LA FIRMA DIGITALE

Estratto dal sito web del *Centro Nazionale per l'Informatica nella Pubblica Amministrazione* (CNIPA)[1]

[1] http://www.cnipa.gov.it/site/it-IT/Attivit%c3%a0/Firma_digitale/

SOMMARIO

1. INTRODUZIONE

La Firma Digitale è il risultato di una procedura informatica che garantisce l'autenticità e l'integrità di messaggi e documenti scambiati e archiviati con mezzi informatici, al pari di quanto svolto dalla firma autografa per i documenti tradizionali. La differenza tra firma autografa e firma digitale è che la prima è legata alla caratteristica fisica della persona che appone la firma, vale a dire la grafia, mentre la seconda al possesso di uno strumento informatico e di un PIN di abilitazione, da parte del firmatario.

1.1. CHE COSA E'?

La firma digitale è il risultato di una procedura informatica (validazione) che consente al sottoscrittore di rendere manifesta l' autenticità del documento informatico ed al destinatario di verificarne la provenienza e l'integrità. In sostanza i requisiti assolti sono:

- Autenticità: con un documento firmato digitalmente si può essere certi dell' identità del sottoscrittore;
- Integrità: sicurezza che il documento informatico non è stato modificato dopo la sua sottoscrizione;
- Non ripudio: il documento informatico sottoscritto con firma digitale, ha piena validità legale e non può essere ripudiato dal sottoscrittore.

1.2. COME FUNZIONA

Per generare una firma digitale è necessario utilizzare una coppia di chiavi digitali asimmetriche, attribuite in maniera univoca ad un soggetto detto Titolare della coppia di chiavi. La prima, chiave privata destinata ad essere conosciuta solo dal Titolare, è utilizzata per la generazione della firma digitale da apporre al documento, la seconda, chiave da rendere pubblica, viene utilizzata per verificare l'autenticità della firma. Caratteristica di tale metodo, detto crittografia a doppia chiave, è che, firmato il documento con la chiave privata, la firma può essere verificata con successo esclusivamente con la corrispondente chiave pubblica. La sicurezza è garantita dalla impossibilità di ricostruire la chiave privata (segreta) a partire da quella pubblica, anche se le due chiavi sono univocamente collegate.

La **firma digitale** costituisce uno dei cardini del processo di e-government. Per quanto riguarda la PA, l'obiettivo, abilitante allo sviluppo dei servizi on line, si sviluppa su tre principali linee di intervento:

- diffusione della firma digitale all'interno delle amministrazioni, con distribuzione a dirigenti e funzionari con potere di firma, e relativa formazione;
- intervento su applicazioni e servizi, per renderli accessibili in sicurezza tramite la firma digitale;
- iniziative specifiche di stimolo all'utilizzo della firma da parte di gruppi specifici di utenti esterni all'amministrazione.

Nell'ambito delle attività come certificatore, sono circa 50 le amministrazioni coinvolte, mentre i certificati di firma digitale emessi al primo semestre del 2006 sono circa 40 mila.

1.3. IL QUADRO NORMATIVO

L'Italia si è posta all'avanguardia nell'uso legale della firma digitale, essendo il primo paese ad avere attribuito piena validità giuridica ai documenti elettronici. Fin dal lontano 1997 l'articolo 15 della L. 59/97 stabilisce infatti che "*gli atti, dati e documenti formati dalla Pubblica amministrazione e dai privati con strumenti informatici o telematici, i contratti stipulati nelle*

