Linee guida per l'interoperabilità dei certificatori
13.07.00

Premessa

Le regole tecniche del DPCM 8 febbraio 1999, fissano i principi generali per esercitare l'attività di certificatore a norma della legge italiana (DPR 513 1997).

Tali principi indicano, fra l'altro, alcuni fra i più diffusi standard internazionali di riferimento nel campo dei sistemi di firma elettronica.

Il meccanismo di firma digitale si basa su concetti fondamentali come quelli di un ente certificatore (Certification Authority) e di chiavi pubblica (Kpub) e privata (Kpri) da utilizzare per la firma.

Tra le principali funzioni che un certificatore deve garantire ci sono quella di produrre il certificato che stabilisce il legame univoco tra la chiave privata ed il legittimo possessore, di custodire la chiave pubblica in una lista consultabile e di garantire la validità temporale del potere di firma (validità del certificato).

Dopo circa un anno dalla pubblicazione delle regole tecniche, sette certificatori sono stati già inclusi ufficialmente nell'elenco pubblico tenuto dall'AIPA e altri sono in procinto di iscriversi. Al fine di garantire omogeneità operativa e corretta interazione tra gli utenti che utilizzano la firma digitale, tutti i certificatori iscritti o in corso di iscrizione hanno concordato sulla necessità di individuare un documento di linee guida che, ad integrazione degli standard esistenti, desse chiare indicazioni su come affrontare i problemi sulla struttura del certificato e delle sue estensioni, sulla struttura delle liste di revoca e su quelle delle "buste elettroniche", colmando in tal modo le lacune dovute ad una interpretazione proprietaria di alcune regole sintattiche e semantiche degli standard. Tale esigenza era per altro già stata manifestata agli intermediari finanziari ed ai gestori dei sistemi di pagamento dalla Banca d'Italia, nell'ambito dell'analisi dei requisiti necessari al pieno e sicuro utilizzo della firma digitale nei trasferimenti elettronici di moneta.

La normativa vigente consente l'utilizzo di una serie di algoritmi e strutture dati definiti in standard de jure o standard de facto. Non era possibile imporre

regole precise, poiché ogni riferimento diretto ad una specifica tecnica avrebbe potuto generare squilibri sul mercato o addirittura escludere a priori una serie di fornitori. Si è perciò preferito seguire la via di fornire delle indicazioni di riferimento e poi orientarle con l'approvazione degli attori di mercato.

Questa è la strada che si è inteso perseguire con la costituzione, da parte dell'Autorità per l'informatica nella Pubblica Amministrazione, di un gruppo di lavoro, denominato "Gruppo di lavoro Interoperabilità dei Certificatori", costituito dai certificatori iscritti, o di prossima iscrizione, nell'elenco pubblico, con l'ulteriore apporto della Banca d'Italia. Attorno a questo tavolo sono stati discussi i problemi di interoperabilità che, a prescindere dalla necessaria aderenza alla normativa tecnica vigente, si pongono in una infrastruttura a chiave pubblica per la firma digitale, in assenza di accordi precisi su una serie di questioni tecnologiche. Le soluzioni al momento concordate costituiscono solo il primo passo di un percorso che si prolungherà nel tempo affrontando i temi dell'adeguamento della legislazione italiana alla normativa europea sulla firma elettronica, dell'aggiornamento delle regole tecniche all'evoluzione tecnologica, ed ogni altra problematica operativa che si dovesse manifestare sul tema della firma elettronica/digitale.

Nei paragrafi successivi, dopo una breve descrizione del processo di firma digitale, verranno descritti i problemi riscontrati e la strategia risolutiva prescelta. Per gli aspetti tecnologici che hanno caratterizzato le soluzioni individuate e concordate al tavolo sopra citato si rimanda all'allegato tecnico.

Il processo di firma digitale

A fine puramente indicativo si riporta nel seguito una breve descrizione del processo di firma digitale, così come prevista dalle norme di legge e garantito dai diversi fornitori che hanno dato origine al citato gruppo di lavoro.

