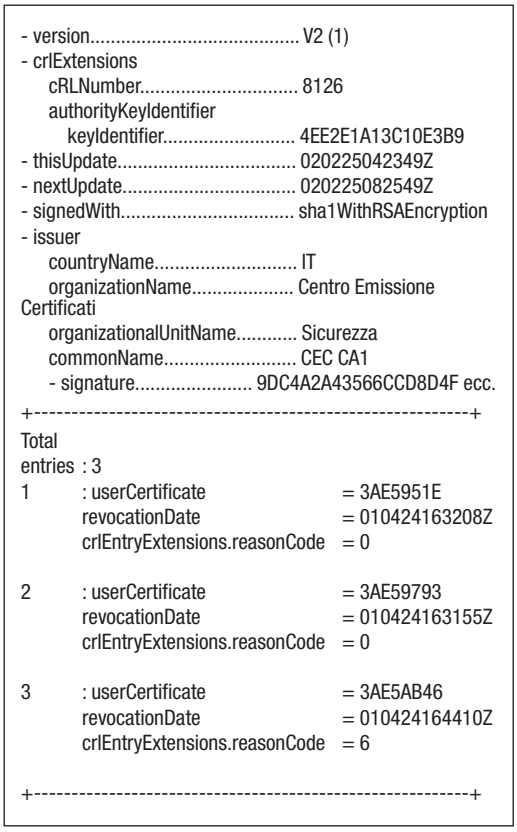

FIGURA 3
Dati principali di una lista di revoca

l'ora di emissione della lista corrente e la data e l'ora di emissione della successiva. Per garantire l'integrità di queste informazioni, la CRL viene firmata dalla CA (*Certificate Authority*) che ha emesso i certificati.
Nella figura 3 sono mostrati i dati essenziali di una CRL.
Si notino i campi *this update* e *next update* che forniscono informazioni sull'intervallo di validità della CRL corrente e le informazioni relative alle tre revoche. Per ciascuna viene indicato il numero seriale del certificato del titolare, la data di revoca e il motivo della revoca. Secondo l'RFC 2459 [8] è possibile specificare alcuni codici di motivazione. Nell'esempio, vengono refenziati il codice 0 che significa *reason: unspecified* e il codice 6 che indica il *Certificate hold*. Ciò significa che un certificato può non essere attivo, cioè sospeso, ma può successivamente essere riattivato.
Qualora il numero dei certificati emessi dal certificatore tenda a diventare molto grande, anche le CRL, di conseguenza, aumentano la loro dimensione. Questo fatto rende più difficile il lavoro di verifica di una firma digitale in quanto, nel corso di tale operazione, il *client* deve disporre e poi elaborare CRL sempre più grandi. L'elaborazione ne risulta appesantita e non è efficace in ambienti che necessitano di alte prestazioni. Per fortuna esistono alternative e una di esse è l'*Online Client Status Protocol* (OCSP). Tale protocollo è descritto nell'RFC 2560 [11] e il suo funzionamento consente ad un client di effettuare una richiesta di verifica della validità di un certificato a un *OCSP server*. Tale server risponde semplicemente con un "valido/non valido": è importante collocare nel tempo questa risposta e quindi, in alcuni contesti, la risposta ottenuta deve poter essere associata a un riferimento temporale.

6. LA FIRMA DIGITALE E IL RUOLO DEL SOTTOSCRITTORE

Come analizzato nel paragrafo dedicato ai certificati qualificati (Paragrafo 2), è senz'altro possibile includere in essi informazioni relative al ruolo del titolare o, come si dice comunemente, ai suoi attributi organizzativi. Tali informazioni, sono indispensabili in tutti quei casi dove la verifica della firma non è sufficiente per poter accettare come "valido a tutti gli effetti" il documento informatico ricevuto.
Due esempi "classici" della vita quotidiana possono essere rappresentati dalla firma di un medico che completa una ricetta o da un avvocato che iscrive una causa in tribunale. Altri esempi sarebbero possibili, ma il problema rimane lo stesso. Chi ha firmato il documento, anche se in maniera corretta, aveva titolo per poterlo fare in quel contesto?
Il ruolo, lo abbiamo già detto, può essere inserito anche in un normale certificato, ma questa operazione porrebbe il certificatore nell'imbarazzo di doversi sostituire agli ordini professionali ovvero all'organizzazione interna delle aziende. Inoltre, il ruolo in molte situazioni può variare molto rapidamente (si pensi, come caso limite, ad una commissione che aggiudica gare d'appalto i cui componenti terminano le attività dopo alcune ore) e ciò rende onerosa la gestione delle revoche e delle successive emissioni dei certificati.
La soluzione che si sta affermando anche in contesti diversi dalla firma digitale è quella delle *Privilege Management Infrastructure* (PMI) che emettono i Certificati degli Attributi