medesime forme, nonché la loro archiviazione e trasmissione con strumenti informatici, sono validi e rilevanti a tutti gli effetti di legge". In base a tale norma, un documento siglato con firma digitale ha lo stesso valore del suo omologo cartaceo. Le implicazioni sono notevoli anche per il settore privato: dalla validità dei contratti on line alla possibilità di emettere fatture commerciali o ordini di acquisto. La normativa pre-direttiva sulla firma digitale, la firma elettronica e la conservazione del documento elettronico, prevedeva un'unica tipologia di certificato, di certificatore e di firma digitale. Con il recepimento della Direttiva 1999/93/CE e l'emanazione del D. lgs n. 10/02 e del DPR 7 aprile 2003 n. 137, il quadro normativo di riferimento ha subito una profonda trasformazione; in particolare, l'articolo 6 del decreto di recepimento ha modificato l'articolo 10 del DPR n. 445/00, stabilendo che il documento informatico (da intendersi, ai sensi del Testo unico del 2000, come la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti e, quindi, non recante alcuna sottoscrizione elettronica), ha l'efficacia probatoria prevista dall'articolo 2712 del codice civile. Con l'entrata in vigore del Codice dell'amministrazione digitale (gennaio 2006), attraverso il Decreto legislativo 7 marzo 2005, n. 82, il valore probatorio del documento informatico ha subito una ulteriore modifica, difatti con il comma 2 dell'articolo 21, come modificato dal D.Lgs. 4 aprile 2006, n. 159, è stabilito che "*Il documento informatico, sottoscritto con firma digitale o con un altro tipo di firma elettronica qualificata, ha l'efficacia prevista dall'articolo 2702 del codice civile. L'utilizzo del dispositivo di firma si presume riconducibile al titolare, salvo che questi dia prova contraria.* ". Il citato decreto legislativo rivede anche le tipologie di firma elettronica previste contemplando tre tipologie di firma:

- **firma elettronica**: l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica.
- **firma elettronica qualificata**: la firma elettronica ottenuta attraverso una procedura informatica che garantisce la connessione univoca al firmatario, creata con mezzi sui quali il firmatario può conservare un controllo esclusivo e collegata ai dati ai quali si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati, che sia basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma.
- **firma digitale**: un particolare tipo di firma elettronica qualificata basata su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici.

Le norme continuano a contemplare due tipologie di certificato (qualificato e non qualificato) e tre di certificatore (che rilascia certificati qualificati: accreditato o notificato; che rilascia certificati non qualificati). Istanze e dichiarazioni inviate per via telematica da e verso la PA sono valide se sottoscritte mediante firma digitale basata su un certificato qualificato rilasciato da un certificatore accreditato e generata mediante un dispositivo sicuro per la creazione di firme elettroniche.

DPCM 12 ottobre 2007: l'autodichiarazione dei certificatori

La Presidenza del Consiglio dei Ministri ha emanato - su proposta del CNIPA – un provvedimento che consente ai certificatori accreditati di autodichiarare la conformità dei dispositivi sicuri per la generazione della firma digitale con procedure automatiche, per un periodo di 24 mesi dall'entrata in vigore del DPCM. Ciò consentirà di agevolare lo sviluppo di sistemi di conservazione documentale, di fatturazione elettronica o di gestione delle informazioni sanitarie. Il decreto è stato pubblicato sulla Gazzetta Ufficiale n. 13 del 16 gennaio 2008.

1.4. IL CERTIFICATORE

Per garantire l'identità dei soggetti che utilizzano la firma digitale e per fornire protezione nei confronti di possibili danni derivanti da un esercizio non adeguato delle attività di certificazione, le norme vigenti in materia richiedono che il soggetto certificatore sia in possesso di particolari requisiti tecnici, organizzativi e societari. Tali soggetti che rilasciano certificati qualificati si distinguono, come precedentemente detto, in certificatori accreditati e notificati. La differenza sostanziale fra le due tipologie è che il certificatore accreditato si sottopone volontariamente ad apposita preventiva istruttoria atta a verificarne il possesso dei requisiti di legge; il certificatore notificato inizia ad operare contastualmente alla comunicazione di inizio attività al CNIPA. Entrambe le tipologie sono soggette ad attività di vigilanza. Documenti informatici sottoscritti con firma digitale possono essere scambiati con le pubbliche amministrazioni solo se le firme digitali sono basate su certificati qualificati emessi da certificatori qualificati. Al termine dell'istruttoria, se positivamente conclusasi, i soggetti che intendono ottenere il riconoscimento dello status di "certificatore accreditato", sono inseriti in apposito elenco pubblico, consultabile telematicamente, predisposto, tenuto ed aggiornato a cura del CNIPA.