Nell'effettuare la firma di un documento elettronico bisogna attivare una serie di procedure che in modo sintetico sono:

1) generazione dell'impronta del documento elettronico (una sorta di rappresentazione binaria ed univoca del documento),

2) cifratura dell'impronta del documento elettronico per mezzo della chiave privata Kpri,

3) creazione di una "busta elettronica" che contiene il documento, la firma definita al punto precedente e il certificato emesso dal certificatore che lega la chiave privata al suo possessore.

Il destinatario del documento elettronico firmato deve essere in grado di:

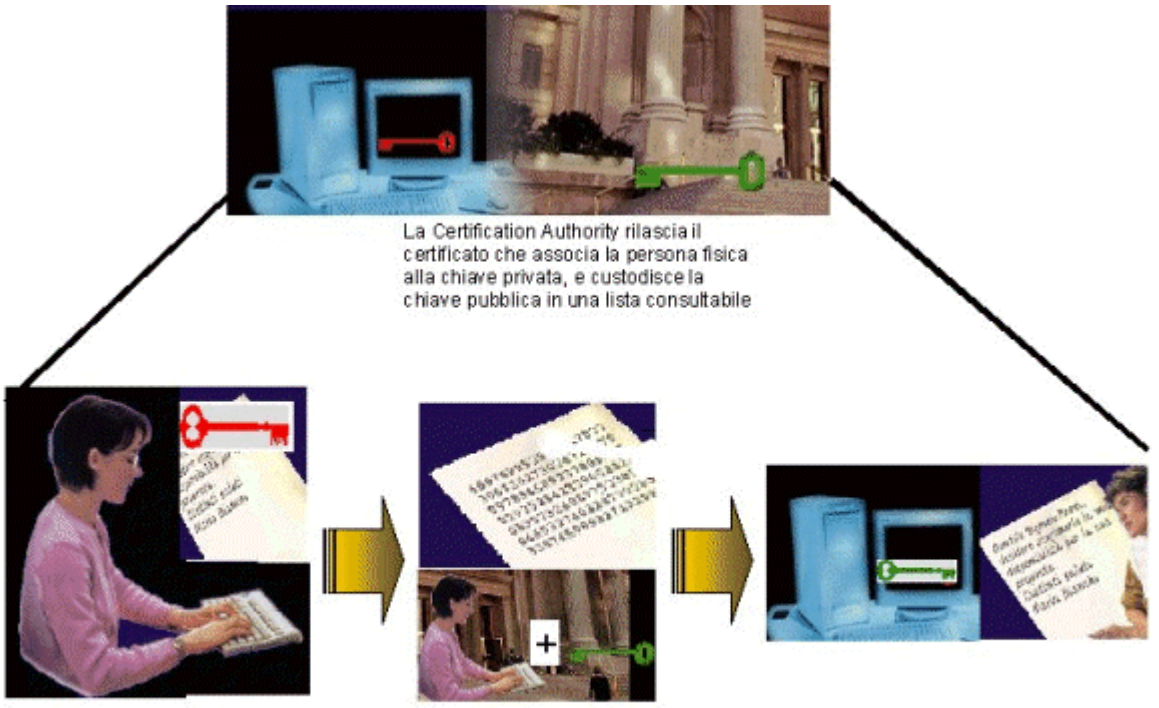
a) aprire la "busta elettronica",

b) decifrare l'impronta del documento elettronico con la Kpub del firmatario estratta dal certificato,

c) calcolare l'impronta del documento elettronico e verificare il valore ottenuto con quello firmato ai fini dell'integrità del messaggio,

d) aprire il certificato e leggere l'identità del soggetto per verificare l'identità del mittente e la validità temporale della sua firma. Per effettuare tale verifica, si deve accedere ad una speciale lista (Certification Revocation List) redatta da ogni certificatore e ricercare se il certificato ricevuto appartenga alla lista oppure no. In caso negativo, il certificato deve essere considerato ancora valido e pertanto il documento elettronico può considerarsi valido secondo quanto previsto dal DPR 513.

