CENTRO NAZIONALE PER L'INFORMATICA NELLA PUBBLICA AMMINISTRAZIONE

DELIBERAZIONE N. 45 DEL 21 MAGGIO 2009

IL COLLEGIO

Visto il decreto legislativo 12 febbraio 1993, n. 39 così come modificato dall'articolo 176, comma 3, del decreto legislativo 30 giugno 2003, n.196;

Visto il decreto legislativo 7 marzo 2005, n. 82, e successive modificazioni ed integrazioni, recante "Codice dell'amministrazione digitale" e, in particolare, la sezione II del Capo II, che disciplina le firme elettroniche ed i certificatori, e l'articolo 71, comma 1;

Visto il decreto del Presidente del Consiglio dei Ministri 30 marzo 2009, recante "Regole tecniche in materia di generazione, apposizione, verifica delle firme digitali e validazione temporale" ed, in particolare, gli articoli 3, comma 2, e 38, comma 4;

Espletata la procedura di notifica alla Commissione europea di cui alla direttiva 98/34/CE del Parlamento europeo e del Consiglio, del 22 giugno 1998, modificata dalla direttiva 98/48/CE del Parlamento europeo e del Consiglio, del 20 luglio 1998, attuata con decreto legislativo 23 novembre 2000, n. 427;

DELIBERA

di adottare le seguenti regole:

REGOLE PER IL RICONOSCIMENTO E LA VERIFICA DEL DOCUMENTO INFORMATICO

TITOLO I

DISPOSIZIONI GENERALI

ART. 1

(Definizioni)

1. Ai fini della presente deliberazione si intendono richiamate le definizioni contenute nell'articolo 1 del decreto legislativo 7 marzo 2005, n. 82 e successive modificazioni ed integrazioni, e nell'articolo 1 del decreto del Presidente del Consiglio dei Ministri 30 marzo 2009 e successive modificazioni. Si intende inoltre per:

a) attributo: informazione associata ad un documento informatico o ad una busta crittografica oppure informazione elementare contenuta in un campo di un certificato elettronico o di una CRL come un nome, un numero o una data;

b) attributo autenticato: attributo incluso nella firma elettronica di un documento e, quindi, ad esso associato in modo protetto dalla firma stessa;

c) campo: unità informativa contenuta in un certificato o in una CRL. Può essere composta da diverse unità informative elementari dette "attributi";

d) CAdES: formato di busta crittografica definito nella norma ETSI TS 101 733 V1.7.4 basata a sua volta sulle specifiche RFC 3852 e RFC 2634 e successive modificazioni;

e) codice: il codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n.82;

f) controfirma: la firma apposta ad una precedente firma;

g) estensione: metodo utilizzato per associare specifiche informazioni (attributi) alla chiave pubblica contenuta nel certificato;

h) ETSI (European Telecommunications Standards Institute): organizzazione indipendente, no profit, la cui missione è produrre standard sulle tecnologie dell'informazione e della comunicazione (ICT). E' riconosciuto ufficialmente dalla Commissione Europea come ESO (European Standards Organisation);

i) firme multiple: firme digitali apposte da diversi sottoscrittori allo stesso documento;

l) firme parallele: le firme apposte da differenti soggetti al medesimo documento informatico utilizzando una sola busta crittografica;

m) HTTP (Hypertext Transfer Protocol): protocollo per il trasferimento di pagine ipertestuali e risorse in rete conforme alla specifica RFC 2616 e successive modificazioni;

n) IETF (Internet Engineering Task Force**):** comunità aperta di tecnici, specialisti e ricercatori interessati all'evoluzione tecnica e tecnologica di Internet;

o) ISO (International Organization for Standardization): organizzazione indipendente, la cui missione è quella di produrre standard riconosciuti a livello mondiale;

p) LDAP (Lightweight Directory Access Protocol): protocollo di rete, conforme alla specifica RFC 3494 e successive modificazioni, utilizzato per rendere accessibili in rete informazioni con servizi di directory basati sulla famiglia di standard ITU X.500;

q) marcatura critica: caratteristica che possono assumere le estensioni conformemente allo specifica RFC 5280 e successive modificazioni;

r) OCSP (Online Certificate Status Protocol): protocollo di rete, conforme alla specifica RFC 2560 e successive modificazioni, utilizzato per verificare la validità dei certificati elettronici;

s) OID (Object IDentifier): codice univoco basato su una sequenza ordinata di numeri per l'identificazione di evidenze informatiche utilizzate per la rappresentazione di oggetti come estensioni, attributi, documenti e strutture di dati in genere nell'ambito degli standard internazionali relativi alla interconnessione dei sistemi aperti che richiedono un'identificazione univoca in ambito mondiale;

t) padding: riempimento dati di evidenze informatiche, tipicamente utilizzato nell'ambito delle applicazioni crittografiche, al fine del raggiungimento di una lunghezza predefinita nei formati a blocchi delle strutture dati utilizzate dagli algoritmi;

u) PAdES: formato di busta crittografica definito nella norma ETSI TS 102 778 basata a sua volta sullo standard ISO/IEC 32000 e successive modificazioni;

v) PDF (Portable Document Format): formato documentale elettronico definito dallo standard internazionale ISO/IEC 32000;

z) regole tecniche: le regole tecniche in materia di generazione, apposizione, verifica delle firme digitali e validazione temporale adottate con decreto del Presidente del Consiglio dei Ministri 30 marzo 2009 pubblicate sulla G.U. 6 giugno 2009, n. 129;

aa) RFC (Request For Comments): documenti contenenti specifiche tecniche standard, riconosciute a livello internazionale, definite dall'Internet Engineering Task Force (IETF) e dall'Internet Engineering Steering Group (IESG);

bb) W3C (World Wide Web Consortium): un consorzio internazionale di soggetti che operano in Internet e con il Web, con lo scopo di sviluppare tecnologie interoperabili come specifiche, linee guida, software e strumenti per l'evoluzione del Web;

cc) XML (eXtended Markup Language): insieme di regole per strutturare in formato testo i dati oggetto di elaborazione.