(AC). Un AC è composto da un insieme di informazioni firmate digitalmente da una terza parte fidata. Un AC non contiene alcuna chiave pubblica, mentre contiene una serie di informazioni la cui codifica e semantica possono essere definite solo in modo generale, in quanto fortemente dipendenti dal contesto. La sintassi è definita nello standard X.509 [9] come mostrato di seguito utilizzando la notazione ASN.1 (*Abstract Syntax Notation*):

```
AttributeCertificate ::= SEQUENCE
{
   acinfo                AttributeCertificateInfo
   signatureAlgorithm    AlgorithmIdentifier
   signatureValue        BIT STRING
}
AttributeCertificateInfo ::= SEQUENCE
{
   version               AttCertVersion DEFAULT v1,
   owner                 Owner
   issuer                AttCertIssuer
   signature             AlgorithmIdentifier
   serialNumber          CertificateSerialNumber
   validity              AttCertValidityPeriod
   attributes            SEQUENCE OF Attribute
   issuerUniqueID        UniqueIdentifier OPTIONAL
}
```

Si nota, con facilità, come il campo degli attributi può contenere più informazioni in quanto è definito come "sequenza".
Le principali informazioni contenute in un certificato di attributo sono, generalmente, quelle mostrate nel seguente esempio:

```
AttributeCertificateInfo ::= SEQUENCE
{
   version          v1,
   owner            c=IT, o=Policlinico, cn=Rossi Mario
   issuer           c=IT, o=Policlinico, ou=Direzione
                          Personale,
                    cn= Ufficio Ruoli

   signature        .....
   serialNumber     234
   validity         .....
   attributes       title=Radiologo
   issuerUniqueID   22341
   extensions       .....
}
```

Come si vede Mario Rossi è un radiologo del Policlinico e l'Ufficio Ruoli della Direzione del Personale gli ha attribuito questa funzione.
In un caso più generale, la struttura che attribuisce i ruoli, pur operando in modo analogo al certificatore non deve essere necessariamente una terza parte fidata. Nella realtà, anzi, risulta più efficace che questo ruolo sia svolto da un'organizzazione che conosce profondamente i ruoli e le loro variazioni. Nel mondo cartaceo, l'attribuzione delle funzioni viene spesso richiesta ai notai, quindi, sia questi ultimi, che gli ordini professionali si stanno attrezzando per operare nel mondo digitale.

7. LE BUSTE CRITTOGRAFICHE

Una volta stabilita la necessità di un certificato di attributo, si deve stabilire come e se la busta **crittografica**, che contiene le informazioni firmate, deve evolvere per contenere questa informazione. Il certificato di attributo viene collegato al certificato di chiave pubblica attraverso il numero di serie di quest'ultimo. Deve essere poi possibile utilizzare nei processi operativi il certificato di chiave pubblica congiuntamente con quello di attributo. Anche in questo caso, si deve fare affidamento all'evoluzione degli standard senza poter ancora disporre di prodotti di mercato adeguatamente diffusi.

L'operazione di **crittografia** consente di trasformare un messaggio (testo in chiaro) in un testo in cifra (crittogramma) mediante l'utilizzo di funzioni matematiche specifiche. La conoscenza di un testo cifrato è, dunque, impossibile per soggetti diversi dal mittente e dal destinatario.