In sintesi:



Affinché la diffusione della firma digitale possa avvenire in modo efficace occorre che i documenti firmati da un soggetto mittente che utilizza i servizi offerti da un certificatore possano essere letti e gestiti da un soggetto destinatario che invece utilizza i servizi offerti da un altro certificatore. Se ciò non fosse possibile, lo scambio di documenti elettronici potrebbe avvenire solo fra soggetti che utilizzano uno stesso certificatore.

Molteplici sono le difficoltà che impediscono di fatto l'interoperabilità dei documenti firmati elettronicamente. Un primo ostacolo di base nasce dal fatto che esistono in linea di principio almeno due grandi classi di procedimenti di crittografia basati su tecniche RSA e DSA. Tutti i certificatori presenti attualmente nell'albo dei certificatori, o in corso di iscrizione, sono in grado di utilizzare solo la tecnica RSA.

Per rendere interoperabili le procedure di firma è necessario:

1) riconoscere il formato di una "busta elettronica";

2) essere in grado di poter aprire ed estrarre le informazioni contenute nella busta elettronica;

3) saper "leggere" il contenuto del certificato ed estrarre correttamente l'identità della persona che ha firmato e la relativa Kpub;

4) essere in grado di capire quale algoritmo sia stato utilizzato per ottenere l'impronta del documento elettronico e applicare lo stesso algoritmo al documento estratto dalla busta elettronica;

5) sapere come ricercare in modo efficace il certificato inserito nella busta elettronica nella CRL del certificatore in modo da validare definitivamente la firma.

E' fondamentale capire che gli attuali standard internazionali non garantiscono i precedenti cinque punti in modo automatico: molte sono le scelte possibili affidate al certificatore anche in funzione dei servizi che il certificatore intende offrire.

Nei mesi di febbraio, marzo e aprile 2000 sono state tenute presso l'Autorità per l'informatica una serie di riunioni con i certificatori per capire se e come fosse possibile definire in modo preciso delle scelte che garantissero l'interoperabilità così come definita nei cinque punti precedenti. Inoltre, a valle delle scelte effettuate si è verificato in modo operativo la possibilità concreta di poter interagire fra certificatori diversi.

Il risultato conseguito è tecnicamente riportato nel documento in allegato. E' importante rilevare che questo risultato rappresenta un "primizia" in campo internazionale e dimostra in modo concreto che su questo argomento l'Italia è e rimane all'avanguardia rispetto agli altri paesi e che può fornire un contributo significativo a livello internazionale al processo di standardizzazione in atto presso le sedi competenti.

Approccio metodologico

La prima e più importante decisione assunta dal GdL è stata quella di affrontare i problemi essenzialmente dal punto di vista operativo, avendo come primo obiettivo quello di raggiungere soluzioni concrete per i problemi più importanti. Da un lato ciò ha opportunamente limitato l’ambito di intervento del gruppo, dall’altro ha dato fondamentale importanza all’effettiva applicabilità delle soluzioni adottate, ossia alla disponibilità sul mercato degli strumenti necessari per attuarle.

Particolare rilevanza è stata attribuita alla semplicità delle soluzioni ed alla loro immediata applicabilità da parte di tutti i certificatori indipendentemente dalla piattaforma tecnologica da essi adottata.

Il secondo aspetto che si è preso in considerazione è stato quello della coerenza con i numerosi processi di standardizzazione in corso sulla tematica della firma digitale. La scelta è stata quella di evitare fughe in avanti,

adottando soluzioni che, pur interessanti, al momento sono ancora allo stato di proposta e non sono supportate dai prodotti commerciali. Si è tuttavia scelto di tenerne conto per quanto possibile, in particolare evitando di adottare scelte che, nel caso in cui tali soluzioni venissero successivamente adottate effettivamente, richiederebbero onerosi riadattamenti dei prodotti sviluppati.