ART. 2

(Ambito di applicazione e contenuto)

1. La presente deliberazione stabilisce le regole per il riconoscimento e la verifica del documento informatico alle quali devono attenersi i certificatori accreditati ai sensi dell'articolo 29 del codice, di seguito denominati certificatori accreditati.
2. Le disposizioni di cui al titolo II indicano gli algoritmi per la generazione e verifica della firma digitale.
3. Le disposizioni di cui al titolo III definiscono il profilo dei certificati qualificati e le informazioni che in essi devono essere contenute.
4. Le disposizioni di cui al titolo IV definiscono il profilo e le informazioni che devono essere contenute nei certificati elettronici di certificazione e di marcatura temporale.
5. Le disposizioni di cui al titolo V definiscono le regole per la validazione temporale, il formato e le informazioni che devono essere contenute nelle marche temporali utilizzate dai sistemi di validazione temporale dei documenti, così come definiti nel Titolo IV delle regole tecniche.
6. Le disposizioni di cui al titolo VI definiscono i formati e le modalità di accesso alle informazioni sulla revoca e sulla sospensione dei certificati, ai sensi dell'articolo 30 delle regole tecniche.
7. Le disposizioni di cui al titolo VII definiscono i formati delle buste crittografiche destinate a contenere gli oggetti sottoscritti con firma digitale.
8. Le disposizioni di cui al titolo VIII definiscono i requisiti delle applicazioni di apposizione e verifica della firma digitale di cui agli articoli 9, comma 10, e articolo 10 delle regole tecniche.

TITOLO II

ALGORITMI PER LA GENERAZIONE E VERIFICA DELLA FIRMA DIGITALE

ART. 3

*(*Algoritmi crittografici)

1. I certificatori accreditati devono utilizzare l'algoritmo RSA (Rivest-Shamir-Adleman) con lunghezza delle chiavi non inferiore a 1024 bit; le chiavi di certificazione di cui all'articolo 4, comma 4, lettera b) delle regole tecniche devono avere una lunghezza non inferiore a 2048 bit.
2. A partire dall'anno successivo a quello dell'entrata in vigore della presente deliberazione, le firme elettroniche apposte utilizzando algoritmi di crittografia asimmetrica basati sulle curve ellittiche hanno valore di firma digitale ai sensi della normativa vigente.
3. Ai fini della realizzazione di quanto previsto ai commi 1 e 2, i certificatori accreditati devono rispettare le specifiche contenute nel documento ETSI TS 102 176.1 V2.0.0.

ART. 4

(Funzioni di hash)

1. I certificatori accreditati devono utilizzare per la sottoscrizione dei certificati elettronici di certificazione, di sottoscrizione e di marcatura temporale e per la sottoscrizione delle relative CRL, il seguente algoritmo, definito nella norma ISO/IEC 10118-3:2004:

   dedicated hash-function 4, corrispondente alla funzione SHA-256.

2. Le applicazioni di generazione e verifica della firma digitale per la sottoscrizione dei documenti informatici devono utilizzare la funzione di *hash* indicata al comma 1.

3. Le applicazioni di generazione e verifica della marca temporale devono utilizzare la funzione di hash indicata al comma 1.

4. Fino allo scadere dei termini previsti nell'articolo 29 della presente deliberazione, i certificatori accreditati devono utilizzare il seguente algoritmo, definito nella norma ISO/IEC 10118-3:2004:

   dedicated hash-function 3, corrispondente alla funzione SHA-1.

ART. 5

(Metodi di sottoscrizione)

1. Per la generazione e la verifica della firma digitale conforme alla specifica ETSI TS 101 733 si deve utilizzare il metodo di sottoscrizione sha256-with-rsa (sha256WithRSAEncryption (OID.1.2.840.113549.1.1.11) con *padding* conforme alla specifica RFC 3447.

2. Le firme di cui all'articolo 3, comma 2 devono utilizzare il metodo di sottoscrizione ecdsa-with-Sha256 (OID 1.2.840.10045.4.3.2).

3. Nella sottoscrizione in linguaggio XML l'algoritmo per la generazione e la verifica della firma digitale in linguaggio XML (*SignatureValue*) da applicare all'elemento *SignedInfo* è l'algoritmo RSA-SHA256. Si deve specificare nell'attributo *Algorithm* dell'elemento *DigestMethod* l'indicatore:

   http://www.w3.org/2001/04/xmlenc#sha256

   Nel caso di utilizzo della crittografia basata sull'algoritmo RSA l'indicatore che deve essere indicato nell'attributo *Algorithm* dell'elemento *SignatureMethod* è:

   http://www.w3.org/2001/04/xmldsig-more#rsa-sha256

   come indicato nella specifica RFC 4051.
   Nel caso di utilizzo della crittografia basata sulle curve ellittiche l'indicatore che deve essere indicato è:

   http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha256

   come indicato nella specifica RFC 4051.