Attualmente, la busta crittografica, ovvero quella struttura dati mediante il formato della quale si aggregano il documento originale, la firma digitale del sottoscrittore e il certificato di chiave pubblica del medesimo, è ampiamente disponibile secondo quanto descritto dalla specifica pubblica PKCS#7 (*Public Key Cryptographic System*, numero 7). Tale standard, nella sua versione 1.5 è stato anche pubblicato come RFC 2315 [10]. Dato che è consentito inserire nella busta crittografica più certificati, potrebbe sembrare ovvio includere, in essa, sia certificati di chiave pubblica che certificati di attributo. La realizzazione pratica non risulta efficace in quanto

nella busta non sarebbe facile distinguere i differenti tipi di certificato, in quanto non sono identificati da riferimenti logici specifici. L'evoluzione dello standard RFC 2315 ha portato alla pubblicazione del nuovo standard RFC 2630 [7] intitolato *Cryptographic Message Syntax* (CMS). Utilizzando questo standard, per produrre buste crittografiche relative a dati firmati (*SignedData*), si ha un documento strutturato, secondo la rappresentazione ASN.1, nel seguente modo:

```
SignedData ::= SEQUENCE
{
   version              CMSVersion,
   digestAlgorithms     DigestAlgorithmIdentifiers,
   encapContentInfo     EncapsulatedContentInfo
   certificates         [0] IMPLICIT CertificateSet
                            OPTIONAL,
   crls                 [1] IMPLICIT CertificateRevoca-
                            tionLists
OPTIONAL,
   signerInfos          SignerInfos
}
```

La struttura mostrata, pur molto simile a quella dell'RFC 2315, presenta una fondamentale differenza.
L'RFC 2630 introduce l'innovativa definizione di *CertificateSet* che consente la gestione dei certificati di attributo. Essi sono addirittura esplicitamente referenziati, come appare evidente dalla seguente rappresentazione ASN.1 estratta dallo standard:

```
CertificateSet::== SET OF CertificateChoices

CertificateChoices::= CHOICE
{
   certificate                Certificate,
 -- See X.509
   extendedCertificate        [0] IMPLICIT
                              ExtendedCertificate,
 -- Obsolete
   attrCert                   [1] IMPLICIT
                              AttributeCertificate,
 -- See X.509 and X9.57
}
```

Attualmente tali strutture, oltre a non essere diffuse nei prodotti di mercato, non sono contemplate dalla normativa vigente. In particolare l'RFC 2630 non è previsto dalla circolare pubblicata a cura dell'Autorità per l'informatica nella pubblica amministrazione con il codice di identificativo AIPA/CR/24 (Autorità per l'Informatica nella Pubblica Amministrazione/Circolare numero 24) relativa all'interoperabilità delle firme digitali rilasciate con modalità tali da poter essere considerate equivalenti a quelle autografe. Il processo di adeguamento di questa norma, sicuramente terrà conto di questa esigenza.

8. LA FIRMA DIGITALE E L'XML

XML si è ormai affermato come valido strumento per lo scambio di dati in modo efficace e flessibile. Attraverso XML è possibile anche costruire delle applicazioni come quella che interessa in questo contesto ovvero *XML-Signature*, nella quale utilizzando XML si specifica un formato per la firma digitale. Con tale specifica, è possibile sottoscrivere digitalmente qualsiasi contenuto, compresi documenti XML stessi. Come descritto nell'RFC 2807 [12], le firme XML sono generate calcolando l'impronta della forma canonica di un *manifest* di firma. La forma canonica è una rappresentazione, normalizzata per effettuare l'operazione su un insieme di oggetti anche non omogenei tra di loro. Il manifest è un insieme di riferimenti agli oggetti che devono essere sottoscritti. Secondo questo schema, la firma può essere applicata contemporaneamente al contenuto di una o più risorse. Su ciascuna risorsa viene calcolata l'impronta. Le impronte e i puntatori alle risorse (in forma di *Uniform Resource Identifier* che come è noto può, per esempio, essere rappresentato da un indirizzo web o un indirizzo di posta elettronica) sono inseriti insieme ad informazioni contestuali nella struttura, già citata, denominata manifest. A questo punto, la sintassi della firma XML associa il contenuto delle risorse presenti nel manifest a una chiave (e a un algoritmo) crittografica utilizzata per la **cifratura** (si veda Box pag. 39) Con il termine *risorse* si indicano gli oggetti ai quali si vuole applicare la firma digitale. Utilizzando la filosofia XML è possibile firmare risorse interne o esterne a un contesto, documenti XML, parti di esso e anche generici oggetti binari (spesso chiamati BLOB, *Binary Large OBject*).