1.5. LE REGOLE TECNICHE

Con la pubblicazione del DPCM del 13 gennaio 2004 (G. U. 27 aprile 2004, n. 98) sono state emanate le regole tecniche per la formazione, trasmissione, conservazione, duplicazione, riproduzione e validazione, anche temporale, dei documenti informatici. Il provvedimento disciplina la formazione della documentazione amministrativa tramite il supporto informatico, con particolare attenzione per la generazione, apposizione e verifica delle firme digitali. Viene quindi portato a compimento il recepimento della Direttiva europea 1999/93/CE. Questo provvedimento delinea i requisiti tecnici ed organizzativi che i soggetti, pubblici e privati, che intendono emettere certificati qualificati devono possedere. Prescrive inoltre le caratteristiche peculiari che devono essere possedute dai soggetti che intendono ottenere il riconoscimento del possesso dei requisiti del livello più elevato, in termini di qualità e di sicurezza. Con l'entrata in vigore di queste regole tecniche viene abrogato il DPCM 8 febbraio 1999.

Sulla gazzetta ufficiale n. 51 del 3 marzo 2005 sono state infine pubblicate le "*Regole per il riconoscimento e la verifica del documento informatico*", attraverso la Deliberazione CNIPA n.4 del 17 febbraio 2005, emanate ai sensi del comma 4 dell'articolo 40 del DPCM 13 gennaio 2004.

Queste ulteriori regole sono fondamentali per garantire l'interoperabilità della firma digitale, cioè la possibilità di verificare qualunque firma digitale con qualsiasi software di verifica purché conformi alle medesime regole. Per tale ragione il rispetto delle stesse è obbligatorio da parte dei certificatori accreditati.

1.6. L'UTILIZZO DELLA FIRMA DIGITALE

Il CNIPA ha predisposto un documento dal titolo "Le Linee guida per l'utilizzo della firma digitale" concepito per supportare gli utenti e le aziende circa l'utilizzo della firma digitale e organizzato in modo tale che gli interessati possano effettuare la sua consultazione in modo mirato, seguendo un percorso specifico secondo le proprie esigenze. In tal modo, sarà possibile comprendere dove acquistare la firma digitale, come utilizzarla e soprattutto come verificare la sua validità legale mediante gli strumenti gratuiti segnalati dal CNIPA.

2. LA CERTIFICAZIONE

2.1. Il CERTIFICATO PER LE CHIAVI DIGITALI

Il certificato è un documento elettronico, contenente informazioni relative al titolare e la chiave pubblica di firma del Titolare. E' il risultato di una apposita procedura di certificazione che garantisce la corrispondenza biunivoca tra una chiave pubblica ed il soggetto a cui essa appartiene.

2.2. L'ENTE CERTIFICATORE

Affinché i soggetti possano riporre completa fiducia nei certificati digitali e nei dati in essi contenuti, occorre che una "terza parte fidata" - il Certificatore - garantisca l'affidabilità dei dati contenuti nel certificato, occupandosi quindi del suo rilascio e pubblicazione su un apposito registro accessibile online.

Le principali attività del Certificatore sono le seguenti:

- verificare ed attestare l'identità del richiedente;
- stabilire il termine di scadenza dei certificati, ed il periodo di validità delle chiavi in funzione della loro "robustezza " e degli usi per i quali sono impiegate;
- emettere e pubblicare il certificato, in un archivio pubblico gestito dallo stesso Certificatore;
- revocare o sospendere i certificati.

I certificatori, per l'attuale normativa, sono accreditati presso il Centro nazionale per l'informatica nella pubblica amministrazione ed iscritti in un apposito elenco.

2.3. COME SI OTTIENE IL CERTIFICATO

Per la legge italiana il Certificatore deve provvedere a verificare l' identità del soggetto che richiede il certificato attraverso procedure appositamente definite.

- Il richiedente deve fornire all'Ente di Certificazione la documentazione utile per accertare la sua identità;
- Il Certificatore, a sua volta, fornisce al richiedente un codice identificativo univoco;
- A seguito della generazione delle chiavi asimmetriche, quella privata da mantenere segreta e quella pubblica da rendere disponibile per la verifica, quest'ultima chiave viene inviata al Certificatore per l'emissione del certificato;
- Il Certificatore, infine, genera e pubblica il certificato che contiene i dati del Titolare e la sua chiave pubblica che i destinatari utilizzano per la verifica della firma.

