CIRCOLARE 19 giugno 2000 n. AIPA/CR/24 (G.U. 30 giugno 2000, Serie generale n. 151)

(urn:nir:autorita.informatica.pubblica.amministrazione:circolare:2000-06-19;24)

Art. 16, comma 1, dell'allegato tecnico al decreto del Presidente del Consiglio dei Ministri 8 febbraio 1999, pubblicato sulla Gazzetta Ufficiale del 15 aprile 1999, serie generale, n. 87 – Linee guida per l'interoperabilità tra i certificatori iscritti nell'elenco pubblico di cui all'articolo 8, comma 3, del decreto del Presidente della Repubblica 10 novembre 1997, n. 513.

Premessa

Com'è noto, con il decreto del Presidente della Repubblica 10 novembre 1997, n. 513 (recante: "Regolamento recante criteri e modalità per la formazione, l'archiviazione e la trasmissione di documenti con strumenti informatici e telematici, a norma dell'art. 15, comma 2, della legge 15 marzo 1997, n. 59") è stata introdotta nel nostro ordinamento la firma digitale. L'art. 8, comma 3, del citato D.P.R. n. 513/1997 stabilisce che le attività di certificazione sono effettuate da certificatori inclusi in apposito elenco pubblico, consultabile in via telematica, predisposto, tenuto e aggiornato dall'Autorità per l'informatica nella pubblica amministrazione.

Con la circolare 26 luglio 1999, n. AIPA/CR/22 sono state stabilite le modalità con le quali le società interessate ad esercitare l'attività di certificatore devono inoltrare all'Autorità la domanda di iscrizione nell'elenco pubblico di cui al citato art. 8. In base a tale norma, i certificatori devono essere dotati di appositi requisiti e, per quanto riguarda le specifiche tecniche, essi devono osservare le regole di cui al D.P.C.M. 8 febbraio 1999.

La disciplina dei requisiti tecnici di sicurezza, pur riferendosi a standard internazionali, dà facoltà ad ogni certificatore di scegliere fra diverse tecnologie e strutture dei certificati. È pertanto possibile che, a causa di incompatibilità delle tecnologie e della struttura dei certificati utilizzati, soggetti che possiedono firme digitali certificate da differenti certificatori non siano in grado di scambiarsi tra loro documenti elettronici firmati. La problematica, peraltro, non ha trovato soluzione neppure con l'emanazione della direttiva europea sulla firma digitale, dove il problema dell'interoperabilità della firma digitale viene demandato ad un processo di standardizzazione internazionale a medio e lungo termine.

Ad un anno circa dalla pubblicazione delle regole tecniche, sette certificatori sono stati inclusi nell'elenco pubblico tenuto dall'Autorità e altri sono in procinto di iscriversi. Al fine perciò di garantire l'omogeneità operativa e la corretta interazione tra gli utenti che utilizzano la firma digitale, è stata avviata dall'Autorità un'azione di sensibilizzazione su queste tematiche nei confronti di tutti i certificatori iscritti, come pure nei confronti di quelli che hanno presentato domanda di iscrizione, affinché concordassero, in base all'art. 17 dell'allegato tecnico al D.P.C.M. 8 febbraio 1999, sulla necessità di individuare un documento di Linee guida che, ad integrazione degli standard esistenti, fornisse chiare indicazioni su come affrontare i problemi sulla struttura del certificato e sulle sue estensioni, sulla struttura delle liste di revoca e su quelle delle "buste elettroniche". Ciò al fine di colmare le lacune dovute ad un'interpretazione proprietaria di alcune regole sintattiche e semantiche degli standard, come peraltro già segnalato 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 *de facto*. Non essendo possibile imporre regole precise, poiché ogni riferimento diretto ad una specifica tecnica potrebbe generare squilibri sul mercato o, addirittura, provocare a priori l'esclusione di alcuni fornitori, si ritiene comunque necessario fornire, con le presenti Linee guida, delle indicazioni di riferimento, anche tenendo conto dei suggerimenti provenienti dagli attori di mercato.

L'Autorità, per suo conto, ritiene che la soluzione del problema dell'interoperabilità della firma digitale è condizione necessaria per consentire il pieno utilizzo dei servizi di interoperabilità della Rete unitaria e per l'erogazione dei servizi diretti al cittadino.