Il processo di codifica viene indicato come **cifratura**. Il procedimento inverso, che permette di ottenere il testo in chiaro, si chiama *decifratura*. Questi processi sono collegati all'uso di una chiave (una sequenza arbitrariamente lunga di caratteri), che fa in modo che la decifratura di un messaggio possa essere eseguita solo conoscendo l'apposita chiave. In generale, la sicurezza non è garantita dalla segretezza delle funzioni matematiche utilizzate, ma dalla difficoltà (in termini computazionali) di effettuare operazioni di attacco all'algoritmo senza conoscere la chiave. Se le chiavi utilizzate per cifrare/decifrare sono uguali tra mittente e destinatario si parla di *algoritmi simmetrici*. Quando le chiavi sono due si parla di *algoritmi asimmetrici*.

La figura 4 sintetizza quanto descritto.
Mediante la gestione delle innumerevoli possibilità offerte da XML è possibile ottenere gli stessi risultati che si ottengono con le buste crittografiche PKCS#7 e CMS. Particolarmente interessante è la possibilità di sottoscrizione di parti di un documento. Come si può facilmente dedurre, la firma digitale in ambiente XML, proprio perché offre numerose possibilità di realizzazione, risulta complessa. Il processo di standardizzazione sta proseguendo in modo rapido, anche se non ha completato tutto il suo percorso. Comunque già si possono prendere a riferimento l'RFC 3275 [3] e l'RFC 3076 [2]. Per superare PKCS#7 (RFC 2315) e CMS (RFC 2630), l'ETSI ha supportato lo sviluppo dello standard XML, *Advanced Electronic Signatures* [5]. In ogni caso, al momento, i prodotti per la sottoscrizione digitale utilizzano PKCS#7 e sembra più probabile un'evoluzione verso le buste crittografiche RFC 2630 prima di una migrazione verso XML. Tale evento è presumibile che avvenga solo se ci saranno significative crescite nel mercato della firma digitale.

9. IL PROBLEMA DELL'INTEROPERABILITÀ

Si è cominciato a discutere del problema dell'interoperabilità nel gennaio 2000, per porre rimedio a una situazione per certi versi sorprendente. Nonostante otto certificatori fossero a norma di legge per quanto