4. La sottoscrizione in formato PDF deve utilizzare il *Message* Digest SHA-256.

ART. 6

(XML: Algoritmi per la canonicalizzazione)

1. L'applicazione di firma in linguaggio XML deve utilizzare per la canonicalizzazione (versione 1.1) dell'elemento *SignedInfo* quanto stabilito dal seguente indicatore:

   http://www.w3.org/2006/12/xml-c14n11

2. Nel caso di sottoscrizione di una parte del documento informatico deve essere utilizzata la canonicalizzazione di tipo esclusivo (versione 1.1) definita dai seguenti indicatori:

http://www.w3.org/2006/12/xml-c14n11#

http://www.w3.org/2006/12/xml-c14n11#WithComments

3. L'applicazione di verifica della firma in linguaggio XML deve supportare la canonicalizzazione (versione 1.1) di cui ai commi 1 e 2 e la canonicalizzazione (versione 1.0) dell'elemento <*SignedInfo*> secondo quanto stabilito dal seguente indicatore:

http://www.w3.org/TR/2001/REC-xml-c14n-20010315

4. Gli indicatori di cui ai commi 1 e 2 devono essere riportati nell'attributo *Algorithm* dell'elemento *CanonicalizationMethod.*

ART. 7

(XML: Algoritmi di trasformazione)

1. L'insieme minimo di trasformazioni che le applicazioni di verifica devono essere in grado di gestire è il seguente:

   a. **Base64** identificata dall'indicatore
   http://www.w3.org/2000/09/xmldsig#base64

   b. **Xpath** identificata dall'indicatore
   http://www.w3.org/2002/06/xmldsig-filter2

   c. **XSLT** identificata dall'indicatore
   http://www.w3.org/TR/1999/REC-xslt-19991116

   Questa trasformazione deve essere sempre eseguita prima della canonicalizzazione.
   L'indicatore che identifica la trasformazione, come stabilito nella specifica RFC 3275, deve essere riportato nell'attributo *Algorithm* dell'elemento *Transform.*

ART. 8

(XML: Regole specifiche di trasformazione)

1. Nella modalità di sottoscrizione *enveloped*, nel caso di firme multiple parallele, descritte nell'articolo 24, comma 1, lettera a) è necessario assicurare che tutte le firme successive alla prima siano riferibili ai medesimi dati sui quali è stata calcolata la prima firma. Poiché ciò non avviene in modo automatico, si deve fare in modo che siano gestite le strutture <*ds:Signature*> a partire dai dati originali sottoscritti.

   Nei casi in cui sia applicata una trasformazione XPath questa deve essere specificata nell'elemento <*ds:Transforms*> all'interno dell'elemento <*ds:SignedInfo*>.

   La trasformazione deve essere basata sulla sintassi descritta nella raccomandazione XPath Filter 2.0 identificata dall'indicatore:

   http://www.w3.org/2002/06/xmldsig-filter2

   o sulla sintassi XPath v2.0 identificata dall'indicatore:
   http://www.w3.org/TR/xpath20

   Le applicazioni di firma e di verifica devono supportare le trasformazioni sopra descritte.

2. Nella trasformazione di cui all'articolo 7, comma 1, lettera c), il foglio di stile deve essere utilizzato al fine della presentazione all'utente del documento informatico. Tale trasformazione, se indicata, deve essere l'unica trasformazione di questo tipo presente nell'elemento <*ds:Reference*> e l'ultima nella sequenza delle operazioni di trasformazione per questo elemento <*ds:Reference*>.
3. La trasformazione di cui all'articolo 7, comma 1, lettera c), deve essere in grado di presentare all'utente il documento informatico in maniera tale da garantire la staticità del contenuto. Se il relativo foglio di stile è autenticato, tale circostanza deve essere presentata all'utente unitamente all'informazione dell'identità di chi ha eseguito l'autenticazione.
4. I formati ammessi per il documento informatico risultante dalla trasformazione sono:
    a. UTF-8 e successive modifiche;
    b. conformi alla specifica XHTML, versione 1.0 definita dall'indicatore:
    http://www.w3.org/TR/xhtml1

    dove la tipologia di documento XML da utilizzare deve essere conforme alla specifica seguente:

    http://www.w3.org/TR/2002/REC-xhtml1-20020801/DTD/xhtml1-strict.dtd

5. Nei casi nei quali il foglio di stile di cui al comma 3, non è completamente contenuto nell'elemento <*Transform*>, ma è identificato tramite un indicatore come risorsa esterna, il foglio di stile deve essere autenticato in conformità a quanto previsto dalla presente deliberazione in materia di firma digitale in linguaggio XML e in particolare a quanto stabilito nell'articolo 22, comma 2, lettera a).

ART. 9

(Elementi specifici per il profilo di firma in linguaggio XML)

1. L'elemento *KeyInfo*, opzionale nella specifica RFC 3275, deve essere sempre presente nella busta crittografica.
2. L'elemento *SignedInfo* deve contenere un elemento *Reference* che includa il *KeyInfo*, in modo che quest'ultimo concorra nel computo della firma.
3. L'applicazione di firma deve includere nella struttura *KeyInfo* l'elemento *X509Data* (http://www.w3.org/2000/09/xmldsig#X509Data) contenente il certificato qualificato del sottoscrittore.
4. L'applicazione di verifica deve gestire almeno l'elemento *X509Data* e utilizzare il certificato contenuto nella busta per le operazioni di verifica della firma.

ART. 10

(Elementi specifici per il profilo di firma in formato PDF)

1. Gli elementi specifici per il profilo di firma in formato PDF devono essere conformi alle specifiche ETSI TS 102 778 parte 2 e successive.

TITOLO III

PROFILO DEI CERTIFICATI QUALIFICATI

ART. 11

(Norme generali)

1. Ove non diversamente indicato, il profilo dei certificati deve essere conforme alla specifica RFC 5280, capitolo 4, recante "Profilo dei certificati e delle estensioni dei certificati" e conforme alla specifica ETSI TS 101 862 V1.3.2, recante "Profilo dei Certificati Qualificati".