3. IL DOCUMENTO INFORMATICO

3.1. DEFINIZIONE DI DOCUMENTO INFORMATICO

La legge n.59 del 1997 - articolo 15 – stabilisce che *"gli atti, dati e documenti, formati dalla pubblica amministrazione e dai privati con strumenti informatici o telematici, i contratti stipulati nelle medesime forme, nonché la loro archiviazione e trasmissione con strumenti informatici, sono validi e rilevanti a tutti gli effetti di legge"*.

Il DPR 445 del 28 dicembre 2000 ha fissato i requisiti che il documento informatico inteso come "la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti" deve rispettare per avere pieno valore legale.

3.2. FORMAZIONE DEL DOCUMENTO INFORMATICO

Con il termine documento cartaceo si intende sia il supporto che il contenuto che in esso viene rappresentato; tramite la sottoscrizione autografa viene identificata la persona che ne assume la paternità, se ne sancisce l'autenticità ed il sottoscrittore stesso fa propri i contenuti rappresentati nel documento. Un documento informatico può essere invece modificato o riprodotto infinite volte, ottenendo copie assolutamente identiche all'originale. Il contenuto è svincolato dal supporto. Per restituire al documento informatico gli stessi requisiti assolti dalla sottoscrizione autografa di un documento cartaceo occorre, quindi, un tipo di autenticazione come la firma digitale, che attribuisca al contenuto del documento informatico piena validità legale.

3.3. FIRMA DIGITALE DI UN DOCUMENTO INFORMATICO

La firma digitale garantisce, nei confronti dei documenti informatici, la presenza degli stessi requisiti che la firma autografa garantisce nei confronti dei documenti cartacei. Grazie alla tecnologia della firma digitale e per mezzo del sistema a "chiavi pubbliche", il destinatario del documento ha la garanzia di disporre di un testo integro e proveniente da una fonte ben precisa. La sequenza di simboli che chiamiamo firma digitale, generata da algoritmi matematici, si riferisce univocamente ad i contenuti di un preciso documento, la modifica anche di un solo carattere sarebbe immediatamente rilevata al momento della verifica.

ATTENZIONE: *E' perciò altamente sconsigliabile la sottoscrizione digitale di documenti contenente elementi dinamicamente variabili. Pertanto è preferibile utilizzare, per i documenti da firmare digitalmente, formati il più possibile statici (rtf, pdf, text, tiff, etc.). Gli elementi dinamici (macro, funzioni, campi variabili, script, etc.), che possono essere inseriti in alcuni tipi di documento informatico (.doc, .xls, etc.), possono provocare la visualizzazione di contenuti differenti al momento della sottoscrizione e della successiva verifica.*

3.4. CIFRATURA

La distribuzione telematica dei documenti digitali e la diffusione delle comunicazioni in rete, ha portato alla ribalta le problematiche relative alla riservatezza dei documenti trasmessi.

Il processo utilizzato per garantire la riservatezza dei documenti informatici, si basa sempre sulla crittografia asimmetrica, ma la normativa italiana prevede l'uso di una coppia di chiavi distinta da quella usata per la firma.

La cifratura è un processo reversibile in grado di codificare un documento e renderlo illeggibile a terze persone non autorizzate sia in fase di trasmissione che di archiviazione. L'operazione inversa è detta decifratura.

3.5. MARCATURA TEMPORALE

La procedura di marcatura temporale serve ad attestare l'esistenza di un documento informatico rispetto ad una data certa; è inoltre essenziale per evitare che documenti redatti utilizzando certificati revocati o scaduti vengano utilizzati a scopi fraudolenti.

Tale procedura prevede la generazione di una marca temporale, da parte di un sistema dedicato, che indica l'ora e il giorno certi in per cui il documento informatico è stata emessa la marca che ne attesta l' esistenza.