Le questioni su cui ci si è concentrati sono state essenzialmente la compatibilità dei certificati e l'interscambiabilità dei documenti firmati. Pertanto i principali problemi affrontati sono stati:

struttura del certificato;

rappresentazione delle informazioni in esso contenute;

struttura e formato delle lista di revoca e sospensione;

struttura e rappresentazione dei documenti firmati.

Struttura del certificato

Riguardo la struttura del certificato sono stati individuati gli elementi che debbono essere comunque presenti e quelli che viceversa possono essere omessi. Particolare attenzione è stata posta nell'individuazione delle estensioni previste dallo standard X.509v3 che è necessario utilizzare per soddisfare i requisiti della normativa, specificando, per quanto possibile le modalità di utilizzo e valorizzazione. Le scelte operate sono specificate nell'Allegato Tecnico, nel quale è disponibile anche una tabella riassuntiva.

Rappresentazione delle informazioni contenute nei certificati

Le modalità di rappresentazione delle informazioni all'interno di un certificato non sono completamente specificate dagli standard di base, tanto che attualmente sono in corso di definizione degli specifici "profili" che le definiscono in modo più dettagliato per specifici contesti applicativi. I problemi principali sono la codifica e la semantica dei campi utilizzati.

Queste linee guida si soffermano principalmente sui campi destinati alla identificazione dei soggetti ed in particolare del titolare. Problemi di non facile soluzione sono posti dai vincoli presenti negli standard riguardo al set di caratteri utilizzabile ed alle limitazioni poste dai prodotti disponibili sul mercato sulla lunghezza dei campi.
Le soluzioni adottate, pur alquanto primitive, sono state scelte per la loro semplicità ed efficacia, congiunte alla possibilità di implementazione immediata. Soluzioni più raffinate, peraltro già proposte a livello di standard internazionali, potranno essere adottate non appena consolidate ed adottate all'interno dei prodotti, senza però comportare onerose conversioni del pregresso.

Struttura e formato delle lista di revoca e sospensione

Le liste di revoca e sospensione, previste dalla normativa italiana e dagli standard internazionali, pongono non pochi problemi a causa della scarso ed

inefficiente supporto che viene offerto dai prodotti commerciali. Per queste linee guida si è cercato di individuare gli elementi strettamente necessari per assicurare la funzionalità del sistema, sacrificando anche l'efficienza, se necessario per garantire la compatibilità. Il Certificatore ha comunque facoltà di mettere a disposizione soluzioni più avanzate, purché aggiuntive rispetto a quelle minime concordate.

Struttura e rappresentazione dei documenti firmati

La rappresentazione complessiva del documento firmato è l'aspetto su cui sono possibili il maggior numero di soluzioni e varianti. È infatti su questo aspetto che il gruppo ha dovuto lavorare maggiormente per raggiungere un sufficiente livello di compatibilità.

L'attenzione si è concentrata sulle numerose varianti del formato PKCS#7, quello maggiormente utilizzato in pratica, adottando una serie di convenzioni, non ultima quella di denominazione dei file in base alla tipologia di documento firmato, atte a rendere univoca l'interpretazione dell'oggetto utilizzato.

Sviluppi futuri

Il lavoro svolto consente di raggiungere un primo importante livello di interoperabilità tra gli strumenti di firma utilizzati nell'ambito della Pubblica Amministrazione.
Come controprova di quanto affermato, si riporta nel seguito una tabella che evidenzia lo stato di interoperabilità all'inizio dei lavori (*chi parla con chi*):