ART. 12

(Profilo dei certificati qualificati)

1. Salvo quanto diversamente disposto nella presente deliberazione, ai certificati qualificati si applica quanto stabilito nella specifica ETSI TS 102 280 V1.1.1, recante "Profilo dei certificati X.509 V.3 per certificati rilasciati a persone fisiche".
2. Il campo *Issuer* (emittente) del certificato deve contenere almeno i seguenti attributi:
   a) *organizationName* (OID: 2.5.4.10), che contiene la ragione sociale o denominazione dell'organizzazione che emette il certificato qualificato;
   b) *countryName* (OID: 2.5.4.6), che contiene il *country code* ISO 3166 dello Stato in cui è registrata l'organizzazione indicata nell'*organizationName*.
3. Il campo *SubjectDN* (Dati identificativi del titolare) del certificato deve contenere i seguenti attributi:
   a) *givenName* e *surname* (OID: 2.5.4.42 e 2.5.4.4), che contengono rispettivamente il nome e il cognome del titolare del certificato;
   b) *countryName* (OID: 2.5.4.6), che, nel caso in cui l'*organizationName* contenga il valore "non presente", contiene il *country code* ISO 3166 dello Stato di residenza del titolare; nel caso in cui l'*organizationName* contenga un valore diverso da "non presente", contiene il *country code* ISO 3166 dello Stato che ha assegnato all'organizzazione il codice identificativo riportato nell'attributo *organizationName*;
   c) *organizationName* (OID: 2.5.4.10), che contiene, se applicabile, la ragione sociale o la denominazione e il codice identificativo dell'organizzazione che ha richiesto o autorizzato il rilascio del certificato del titolare. Il codice identificativo è un codice rilasciato dalla competente autorità dello Stato indicato nell'attributo *countryName*. Se l'*organizationName* non è applicabile, assume il valore "non presente";
   d) *serialNumber* (OID: 2.5.4.5) che contiene il codice fiscale del titolare rilasciato dall'autorità fiscale dello Stato di residenza del titolare o, in mancanza, un analogo codice identificativo, quale ad esempio un codice di previdenza sociale o un codice identificativo generale. In mancanza di tale codice identificativo potrà essere utilizzato il numero del passaporto preceduto da "PASSPORT".Allo scopo di definire il contesto per la comprensione del codice in questione, il codice stesso è preceduto dal *country code* ISO 3166 e dal carattere ":"(in notazione esadecimale "0x3A").;
   e) in alternativa agli attributi specificati alla lettera a), il certificato può contenere l'attributo *pseudonym* (OID: 2.5.4.65), che contiene una qualsiasi stringa univoca nell'ambito del certificatore, a discrezione del titolare. La stringa utilizzata non permette di risalire ai dati identificativi del titolare. Se l'attributo *pseudonym* è presente, l'attributo *countryName* assume il valore "IT", l'attributo *organizationName* assume il valore "non presente", l'attributo *serialNumber* il valore "pseudonimo" e gli attributi *title* e *localityName* non sono presenti;
   f) *dnQualifier* (OID: 2.5.4.46), contiene il codice identificativo del titolare presso il certificatore. Detto codice, assegnato dal certificatore, è univoco nell'ambito del certificatore stesso.
4. Il campo *subjectDN* (Dati identificativi del titolare) del certificato può contenere altri attributi purché non in contrasto con quanto previsto dal documento ETSI TS 102 280. L'eventuale codifica degli

attributi *title*, *localityName*, *commonName* e *organizationalUnitName* deve rispettare le seguenti regole:

a) *title* (OID: 2.5.4.12), contiene una indicazione della qualifica specifica del titolare, quale l'appartenenza ad ordini o collegi professionali, l'iscrizione ad albi o il possesso di altre abilitazioni professionali, ovvero i poteri di rappresentanza nell'ambito dell'organizzazione specificata nell'attributo *organizationName*. Nel caso in cui l'attributo *organizationName* contenga un valore diverso da "non presente", l'inserimento delle informazioni nel *title* è richiesto dall'organizzazione ivi indicata ed il certificatore deve conservare tale richiesta per il periodo indicato nell'articolo 15, comma 7 delle regole tecniche; in caso contrario deve contenere informazioni derivanti da autocertificazione effettuata dal titolare ai sensi della normativa vigente;

b) *localityName* (OID: 2.5.4.7), contiene, nel caso in cui l'attributo *organizationName* contenga un valore diverso da "non presente", informazioni pertinenti all'organizzazione specificata;

c) *commonName* (OID: 2.5.4.3), in aggiunta a *surname* e *givenName*, contiene l'eventuale altro nome con il quale il titolare è comunemente conosciuto.

d) *organizationalUnitName* (OID: 2.5.4.11), contiene ulteriori informazioni inerenti all'organizzazione.
Tale attributo può comparire, al massimo, cinque volte.

5. Il certificato deve contenere inoltre le seguenti estensioni:

a) *keyUsage* (OID: 2.5.29.15), che contiene esclusivamente il valore *nonRepudiation* (bit 1 impostato a 1). L'estensione è marcata critica;

b) *certificatePolicies* (OID: 2.5.29.32), che contiene l'*OID* della *Certificate Policy* (CP) e l'*Uniform Resource Locator (URL*) che punta al *Certificate Practice Statement* (CPS) nel rispetto del quale il certificatore ha emesso il certificato. Se non viene adottata una CP definita a livello nazionale o europeo, il certificatore deve definire una propria CP e tale *OID* deve essere definito e pubblicizzato dal certificatore. Possono essere indicate più *Certificate Policy* (CP). L'URL deve configurare un percorso assoluto per l'accesso al CPS. L'estensione non è marcata critica;

c) *CRLDistributionPoints* (OID: 2.5.29.31), che contiene l'URL che punta alle CRL pubblicate dal certificatore dove eventualmente saranno disponibili le informazioni relative alla revoca o sospensione del certificato in questione. L'URL configura un percorso assoluto per l'accesso alla CRL. Lo schema da utilizzare per l'URL è HTTP oppure LDAP e consente lo scaricamento anonimo della CRL. Nel caso vengano valorizzati più di un URL per l'estensione, tali URL configurano percorsi coerenti con l'ultima CRL pubblicata. L'estensione non è marcata critica;

d) *authorityKeyIdentifier* (OID: 2.5.29.35), che contiene almeno il campo *keyIdentifier*. L'estensione non è marcata critica;

e) *subjectKeyIdentifier* (OID: 2.5.29.14), che contiene il valore *keyIdentifier* per identificare il certificato. L'estensione non è marcata critica;

f) *qcStatements*, identificate nel documento ETSI TS 101 862 come segue:

1) *id-etsi-qcs-QcCompliance* (OID: 0.4.0.1862.1.1);

2) *id-etsi-qcs-QcLimitValue* (OID: 0.4.0.1862.1.2) – presente se sono applicabili limiti nelle negoziazioni;

3) *id-etsi-qcs-QcRetentionPeriod* (OID: 0.4.0.1862.1.3) – il valore indicato è pari o superiore a "20";

4) *id-etsi-qcs-QcSSCD* (OID: 0.4.0.1862.1.4).

L'estensione non è marcata critica.

6. Il certificato di sottoscrizione può contenere le seguenti estensioni:

a) *SubjectDirectoryAttributes* (OID: 2.5.29.9). Essa non contiene alcuno dei campi indicati ai commi 3 e 4. L'attributo *dateOfBirth* (OID: 1.3.6.1.5.5.7.9.1), se presente, è codificato nel formato *GeneralizedTime*. L'estensione non è marcata critica;

b) *authorityInfoAccess* (OID: 1.3.6.1.5.5.7.1.1).

Nel caso in cui il certificatore metta a disposizione, conformemente all'articolo 19, un sistema OCSP per la verifica della validità di un certificato, l'estensione *AuthorityInfoAccess* deve contenere un campo *accessDescription* con la descrizione delle modalità di accesso al servizio OCSP e i seguenti attributi:

1) *accessMethod*, che contiene l'identificativo *id-ad-ocsp* (OID: 1.3.6.1.5.5.7.48.1);

2) *accessLocation*, che contiene l'URI che punta all'OCSP *Responder* del certificatore, utilizzabile per effettuare la verifica del certificato stesso. L'URI configura un percorso assoluto per l'accesso all'OCSP *Responder*.

Nel caso in cui siano specificati più campi *accessDescription* contenenti l'identificativo *id-ad-ocsp* nell'attributo *accessMethod*, tali indicazioni devono configurare diversi percorsi alternativi per l'interrogazione, tramite OCSP, dello stato del certificato. L'estensione non è marcata critica;

c) Salvo quanto disposto all'articolo 12, comma 5, lettera f), gli eventuali ulteriori limiti d'uso di cui all'articolo 41 delle regole tecniche sono inseriti nell'attributo *explicitText* del campo *userNotice* dell'estensione *certificatePolicies*. Sul sito istituzionale del CNIPA vengono pubblicati i testi e le codifiche delle limitazioni d'uso che i certificatori devono garantire agli utenti.

d) Ulteriori estensioni possono essere inserite nel certificato purché conformi ai documenti e alle specifiche citati nella presente deliberazione e non marcate critiche. Possono essere utilizzate altre estensioni definite in standard internazionalmente riconosciuti purché questi non siano in contrasto con la presente deliberazione, anche queste non marcate critiche.

TITOLO IV

PROFILO DEI CERTIFICATI DI CERTIFICAZIONE E MARCATURA TEMPORALE

ART. 13

(Profilo dei certificati di certificazione e marcatura temporale)

1. Se non diversamente previsto, il profilo dei certificati di certificazione e marcatura temporale deve essere conforme alla specifica RFC 5280.
2. Per la codifica dei certificati deve essere utilizzato il formato ASN.1 – DER (ISO/IEC 8824, 8825) in rappresentazione binaria o alfanumerica ottenuta applicando la trasformazione BASE 64 (RFC 1421 e successive modifiche). La testata e la coda previsti in RFC 1421 possono essere assenti. Nel primo caso il file contenente il certificato deve assumere l'estensione .der o .cer, nel secondo caso .b64.

ART. 14

(Uso delle estensioni nei certificati di certificazione)

1. I certificati di certificazione devono contenere le seguenti estensioni:
   a) *keyUsage* (OID 2.5.29.15) – contiene i valori *keyCertSign* e *cRLSign* (bit 5 e 6 impostati a 1). L'estensione è marcata critica;
   b) *basicConstraints* (OID 2.5.29.19) - contiene il valore CA=*true*. L'estensione è marcata critica;

c) *certificatePolicies* (OID 2.5.29.32) - contiene uno o più identificativi delle *policyIdentifier* e le URL dei relativi CPS. Può contenere l'OID generico previsto dall'RFC 5280 (2.5.29.32.0). L'estensione non è marcata critica;

d) *CRLDistributionPoints* (OID 2.5.29.31) - contiene uno o più URL di accesso a CRL. L'URL configura un percorso assoluto per l'accesso alla CRL. L'estensione non è marcata critica;

e) *subjectKeyIdentifier* (OID 2.5.29.14) - contiene il valore *keyIdentifier* per identificare il certificato. L'estensione non è marcata critica.

2. Ulteriori estensioni possono essere inserite nel certificato purché conformi agli standard citati nella presente deliberazione e non marcate "critiche".

ART. 15

(Uso delle estensioni nei certificati di marcatura temporale)

1. I certificati di marcatura temporale devono contenere le seguenti estensioni:

a) *keyUsage* (OID 2.5.29.15) – contiene il valore *digitalSignature* (bit 0 impostato a 1). L'estensione è marcata critica;

b) *extendedKeyUsage* (OID 2.5.29.37) – contiene esclusivamente il campo *keyPurposeId=timeStamping*. L'estensione è marcata critica;

c) *certificatePolicies* OID 2.5.29.32) – contiene uno o più identificativi delle *policyIdentifier* e le URL del relativo CPS. L'estensione non è marcata critica;

d) *authorityKeyIdentifier* (OID 2.5.29.35) – contiene almeno il valore *keyIdentifier* corrispondente al *subjectKeyIdentifier* del certificato di certificazione utilizzato per sottoscrivere il certificato di marcatura temporale. L'estensione non è marcata critica;

e) *subjectKeyIdentifier* (OID 2.5.29.14) – contiene il valore *keyIdentifier* per identificare il certificato. L'estensione non è marcata critica.