4. LA CRITTOGRAFIA

4.1. COSA E' LA CRITTOGRAFIA?

Vista la rilevanza giuridica del documento informatico, occorre poter individuare in maniera semplice il suo sottoscrittore e poter rilevare immediatamente se il documento è integro oppure è stato alterato dopo la sua sottoscrizione. A tale scopo riveste particolare importanza la crittografia , tecnica per rendere intellegibili i documenti a chi non dispone della relativa chiave e dell'algoritmo necessario. La crittografia può essere:

- **simmetrica**, nel caso in cui ogni titolare dispone di una chiave per la firma dei documenti; la stessa chiave deve essere a conoscenza del destinatario che la utilizza per la verifica;
- **asimmetrica**, ogni titolare dispone di una coppia di chiavi, una privata , da mantenere segreta, utilizzata per la sottoscrizione dei documenti, l'altra da rendere pubblica e da usare per la verifica.

La normativa vigente in Italia, prevede l'uso della crittografia asimmetrica per la sottoscrizione dei documenti informatici.

4.2. COS' E' UNA COPPIA DI CHIAVI ASIMMETRICHE?

E' una coppia di chiavi crittografiche, una privata ed una pubblica, da utilizzarsi per la sottoscrizione dei documenti informatici. Pur essendo univocamente correlate, dalla chiave pubblica non è possibile risalire a quella privata che deve essere custodita in maniera riservata dal Titolare.

Chiave privata: elemento della coppia di chiavi asimmetriche, destinato ad essere conosciuto soltanto dal soggetto Titolare, mediante il quale si appone la firma digitale sul documento informatico.

Chiave pubblica: elemento della coppia di chiavi asimmetriche destinato ad essere reso pubblico, con il quale si verifica la firma digitale apposta sul documento informatico dal Titolare delle chiavi asimmetriche.

4.3. COS'E' UN CERTIFICATO PER CHIAVI DI FIRMA

Il certificato è un documento elettronico contenente informazioni relative al Titolare e la sua chiave pubblica; è firmato dal Certificatore con la propria chiave privata utilizzata solo per questo scopo.

Il Certificatore emette il certificato e lo sottoscrive apponendo la sua firma digitale mediante la chiave privata di certificazione. Chiunque desideri assicurarsi dell'autenticità e dell'integrità dei

dati in esso contenuti, può verificarlo utilizzando la chiave pubblica del certificatore stesso.

Il certificato viene inviato al richiedente che, nel rispetto della normativa vigente, lo allega, per la verifica, al documento informatico ed alla relativa firma digitale.

4.4. L'IMPRONTA UNIVOCA DEL DOCUMENTO -HASHING –

La prima operazione per generare una firma digitale è l'estrazione, dal documento originario, della cosiddetta "impronta digitale", cioè una stringa di dati, ottenuta con una funzione matematica, detta "hash", irreversibile (non è possibile, a partire dall' impronta, risalire al documento originario). Tale funzione sintetizza il testo in modo univoco (a due testi che differiscono anche per un solo carattere, corrispondono due impronte diverse).

4.5. FIRMA DIGITALE COME OPERAZIONE DI CRITTOGRAFIA

La generazione della firma consiste nella cifratura con la chiave privata dell'impronta precedentemente generata. In questo modo la firma risulta legata:

- attraverso la chiave pubblica - univocamente correlata alla chiave privata utilizzata per la firma del documento informatico - al soggetto sottoscrittore
- tramite l'impronta al testo sottoscritto

La firma digitale, vale a dire l'impronta cifrata, viene allegata al documento in chiaro insieme al certificato da cui è possibile ottenere la chiave pubblica per la verifica.

4.6. COME SI GENERA LA FIRMA DIGITALE

Le principali fasi del processo di firma digitale sono:

1. Viene prodotta l'impronta del documento da firmare, utilizzando la funzione di hash;
2. Si genera la firma digitale cifrando, con la chiave privata del sottoscrittore, l'impronta precedentemente prodotta;
3. Viene creata la "busta elettronica", contenente il documento informatico, la firma digitale ed il certificato della chiave pubblica; il "pacchetto" così formato viene trasmesso al destinatario.

4.7. COME SI VERIFICA LA FIRMA DIGITALE

Il processo di verifica consiste nei seguenti fasi fondamentali:

1. la decifratura della firma digitale con la chiave pubblica del mittente, contenuta nel certificato allegato; si ottiene così l'impronta in precedenza generata dal mittente del documento - l'esito positivo di questa operazione assicura l'autenticità dell'origine dei dati;
2. la creazione, a partire dal documento informatico ricevuto, dell'impronta univoca, utilizzando la stessa funzione di hash precedentemente utilizzata dal mittente;
3. il confronto tra le due impronte, quella ricevuta in maniera cifrata - e decifrata utilizzando la chiave pubblica - e quella calcolata utilizzando la funzione di hash, dà la garanzia che il documento non è stato alterato.