		Ente Mittente							
		Bnl Multiservizi	**Finital**	**Infocamere**	**Postecom**	**Saritel**	**Seceti**	**SIA**	**SSB**
Ente Destinatario	**Bnl mutiservizi**	sì	sì	sì	sì	sì	sì	sì	sì
	Finital	sì	sì	sì	no	no	no	sì	no
	Infocamere	no	no	sì	no	no	no	no	no
	Postecom	sì	no	sì	sì	no	no	no	sì
	Saritel	no	no	no	no	sì	no	no	no
	Seceti	no	no	no	no	no	sì	no	no
	SIA	no	no	no	no	no	no	sì	no
	SSB	sì	no	sì	no	sì	sì	sì	sì

Attualmente ognuna delle otto Certification Authority è in grado di leggere documenti firmati utilizzando il certificato emesso da un'altra Certification Authority.

È auspicabile che il tavolo di discussione costituito dal GdL, esaurito il suo compito istituzionale continui, nelle forme e con gli strumenti che saranno

ritenuti più idonei, ad operare per attuare un armonico processo di sviluppo che fornisca soluzioni adeguate e coerenti a tutte le problematiche di interesse.

Allegato Tecnico

Premessa

Questo documento descrive le "Linee guida per l'interoperabilità tra i Certificatori" elaborate dal gruppo di lavoro costituito dal Presidente dell'Autorità per l'informatica nella pubblica amministrazione con apposita deliberazione.

Tali Linee guida sono concepite per garantire omogeneità operativa e corretta interazione tra gli utenti che utilizzano la firma digitale. La conformità alle specifiche in esse contenute è un requisito indispensabile perché l'A.I.P.A. possa operare correttamente nei riguardi della Pubblica Amministrazione.

Le Linee guida elaborate dal Gruppo di Lavoro costituiscono l'avvio di una continua collaborazione tra l'Autorità ed i Certificatori con l'obiettivo di garantire la massima diffusione ed efficienza dei processi connessi alla firma digitale.

Tali processi seguiranno tempestivamente gli standard de jure e de facto mano a mano che questi si renderanno disponibili a livello europeo e mondiale.

Introduzione

La considerazione che solo attraverso una piena interoperabilità tra i certificatori si garantisce piena efficienza e diffusione ai processi amministrativi utilizzanti la firma digitale ha orientato gli obiettivi del Gruppo di Lavoro che ha sviluppato queste linee guida.

L'interoperabilità è da intendersi come la capacità di riconoscere e verificare buste firmate utilizzando tecnologie e strutture dati di differenti certificatori.

La soluzione al problema può essere duplice:

- a livello organizzativo con un servizio fornito dai certificatori ed in grado di comprendere e tradurre i vari dialetti di firma;
- a livello tecnico concordando uno standard per la P.A. italiana in termini di struttura del certificato e di semantica dei campi.

Appare subito evidente che la soluzione a livello tecnico è la più semplice in quanto non richiede sforzi realizzativi onerosi ed inoltre consente di seguire con sufficiente armonia e celerità le evoluzioni degli standard internazionali.
Nel seguito di queste Linee Guida sono state prese in considerazione ai fini dell'interoperabilità:

- i contenuti del certificato e la loro rappresentazione;
- le estensioni del certificato ed i loro contenuti;
- le liste di revoca e di sospensione ed i loro contenuti;
- la rappresentazione delle informazioni nelle buste PKCS#7.

L'analisi è stata condotta tenendo in conto gli standard internazionali ed le caratteristiche offerete dai prodotti di mercato.

Aspetti generali

Le tipologie di certificati cui si applicano le convenzioni stabilite in queste linee guida sono esclusivamente le seguenti:

1. certificati relativi a chiavi di certificazione di chiavi di sottoscrizione ai sensi del DPCM 8/2/1999;
2. certificati relativi a chiavi di certificazione di chiavi di marcatura temporale ai sensi del DPCM 8/2/1999;
3. certificati relativi a chiavi di sottoscrizione ai sensi del DPCM 8/2/1999;
4. certificati relativi a chiavi di marcatura temporale ai sensi del DPCM 8/2/1999.