2. Ulteriori estensioni possono essere inserite nel certificato purché conformemente agli standard citati nella presente deliberazione e non marcate "critiche".

TITOLO V

REGOLE PER LA VALIDAZIONE TEMPORALE

ART. 16

(Regole per i servizi di Validazione Temporale)

1. L'accesso al servizio di validazione temporale fornito dai certificatori avviene tramite il protocollo e il formato definiti nella specifica ETSI TS 101 861 V.1.2.1, recante "Profilo di Validazione Temporale" e nella specifica RFC 3161 e successive modificazioni. Le marche temporali inviate in risposta al richiedente seguono i medesimi standard.

2. I certificatori rendono disponibile o indicano un sistema che permetta l'apertura, l'analisi e la visualizzazione delle marche temporali di cui al comma 1. Detto sistema gestisce correttamente le strutture *TimeStampToken* e *TimeStampResp* almeno nel formato *detached*, con verifica della firma del sistema di validazione temporale e della corretta associazione, effettuata tramite la funzione di hash, con il documento per il quale è stata generata la marca temporale stessa.

3. L'estensione associata alla struttura *TimeStampToken* e *TimeStampResp* non deve influire sul corretto funzionamento del sistema di cui al comma 2.

4. I *TimeStampToken* devono includere un identificativo univoco della *policy* di sicurezza in base alla quale il token stesso è stato generato. Detto identificativo, ove non definito a livello nazionale od europeo, è definito e reso pubblico dal certificatore.

ART. 17

(Associazione di una marca temporale al documento sottoscritto)

1. Se al documento informatico viene apposta una sola firma, la marcatura temporale del documento sottoscritto in conformità al documento ETSI TS 101 733 (CAdES) deve essere conforme alle specifiche RFC 3161.
2. Se al documento informatico si devono applicare due o più firme e il tempo di apposizione di ciascuna firma è rilevante, il formato da utilizzare deve essere conforme al documento ETSI TS 101 733 (CAdES), alle specifiche RFC 3161.
3. Quando sia necessario attestare l'esistenza in un dato momento dell'intero documento sottoscritto con una o più firme digitali, il formato da utilizzare deve essere conforme alle specifiche RFC 5544.
4. Le estensioni dei file da utilizzare per i formati detached sono:
    a) TimeStampedData: .tsd;
    b) TimeStampResponse: .tsr;
    c) TimeStampToken : .tst.
5. La marcatura temporale del documento sottoscritto utilizzando il linguaggio XML deve essere realizzata mediante il formato XAdES-T descritto nel documento ETSI TS 101 903.
6. La marcatura temporale del documento sottoscritto utilizzando il formato PDF deve essere realizzata conformemente alle specifiche ETSI TS 102 778.

TITOLO VI

INFORMAZIONI SULLA REVOCA E SOSPENSIONE DEI CERTIFICATI

ART. 18

(Verifica dei certificati - CRL)

1. Le informazioni sulla revoca e sospensione dei certificati pubblicate in rete dai certificatori e rese disponibili pubblicamente tramite liste di revoca e sospensione, hanno un formato conforme alla specifica RFC 5280, capitolo 5, esclusi i paragrafi 5.2.4 e 5.2.6.
2. Le liste di certificati revocati e sospesi sono liberamente accessibili al pubblico tramite protocollo HTTP o LDAP.
3. I certificati revocati o sospesi devono permanere nella CRL, anche dopo la loro naturale scadenza, fino alla scadenza del relativo certificato di certificazione.
4. La revoca o sospensione dei certificati di sottoscrizione, richiesta o prevista dalle regole tecniche, deve essere effettuata entro ventiquattro ore dalla richiesta pervenuta.

ART. 19

(Verifica dei certificati - OCSP)

1. Fermo restando quanto prescritto dall'articolo 18, i certificatori hanno la facoltà di rendere disponibili le informazioni sulla revoca e sospensione dei certificati, anche attraverso servizi OCSP. In tal caso, detti servizi devono essere conformi alla specifica RFC 2560 e successive modificazioni.

ART. 20

(Coerenza delle informazioni sulla revoca e sospensione dei certificati)

1. Se un certificatore mette a disposizione diversi servizi per l'accesso alle informazioni sulla revoca o la sospensione dei certificati, o diversi URL di accesso allo stesso servizio, le informazioni ottenute accedendo con le diverse modalità devono essere coerenti, fatto salvo l'intervallo temporale strettamente necessario per l'allineamento. Tale intervallo temporale deve essere non superiore a sessanta secondi.