5. CONTESTO TECNOLOGICO

5.1. L'INFRASTRUTTURA A CHIAVE PUBBLICA

E' un insieme di apparati, regole di sicurezza, procedure operative e servizi che rendono possibile la gestione affidabile ed efficiente di applicazioni per la firma digitale, l'autenticazione, la protezione della riservatezza e la marcatura temporale dei documenti informatici.

Si basa sulla crittografia asimmetrica a chiave pubblica e svolge le seguenti funzioni principali:

- generazione e distribuzione di coppie di chiavi digitali;
- verifica dell'identità dei richiedenti i certificati;
- emissione e pubblicazione dei certificati;
- gestione del ciclo di vita dei certificati (sospensione, revoca, rinnovo)

5.2. CUSTODIA DELLA CHIAVE PRIVATA E DIFFUSIONE DELLA CHIAVE PUBBLICA

La chiave privata utilizzata per la firma dei documenti informatici deve essere conservata in maniera sicura e segreta dal Titolare che ne è responsabile, per tale ragione le smart card crittografiche, opportunamente protette da PIN di accesso, sono state individuate come un valido supporto, in quanto oltre a permettere la generazione delle chiavi al loro interno e l' applicazione della firma digitale, dispongono di sistemi di sicurezza che impediscono l'esportazione e la copia della chiave privata, fuori dalla smart card in cui è stata generata.

La diffusione della chiave pubblica, invece, consente a tutti i possibili destinatari dei documenti informatici di disporre della chiave necessaria per la verifica dei documenti. Per individuare in maniera sicura il sottoscrittore del documento, deve essere legata in maniera certa al titolare della corrispondente chiave privata.

5.3. DISPOSITIVO DI FIRMA

Per la normativa italiana con dispositivo di firma si intende "un apparato elettronico programmabile solo all'origine, facente parte del sistema di validazione, in grado almeno di conservare in modo protetto la chiave privata e generare al suo interno le firme digitali."

Uno degli strumenti che è possibile utilizzare come dispositivo di firma è la smart card crittografica.

5.4. SMART CARD

La smart card è simile, per forma e dimensioni, ad una tradizionale carta di credito. A differenza di quest'ultima, incorpora un processore in grado di memorizzare dati ed informazioni, a cui è possibile accedere tramite un codice di sicurezza riservato e personale (PIN).

E' perciò uno strumento di memorizzazione molto sicuro, oltre che facilmente portabile e legato al Titolare. Con le smart card dotate di processore crittografico, possono essere sviluppate applicazioni in ambiti diversi; nel campo della firma digitale svolge pricipalmente le seguenti funzioni:

- generazione e memorizzazione al suo interno della chiave privata di firma
- apposizione della firma digitale a documenti informatici

La smart card si collega con il computer mediante un apposito lettore ed il relativo software di interfaccia.

5.5. IL CERTIFICATO DIGITALE

Il certificato è il mezzo di cui dispone il destinatario per avere la garanzia sull'identità del suo interlocutore e per venire in possesso della chiave pubblica di quest'ultimo.

Per tale ragione il certificato contiene, oltre la chiave pubblica per la verifica della firma, anche i dati del titolare; è garantito e firmato da una "terza parte fidata": il certificatore.

Per la normativa italiane deve contenere almeno le seguenti informazioni:

- numero di serie del certificato
- ragione e denominazione sociale del certificatore
- codice identificativo del titolare presso il certificatore
- nome, cognome e data di nascita ovvero ragione o denominazione sociale del titolare
- valore della chiave pubblica
- algoritmi di generazione e verifica utilizzabili
- inizio e fine del periodo di validità delle chiavi
- algoritmo di sottoscrizione del certificato

Il certificato in formato X.509, contiene in uno standard riconosciuto, una serie di campi per dati obbligatori ai quali possono essere aggiunte ulteriori estensioni per riportare informazioni aggiuntive.