Con la presente circolare, resa disponibile anche sul sito Internet dell'Autorità per l'informatica www.aipa.it, tenuto anche conto del disposto di cui all'art. 21 del D.P.C.M. 8 febbraio 1999 in tema di accordi tra certificatori, vengono appunto indicate le Linee guida per garantire l'omogeneità operativa e la corretta interazione tra gli utenti che utilizzano la firma digitale e la massima diffusione ed efficienza dei processi connessi alla firma digitale.

1. Il processo di firma digitale

Solo attraverso una piena interoperabilità tra i documenti elettronici firmati utilizzando certificatori diversi si garantisce piena efficienza e diffusione ai processi amministrativi utilizzanti la firma digitale.

La soluzione al problema può essere duplice:

- a livello organizzativo, con un servizio fornito dai certificatori ed in grado di interpretare e tradurre i vari formati di firma;
- a livello tecnico, concordando uno standard per la P.A. italiana in termini di struttura del certificato e delle sue estensioni.

Appare 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 coerenza e tempestività le evoluzioni degli standard internazionali.
Ai fini di un primo livello base di interoperabilità sono da prendere in considerazione, oltre ai contenuti del certificato ed alla 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.

La redazione delle Linee guida discende da un'analisi degli attuali standard internazionali e delle caratteristiche offerte dai prodotti di mercato.
Le tipologie di certificati cui si applicano le convenzioni stabilite nelle presenti Linee guida sono esclusivamente le seguenti:

1. certificati relativi a chiavi di certificazione di chiavi di sottoscrizione ai sensi del D.P.C.M. 8 febbraio 1999;
2. certificati relativi a chiavi di certificazione di chiavi di marcatura temporale ai sensi del D.P.C.M. 8 febbraio 1999;
3. certificati relativi a chiavi di sottoscrizione ai sensi del D.P.C.M. 8 febbraio 1999;
4. certificati relativi a chiavi di marcatura temporale ai sensi del D.P.C.M. 8 febbraio 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 certificatori finora iscritti nell'elenco pubblico, che 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 dovesse essere il RFC 2459 "Internet X.509 Public Key Infrastructure Certificate and CRL Profile".

2. 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 pubblica amministrazione italiana.
Nell'intento di porre rimedio a questi problemi, si è 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.

a) 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 febbraio 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 sia titolare di più certificati per più ruoli, deve possedere più codici identificativi distinti (come previsto dall'art. 22, comma 3 del D.P.C.M. 8 febbraio 1999).
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 febbraio 1999), questa può essere inserita nella DESCRIPTION (discusso di seguito).

Esempio: **CommonName =** "Rossi/Mario/RSSMRA60D02F220M/XYZ123456"

b) 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 evidenziate 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.).

Es.: **description** = "C Großmann = /N= Günther/D=03-11-1947/R=Direttore Generale".

3. Estensioni del certificato e suoi contenuti

Le Linee guida prevedono che le estensioni che devono essere contenute 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 un'estensione dipendono dalla tipologia del certificato. La tabella che segue 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:

a. 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.
b. 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}**).
c. "CRITICA" significa che l'estensione ***deve*** essere presente nel certificato e marcata come critica.
d. "NON CRITICA" significa che l'estensione ***non deve*** essere marcata come critica, ma tuttavia ***deve*** essere presente.
e. Le celle ombreggiate indicano che la corrispondente estensione ***non deve*** essere presente nel certificato.
f. TimeStamping = lo OID di valore **{1 3 6 1 5 5 7 3 8}** definito nella specifica pubblica RFC 2459.
g. L'uso delle estensioni non indicate nella seguente tabella è a discrezione del certificatore, purché questi si attenga alla specifica pubblica RFC 2459.

4. 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.

5. 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 sono due:

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

Per quanto concerne la rappresentazione dei dati, viene previsto 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 avrà 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, con le presenti Linee guida si stabilisce 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 pubblica amministrazione, 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.

IL PRESIDENTE: REY

Riferimenti

Si riportano alcuni standard presi a riferimento per la stesura delle presenti Linee guida.

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)