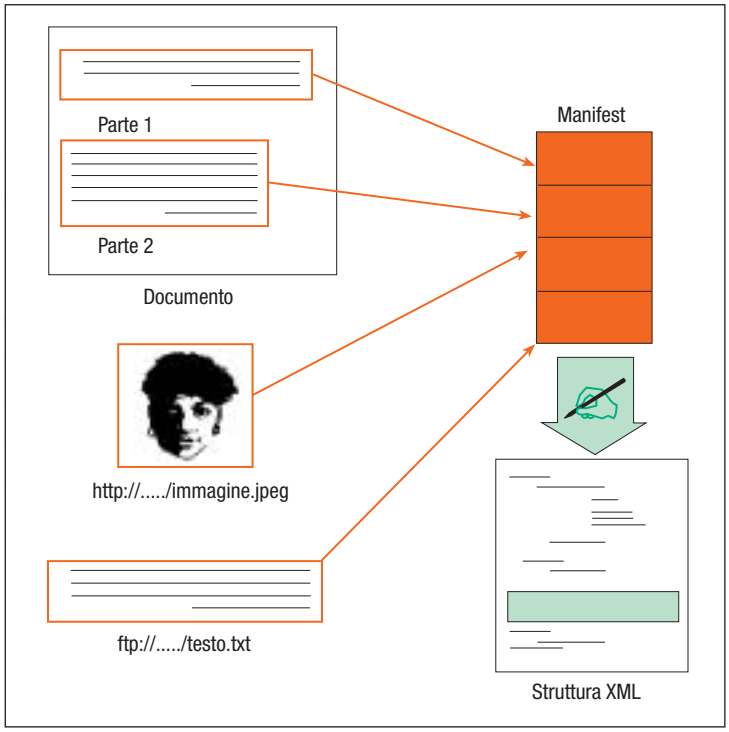

FIGURA 4
Esempio di signature XML

concerne l'emissione di certificati di chiave pubblica, nel momento in cui venivano utilizzati per la produzione di una firma digitale equivalente ad una autografa, i prodotti di verifica delle firme il più delle volte non riuscivano nel loro scopo. In altri casi, alcuni insiemi di dati, pur aderenti agli standard, erano soggetti ad interpretazioni differenti e quindi il risultato che si otteneva non era univoco.
Il processo di evoluzione degli standard, accelerato dalle necessità di aderire alle esigenze della Direttiva Europea, porterà ad adeguare anche questa legislazione minore ma indispensabile per il corretto funzionamento del sistema.
Si veda, dunque, sulla base di quanto descritto precedentemente, in che modo il legislatore può prendere atto dei nuovi standard e modificare in tal senso le vecchie regole di interoperabilità.
I problemi che la circolare 24 dell'AIPA ha risolto hanno riguardato le informazioni all'interno del certificato, comprese le estensioni, la struttura delle liste di revoca e sospensione e la rappresentazione delle informazioni nelle buste crittografiche. Seguendo il principio che l'imposizione di regole non condivise dai certificatori non avrebbe

portato risultati, si è preso atto delle tecnologie disponibili presso di essi. Questo ha definito, anche se la legislazione tecnica vigente in quel periodo (D.P.C.M. 8 febbraio 1999[3]) consentiva altre scelte, come algoritmo di generazione e verifica delle firme l'RSA (*Rivest, Shamir, Adleman*) e come funzione per il calcolo dell'impronta la SHA-1 (Secure Hashing Algorithm 1). Come busta crittografica è stata scelta la PKCS#7 che, nella sua versione 1.5, è regolata dall' RFC 2315. Altre scelte sono state fatte per il collocamento del codice fiscale all'interno del certificato e per rappresentare nomi molto grandi o contenenti caratteri speciali come le dieresi e gli accenti slavi o spagnoli. In particolare, il codice fiscale viene posto nel *Common Name* insieme al nome e al cognome del titolare. Le altre informazioni sono state inserite in un oggetto particolare, fino a quel momento poco utilizzato, anche se standard, denominato description. Di seguito, viene mostrato un esempio di campi *Common Name* e *Description* conformi alle regole di interoperabilità.

CommonName =
Manca/Giovanni/MNCGNN57D15H501G/AA4561

Description = "C= <cognome esteso>"/N="<nome esteso>"/D="<data di nascita>"/R="<ruolo titolare>"

Le parentesi acute sono dei delimitatori grafici. Il ruolo è opzionale e ha rilevanza per l'applicazione e quindi non ha formato predefinito. Il numero AA4561 è un esempio di identificativo unico del titolare presso il certificatore e viene inserito perché previsto dalla legislazione italiana.
Le scelte presentate sono state effettuate perché non esisteva uno standard a supporto (il testo della circolare infatti è stato approvato alla fine di marzo 2000). Nel gennaio 2001, lo standard è arrivato ed è il già citato RFC 3039, con cui è possibile strutturare in modo standard i dati. In questo documento vengono introdotti i *Subject Directory attributes* ed in questi troviamo il *title* che può prendere il posto del ruolo e *dateOfBirth* che conterrà la data di nascita.
Nei campi che, secondo questo standard, compongono *subject* viene definito il *serial number*. Come affermato, nello standard stesso questo attributo deve essere usato per differenziare soggetti che non lo possono essere con gli altri campi disponibili. In particolare, recita sempre lo standard, si può utilizzare un numero o un codice assegnati dal certificatore, dal governo o altra autorità pubblica. Il certificatore, comunque, deve assumersi la responsabilità di assicurare che il serial number sia sufficiente a risolvere qualsiasi collisione sul nome del titolare.
Quanto esposto rende evidente che in questo campo attributo può essere inserito il codice fiscale. Tale codice è, infatti, assegnato da un organismo governativo ed è univoco.
Questo nuovo approccio sarà applicato, ancora una volta con il consenso dei certificatori, non appena sarà chiaro l'approccio della Commissione Europea sugli standard in base a quanto stabilito nella Direttiva 1999/93/CE. Anche con l'RFC 3039 non viene risolto il problema dei nomi con caratteri speciali anche se, per esempio in Germania, viene utilizzato l'approccio dell'allitterazione. L'identificativo unico del titolare presso il certificatore deve trovare una collocazione al di fuori del *Common Name*, ma questo non sarà un problema visto che esistono alcuni campi candidati tra le estensioni X.509 del certificato.