Nessun certificato delle tipologie sopra indicate può essere utilizzato per scopo diverso da quello cui è destinato secondo la normativa.
Vengono presi in esame solo i formati di codifica, certificazione ed imbustamento delle firme utilizzate da tutti i componenti del Gruppo di Lavoro.
Questi sono rispettivamente il PKCS#1 (RSA), lo X.509 ed il PKCS#7 ver 1.5 (RFC 2315).
Per quanto attiene alle possibili differenze di formato, tutti i certificatori tratteranno le componenti di firma indistintamente nei formati ASN.1-DER (ISO 8824, 8825), BASE64 (RFC 1421) e PKCS#7 (RFC 2315).
Ciò significa che saranno elaborate correttamente tutte le componenti (certificato, busta PKCS#7, dati firmati, ecc.) indipendentemente da quale dei tre formati citati venga utilizzato per la trasmissione del dato.
Inoltre si è convenuto che un ulteriore standard di riferimento per il gruppo di lavoro dovesse essere il RFC 2459 "Internet X.509 Public Key Infrastructure Certificate and CRL Profile".

Contenuti del certificato e loro rappresentazione

L'aderenza agli standard internazionali sulla certificazione delle chiavi pubbliche non è sufficiente a garantire la corretta rappresentazione delle informazioni relative all'identificazione del titolare.
In particolare, le varie possibilità offerte dagli standard in termini di rappresentazione dei dati e la loro realizzazione nei prodotti commerciali non garantiscono una completa interazione tra i vari prodotti.

Ulteriore difficoltà è la mancanza di una collocazione naturale per alcune tipologie di dati come il codice fiscale, che è di poco interesse in senso generale ma ampiamente utilizzato (in verità è obbligatorio) nella PA italiana.
Nell'intento di porre rimedio a questi problemi, il gruppo di lavoro ha stabilito che debbano essere inserite determinate informazioni – e con una certa struttura – in alcune componenti dell'identificativo del titolare (campo **subject**) nel certificato. Le componenti interessate (la cui presenza è quindi da considerarsi obbligatoria) sono:

- **common name** (object ID = 2.5.4.3)
- **description** (object ID = 2.5.4.13)

Di seguito si forniscono le regole per la valorizzazione e strutturazione delle due componenti.

Common Name

COMMON NAME = <cognome>/<nome>/<codice fiscale titolare>/<identificativo titolare presso il certificatore>
Le parentesi acute individuano gli elementi non terminali. Il carattere / (slash) viene utilizzato come separatore di campo.
I quattro campi devono essere codificati usando il set di caratteri **PrintableString.**
Il campo <identificativo titolare presso il certificatore> contiene il dato di cui all'Art. 11, comma 1, lettera c) del D.P.C.M. 8/2/1999. Questo dato viene conservato nel COMMON NAME per garantire l'univocità del certificato e favorire eventuali operazioni di inserimento e ricerca all'interno del Directory X.500. Ai fini dell'interoperabilità NON è importante identificare il meccanismo attraverso il quale il certificatore attribuisce questo dato, né la forma assunta dal medesimo.
Qualora uno stesso soggetto è titolare di più certificati per più ruoli, deve possedere anche più codici identificativi distinti (come previsto dall'art. 22, comma 3 del D.P.C.M. 8 febbraio 2000).
Per quanto riguarda l'informazione relativa al ruolo del titolare, che permette di avere, per uno stesso soggetto, diversi certificati presso lo stesso certificatore (Art. 22, comma 3 del D.P.C.M. 8/2/99), questa può essere inserita nella DESCRIPTION (discusso di seguito).
Esempio: **commonName =** "Rossi/Mario/RSSMRA60D02F220M/XYZ123456"

Description

DESCRIPTION = "**C=**"<cognome esteso>"/**N=**"<nome esteso>"/**D=**"<data di nascita>["/**R=**"<ruolo titolare>]
Il valore di description è quindi ottenuto dalla concatenazione di quattro campi "etichettati" (tagged), il cui ordine NON è rilevante. In grassetto sono evidenziati le etichette (tag) da utilizzare. Ai quattro campi si applicano le seguenti regole:

- <cognome esteso> è il cognome per esteso del titolare, eventualmente multiplo (es. "Battistotti Sassi")
- <nome esteso> è il nome per esteso del titolare, eventualmente multiplo (es. "Carlo Maria")

- la <data di nascita> deve essere rappresentata nel formato "GG-MM-AAAA" con il carattere "0" (zero) a completamento dei numeri ad una cifra.
- il <ruolo del titolare> è l'unico campo opzionale; trattandosi di un dato di interesse applicativo e non determinante ai fini dell'interoperabilità, non si impongono regole nel suo formato

La stringa risultante dalla concatenazione dei quattro campi può essere codificata col set di caratteri **BMPString** quando ciò è necessario per rendere in modo esatto l'ortografia originale del nome e cognome estesi del titolare (es. nel caso di nomi, francesi, spagnoli, ecc.).
Esempio: **description** = "C= Großmann /N= Günther /D=03-11-1947/R=Direttore Generale"

Estensioni del certificato e loro contenuti

Queste Linee guida prevedono che le estensioni necessariamente presenti nei certificati siano:

- Authority Key Identifier: seleziona una chiave tra quelle utilizzate dal Certificatore;
- Subject Key Identifier: seleziona una chiave tra quelle a disposizione del titolare;
- Key usage: indica l'uso delle chiavi;
- Extended Key Usage: fornisce indicazioni ulteriori sull'uso delle chiavi;
- Basic Constraints: specifica se la chiave corrispondente al certificato è una chiave di certificazione;
- Certificate Policies: specifica la policy di riferimento del certificato ed il sito di distribuzione del manuale operativo;
- CrlDistributionPoint: indica dove reperire la CRL;

La presenza e le caratteristiche di una estensione dipendono dalla tipologia del certificato; la seguente tabella definisce, per i tre tipi di certificato considerati dalla normativa, le modalità di utilizzo di ciascuna estensione. Per l'interpretazione degli elementi si vedano le note esplicative appresso riportate.

Estensioni X.509v3	**Certificato per chiave di *certificazione***	**Certificato per chiave di *marcatura temporale***	**Certificato per chiave di *sottoscrizione***
Key Usage (15)	CRITICA keyCertSign + cRLSign	CRITICA digitalSignature	CRITICA nonRepudiation
Basic Constraints (19)	CRITICA cA=true		
Extended Key Usage (37)		CRITICA keyPurposeId=timeStamping	

Certificate Policies (32)	NON CRITICA policyIdentifier + URL del CPS	NON CRITICA policyIdentifier + URL del CPS	NON CRITICA policyIdentifier + URL del CPS
CRL Distribution Points (31)	NON CRITICA URL di accesso alla CRL/CSL		NON CRITICA URL di accesso alla CRL/CSL
Authority Key Identifier (35)		NON CRITICA Almeno keyIdentifier	NON CRITICA Almeno keyIdentifier
Subject Key Identifier (14)	NON CRITICA Almeno keyIdentifier	NON CRITICA Almeno keyIdentifier	NON CRITICA Almeno keyIdentifier

Note esplicative :

- Ciascun elemento della tabella indica se l'estensione associata alla riga deve essere presente o meno nel certificato corrispondente alla colonna e, nel caso debba essere presente, quale valore deve assumere; nel caso in cui non si forniscano informazioni sul valore, si intende che questo deve essere impostato seguendo le indicazioni fornite nella specifica pubblica RFC 2459.
- Il numero riportato tra parentesi nella prima colonna accanto al nome dell'estensione è l'ultima parte dello OID che individua l'estensione stessa; tale numero segue il prefisso **{2 5 29}** che individua le estensioni di certificato (esempio: lo OID completo dell'estensione Key Usage è **{2 5 29 15}**).
- "CRITICA" significa che l'estensione *deve* essere presente nel certificato e marcata come critica.
- "NON CRITICA" significa che l'estensione non deve essere marcata come critica, ma tuttavia *deve* essere presente.
- Le celle ombreggiate indicano che la corrispondente estensione *non deve* essere presente nel certificato.
- timeStamping = lo OID di valore **{1 3 6 1 5 5 7 3 8}** definito nella specifica pubblica RFC 2459.
- l'uso delle estensioni non indicate nella seguente tabella è a discrezione del certificatore, purché questi si attenga alla specifica pubblica RFC 2459.