TITOLO VII

FORMATI DI SOTTOSCRIZIONE

ART. 21

(Busta crittografica di firma)

1. La busta crittografica destinata a contenere il documento informatico sottoscritto deve essere conforme, salvo i casi previsti dai commi 8 e 9, al documento ETSI TS 101 733 (CAdES) nella modalità denominata CAdES – BES.
2. La busta crittografica di cui al comma 1 deve essere di tipo *signedData* (OID: 1.2.840.113549.1.7.2).
3. Per la codifica della busta crittografica deve essere utilizzato il formato ASN.1 (ISO/IEC 8824) in rappresentazione binaria (ISO/IEC 8825, BER - DER) o alfanumerica ottenuta applicando la trasformazione BASE 64 (RFC 1421, RFC 2045). La testata e la coda previsti nelle specifiche RFC 1421 e RFC 2045 possono essere assenti.
4. Il documento da firmare deve essere imbustato nel formato originale, senza aggiunte in testa o in coda al formato stesso.
5. Il nome del *file* firmato, ossia della busta, deve assumere l'ulteriore estensione "p7m".
6. Le buste crittografiche di cui al comma 5 possono contenere a loro volta buste crittografiche. In questo caso deve essere applicata una ulteriore estensione "p7m".
7. L'eventuale presenza di attributi autenticati nella busta crittografica non è considerata critica. La gestione degli stessi non deve rappresentare un vincolo per le applicazioni di verifica di cui all'articolo 25.
8. Il CNIPA, con successive deliberazioni, stabilisce e rende noti, eventuali diversi formati di busta crittografica e formati di firma, riconosciuti a livello nazionale o internazionale, conformi a specifiche pubbliche (*Publicly Available Specification* – PAS).
9. Ai fini di cui al comma 8, il CNIPA può sottoscrivere specifici protocolli d'intesa al fine di rendere disponibili ulteriori formati di firma. Detti protocolli d'intesa devono contenere l'impegno del sottoscrittore ad assicurare:
    a) la disponibilità delle specifiche necessarie per lo sviluppo di prodotti di verifica o di generazione e eventuali librerie *software* necessarie per lo sviluppo di prodotti di verifica di firme digitali conformi al formato oggetto del protocollo d'intesa;
    b) l'assenza di qualunque onere finanziario a carico di chi sviluppa, distribuisce o utilizza i prodotti menzionati al comma 8;
    c) la disponibilità di ogni modifica inerente a quanto indicato alla lettera a) con un anticipo di almeno 90 giorni rispetto alla data di rilascio di nuove versioni del prodotto che realizza il formato di busta crittografica oggetto del protocollo d'intesa;

d) la disponibilità, a titolo gratuito per uso personale, di un prodotto per verificare firme digitali e per visualizzare il documento informatico del formato oggetto del protocollo d'intesa;

e) l'utilizzo, nel prodotto di verifica di cui al comma 8, delle informazioni contenute nell'elenco pubblico dei certificatori di cui all'articolo 39 e nelle liste di revoca di cui all'articolo 30, delle regole tecniche.

10. Fermo restando il rispetto delle condizioni previste al comma 9, il CNIPA, consultando preventivamente le Autorità di settore e le associazioni di categoria maggiormente rappresentative, valuta le richieste di sottoscrizione dei protocolli d'intesa previsti dal comma sopra citato avendo riguardo:

    a) alla rilevanza delle esigenze che con il protocollo sia possibile soddisfare;

    b) alla capacità di assicurare idoneo supporto e adeguata diffusione a livello nazionale ed internazionale ai prodotti di cui si tratta, che devono essere riconosciuti ed accettati quali standard di riferimento;

    c) alla necessità di evitare effetti negativi sulla interoperabilità.

11. Le pubbliche amministrazioni possono accettare documenti informatici sottoscritti con i formati di firma di cui ai commi 8 e 9 e, nel caso ritengano opportuno accettare uno o più di detti formati, dovranno farne apposita menzione nei procedimenti amministrativi cui si applicano e comunicarlo al CNIPA. Le pubbliche amministrazioni garantiscono la gestione del formato di cui al comma 1.

12. Il soggetto che sottoscrive il protocollo d'intesa di cui al comma 9 deve indicare al CNIPA gli indirizzi *internet* dove è possibile ottenere, gratuitamente e liberamente, quanto indicato alle lettere a) e d) del medesimo comma 9,

13. Il CNIPA rende disponibili sul proprio sito *internet*: l'elenco dei formati oggetto di protocolli d'intesa, gli indirizzi *internet* di cui al comma 12 e gli eventuali formati di busta crittografica di cui al comma 8.

14. In caso di inadempienza da parte del sottoscrittore del protocollo d'intesa di quanto previsto ai commi 9 e 12, il CNIPA, previa tempestiva informazione del soggetto interessato, risolverà il protocollo d'intesa dandone pubblicità nell'elenco di cui al comma 13 e ne informa le pubbliche amministrazioni di cui al comma 11.

15. Ai sensi del comma 8, con la presente deliberazione, sono riconosciuti il formato di busta crittografica e di firma descritti nello standard ISO/IEC 32000 – Portable Document Format (PDF) sviluppati in conformità alle specifiche ETSI TS 102 778 - PAdES.

16. Ai sensi del comma 8, sono altresì riconosciuti il formato di busta crittografica e di firma descritti nei documenti ETSI TS 101 903 – XAdES (versione 1.4.1) e ETSI TS 102 904 (versione 1.1.1).

ART. 22

(Busta crittografica di firma XML)

1. La sottoscrizione in linguaggio XML di cui all'Art. 21, comma 16, è conforme, salvo diversa esplicita indicazione, alla specifica RFC 3275.

2. Le modalità di imbustamento consentite, salvo diversa esplicita indicazione, sono, alternativamente:

    a) Enveloped
    http://www.w3.org/TR/xmldsig-core/#def-SignatureEnveloped

    b) Enveloping
    http://www.w3.org/TR/xmldsig-core/#def-SignatureEnveloping

    c) Detached
    http://www.w3.org/TR/xmldsig-core/#def-SignatureDetached

3. L’elemento Manifest definito nel paragrafo 5.1 della specifica RFC 3275 non deve essere utilizzato.

ART. 23

(Regole per l’utilizzo dello XAdES)

1. Devono essere garantiti i seguenti requisiti minimi:
    a) la generazione della firma deve supportare il formato XAdES-BES;
    b) la generazione della firma può supportare i formati XAdES-T, XAdES-A purché questi non racchiudano una busta XAdES-EPES;
    c) la verifica della firma deve supportare il formato XAdES-BES e XAdES-A purché questa non racchiuda una busta XAdES-EPES.