10. CONCLUSIONI

In base a quanto esposto, si può affermare che la firma digitale applicata a un documento informatico garantisce proprietà particolari che le firme tradizionali non hanno. Tali proprietà derivano direttamente dal fatto che la sottoscrizione digitale è il risultato di un calcolo matematico effettuato sul contenuto binario del documento cui la firma si riferisce.

[3] D.P.C.M. 8 febbraio 1999. Regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validità, anche temporale, dei documenti informatici ai sensi dell'art. 3, comma 1, del decreto del Presidente della Repubblica 10 novembre 1997, n 513.

Di seguito, vengono elencate alcune di queste proprietà.

- La firma digitale è differente tra un documento e un altro. Essa è strettamente connessa al documento sul quale viene calcolata. Questo significa che non è possibile imitare o falsificare una firma digitale, né duplicarla su un documento differente pur prelevandola da un documento valido.
- La firma digitale non può essere apposta su un documento "in bianco". Essa è relativa sempre a un contenuto: la mancanza del documento non consentirebbe di calcolare l'impronta e quindi la firma.
- La firma digitale consente di rilevare modifiche al testo originale ovvero riesce a mettere in evidenza anche minime differenze tra il testo originale, sul quale è stata calcolata la firma, e quello modificato.
- La validità di una firma digitale può essere verificata in modo certo e ripetibile: derivando da un processo matematico noto non vi sono margini di incertezza nella verifica.

La firma digitale, come si è osservato, è ancora in fase evolutiva. Il legislatore italiano è stato il primo a introdurla e a regolamentarla, conferendole lo stesso valore legale della firma autografa. Con l'accettazione della Direttiva Europea 1999/93/CE, viene ampliato lo spazio di azione dello strumento. Tutte queste modifiche hanno portato a un primo consolidamento organizzativo e tecnologico che consente a 13 aziende italiane (più una struttura della pubblica amministrazione) di operare come certificatori. Per proseguire il cammino il mercato dovrà aggiornare le tecnologie utilizzate soprattutto per essere in linea con le evoluzioni europee e mondiali.

Resta il fatto che la firma digitale è una realtà e numerose strutture pubbliche e private iniziano ad utilizzarla, per ottimizzare i propri processi organizzativi e operativi con l'ambizioso obiettivo di riuscire, il più possibile, a lavorare in un ufficio moderno e *paperless*.

Bibliografia

[1] Adams, Cain, Pinkas, Zuccherato: *Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)*. RFC 3161, August 2001.

[2] Boyer, Canonical XML Version 1.0, RFC 3076, March 2001.

[3] Eastlake, Reagle, Solo: *(Extensible Markup Language) XML-Signature Syntax and Processing*. RFC 3275, March 2002.

[4] ETSI TS 101 733, Electronic Signature Formats.

[5] ETSI TS 101 903, XML Advanced Electronic Signatures (XAdES).

[6] ETSI TS 101 861, Time Stamping Profile.

[7] Housley: *Cryptographic Message Syntax*. RFC 2630, June 1999.

[8] Housley, Ford, Polk, Solo: *Internet X.509 Public Key Infrastructure Certificate and CRL Profile*. RFC 2459, January 1999.

[9] ITU-T Recommendation X.509 (1997 E): Information Technology – *Open System Interconnection – The Directory: Authentication Framework*. June 1997.

[10] Kaliski, PKCS#7: *Cryptographic Message Syntax* – Version 1.5, RFC 2315, March 1998.

[11] Myers, Ankney, Malpani, Galperin, Adams: *Internet X.509 Public Key Infrastructure Online Certificate Status Protocol – OCSP*. RFC 2560, June 1999.

[12] Reagle: *XML Signature Requirements*. RFC 2807, July 2000

GIOVANNI MANCA laureato in ingegneria, si è occupato di sistemi distribuiti, sicurezza e servizi telematici in ambito fiscale. Successivamente, nella pubblica amministrazione, ha sviluppato ulteriori esperienze nella sicurezza. Attualmente è dirigente nell'Autorità per l'informatica nella pubblica amministrazione con la responsabilità tecnica della vigilanza sui certificatori di firma digitale.
e-mail: manca11@tiscali.it