Contenuti delle liste di revoca e sospensione

La rappresentazione delle liste di revoca e sospensione è identica, in quanto le liste di sospensione si possono considerare delle liste di revoca con il codice di revoca (CRLReason) di valore pari a 6 ("certificate hold"). Ad ogni emissione verrà prodotta un'unica lista contenente sia i certificati revocati, sia quelli sospesi.

Le liste di revoca e sospensione, emesse in formato X.509v2, oltre alle informazioni obbligatorie devono contenere le seguenti estensioni:

- estensioni al livello dell'intera lista
    - **cRLNumber** (il numero della CRL)
- estensioni a livello di singola entry
    - **reasonCode**

Il valore di tale estensione, a livello di singola entry o di intera lista è a discrezione del certificatore, purché si seguano le regole fornite nella specifica pubblica RFC 2459.

Rappresentazione delle informazioni nelle buste PKCS#7

La struttura delle buste PKCS#7 deve essere aderente a quanto previsto nella specifica pubblica RFC 2315.

Le criticità individuate dal Gruppo di Lavoro sono due:

- la rappresentazione dei dati interna ed esterna alla busta
- l'attributo autenticato "signing time".

Per quanto concerne la rappresentazione dei dati, queste Linee Guida prevedono quanto segue:

- il documento deve sempre essere *contenuto* nella busta crittografica (ovvero: non è ammessa la "detached signature")
- il documento da firmare deve essere imbustato nel formato originale (senza header o trailer aggiuntivi);
- il nome del file firmato (ossia della busta) deve assumere una doppia estensione in modo da conservare l'informazione relativa al tipo di documento che è stato firmato; il file firmato avrò quindi un nome del tipo: nome_file.tipo_documento_originale.P7M

Il tipo documento deve seguire la prassi standard delle estensioni (".DOC" per i documenti MS Word™, ".PDF" per quelli Adobe Acrobat™, ".HTM" per la pagine web, ecc.). Eventuali collisioni che si venissero a determinare devono essere gestite a parte.

Per quanto concerne gli attributi autenticati, queste Linee guida stabiliscono quanto segue.

L'attributo autenticato "signing time" si deve considerare opzionale, sia dal punto di vista della sua presenza/assenza nella busta PKCS#7, sia dal punto di vista dell'utilizzo del suo valore.

Per garantire l'interoperabilità nell'ambito della P.A., questo dato non può essere considerato critico. L'eventuale presenza di questo attributo autenticato (o di altri attributi autenticati) nella busta PKCS#7, quindi, non deve comportare di per sé l'accettazione piuttosto che il rifiuto della busta stessa. L'eventuale presenza di attributi autenticati sarà significativa solo in base a specifiche esigenze del particolare contesto applicativo in cui si opera, mentre non deve essere considerata significativa a livello di API crittografiche.

Riferimenti

Nel seguito sono riportati alcuni standard presi a riferimento nell'ambito del Gruppo di Lavoro.

D.P.R. 513/1997
D.P.C.M. 08/02/1999
RFC 1421 (P.E.M.)
RFC 2437 (PKCS#1)
RFC 2459
RFC 2314 (PKCS#10)
RFC 2315 (PKCS#7)
X.501
X.509
X.520
X.690
X.691
ISO 10118-3 (Algoritmi di hash)