ART. 24

(Regole per l’apposizione di firme multiple)

1. Una stessa busta crittografica può contenere più firme digitali. Queste ultime sono identificate in:
    a) “Firme parallele”, in tal caso il sottoscrittore, utilizzando la propria chiave privata, firma solo i dati contenuti nella busta stessa (OID: 1.2.840.113549.1.7.1);
    b) “Controfirme”, in tal caso il sottoscrittore, utilizzando la propria chiave privata, firma una precedente firma (OID: 1.2.840.113549.1.9.6) apposta da altro sottoscrittore.
2. Il formato delle firme multiple definite nel presente articolo è conforme al documento ETSI TS 101 733 nella modalità BES.
3. L’apposizione di firme multiple di cui al presente articolo non comporta l’applicazione di ulteriori estensioni al nome del file contenente il documento firmato.

TITOLO VIII

APPLICAZIONI DI VERIFICA DELLA FIRMA

ART. 25

(Applicazioni di verifica)

1. I certificatori accreditati, che rilasciano strumenti per la sottoscrizione nei formati previsti dalla presente deliberazione, devono fornire ovvero indicare come stabilito nell’articolo 10, comma 1 delle regole tecniche, almeno un sistema che consenta di effettuare la verifica della sottoscrizione stessa.

ART. 26

(Regole per la verifica di firme multiple)

1. Le procedure di verifica di sottoscrizioni che utilizzano firme multiple devono gestire almeno:
    1) cinque firme parallele e due livelli di controfirma;
    2) cinque controfirme distinte per ogni sottoscrizione;
    3) una controfirma apposta ad una controfirma.

ART. 27

(Requisiti delle applicazioni di apposizione e verifica)

1. Le applicazioni di verifica della firma digitale indicate o distribuite dai certificatori accreditati, ai sensi dell'articolo 10 delle regole tecniche, oltre a gestire correttamente i certificati elettronici il cui formato è stabilito nella presente deliberazione, riconoscono i seguenti elementi dei certificati qualificati:
    a) l'attributo *DateOfBirth* dell'estensione *SubjectDirectoryAttributes*;
    b) le seguenti *qcStatements*:
        1) *id-etsi-qcs-QcCompliance* (OID: 0.4.0.1862.1.1);
        2) *id-etsi-qcs-QcLimitValue* (OID: 0.4.0.1862.1.2);
        3) *id-etsi-qcs-QcRetentionPeriod* (OID: 0.4.0.1862.1.3);
        4) *id-etsi-qcs-QcSSCD* (OID: 0.4.0.1862.1.4).
2. Oltre a quanto prescritto al precedente comma 1, le applicazioni di verifica della firma digitale indicate o distribuite dai certificatori accreditati gestiscono i formati di firma e le buste crittografiche di cui all'articolo 21, commi da 1 a 7 e 16, e all'articolo 17, commi 1,2 e 3 e all'articolo 24.
3. Le applicazioni di verifica della firma digitale indicate o distribuite dai certificatori accreditati, ai sensi dell'articolo 10 delle regole tecniche, devono consentire all'utente di verificare la validità della firma nel periodo di vigenza del corrispondente certificato. Ciò al fine di verificare, ai sensi dell'articolo 51 delle regole tecniche, la validità della firma digitale nel tempo. Tale verifica deve essere presentata all'utente indicando le informazioni temporali utilizzate per la verifica stessa.
4. Le applicazioni di cui al presente articolo gestiscono correttamente il processo di verifica delle firme digitali prodotte fino all'entrata in vigore della presente deliberazione che non perdono la loro specifica validità.

TITOLO IX

DISPOSIZIONI FINALI E TRANSITORIE

ART. 28

(Guide tecniche)

1. Sul sito istituzionale del CNIPA saranno pubblicate e, periodicamente aggiornate, guide tecniche di riferimento che forniranno indicazioni pratiche in merito alle modalità di utilizzo della firma digitale in specifici contesti rilevati nella prassi attuativa, anche a seguito delle segnalazioni eventualmente pervenute.

ART. 29

(Norme transitorie)

1. La presente deliberazione entra in vigore dalla data di pubblicazione sulla Gazzetta Ufficiale della Repubblica Italiana.
2. I certificati elettronici emessi precedentemente all'entrata in vigore della presente deliberazione rimangono validi fino alla scadenza prevista al momento dell'emissione, salva eventuale revoca o sospensione.
3. L'articolo 4, commi 1 e 2, l'articolo 5, l'articolo 17 e l'articolo 21, comma 1, devono essere applicati dopo duecentosettanta giorni dall'entrata in vigore della presente deliberazione. Fino a tale data

continuano ad applicarsi le previsioni in merito contenute nelle deliberazioni del CNIPA 17 febbraio 2005, n. 4 e 18 maggio 2006, n. 34.

4. L'applicazione del comma precedente può essere anticipata fino a novanta giorni rispetto ai termini stabiliti nel medesimo comma, nei casi in cui non è possibile una diffusione tempestiva delle applicazioni a causa della complessità delle attività connesse. Al fine di non creare problemi di interoperabilità, tale anticipazione è consentita solo nell'ambito di attività relative al medesimo procedimento.
5. Le marche temporali e le CRL emesse precedentemente all'entrata in vigore della presente deliberazione sono valide ed efficaci per l'intervallo di tempo previsto.

ART. 30

(Abrogazioni)

1. La presente deliberazione abroga la circolare dell'Autorità per l'informatica nella pubblica amministrazione 19 giugno 2000, n. 24 e, fatto salvo quanto previsto dall'articolo 29, comma 3, le deliberazioni del CNIPA 17 febbraio 2005, n. 4 e 18 maggio 2006, n. 34.

Il presidente Pistella