DELIBERAZIONE 17 febbraio 2005

Regole per il riconoscimento e la verifica del documento informatico.
(Deliberazione n. 4/2005).
(GU n. 51 del 3-3-2005)

DISPOSIZIONI GENERALI

IL COLLEGIO

Visto il decreto legislativo 12 febbraio 1993, n. 39, così come modificato dall'art. 176, comma 3, del decreto legislativo 30 giugno 2003, n. 196;
Visto il decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, recante testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa;
Visto il decreto legislativo 23 gennaio 2002, n. 10, recante attuazione della direttiva 1999/93/CE, relativa ad un quadro comunitario per le firme elettroniche;
Visto l'art. 40, comma 4, del decreto del Presidente del Consiglio dei Ministri 13 gennaio 2004;

Delibera

di emanare le seguenti regole per il riconoscimento e la verifica del documento informatico.

Art. 1.
Definizioni

1. Fatte salve le definizioni contenute negli articoli 1 e 22 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, e successive modificazioni, ai fini delle presenti regole si intende per:

a) testo unico, il testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa, emanato con decreto del Presidente della Repubblica 28 dicembre 2000, n. 445;

b) regole tecniche, le regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici emanate con decreto del Presidente del Consiglio dei Ministri 13 gennaio 2004 pubblicate nella Gazzetta Ufficiale 27 aprile 2004, n. 98;

c) firme multiple, firme digitali apposte da diversi sottoscrittori allo stesso documento;

d) campo, unità informativa contenuta nel certificato. Può essere composta da diverse unità informative elementari dette «attributi»;

e) estensione, metodo utilizzato per associare specifiche informazioni (attributi) alla chiave pubblica contenuta nel certificato, utilizzata per fornire ulteriori informazioni sul titolare del certificato e per gestire la gerarchia di certificazione;

f) attributo, informazione elementare contenuta in un campo di un certificato elettronico come un nome, un numero o una data;

g) attributi autenticati, insieme di attributi sottoscritti con firma elettronica dal sottoscrittore;

h) marcatura critica, caratteristica che possono assumere le estensioni conformemente allo standard RFC 3280;

i) marca temporale, un'evidenza informatica che consente la validazione temporale;

l) OID (Object Identifier), codice numerico standard per l'identificazione univoca di evidenze informatiche utilizzate per la rappresentazione delle strutture di dati nell'ambito degli standard internazionali relativi alla interconnessione dei sistemi aperti;

m) 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);

n) ETSI (European Telecommunications Standards Institute), organizzazione indipendente, no profit, la cui missione è produrre standard sulle telecomunicazioni. E' ufficialmente responsabile per la creazione di standard in Europa;

o) HTTP (Hypertext Transfer Protocol), protocollo per il trasferimento di pagine ipertestuali e risorse in rete conforme allo standard RFC 2616 e successive modificazioni;

p) LDAP (Lightweight Directory Access Protocol), protocollo di rete utilizzato per rendere accessibili informazioni in rete conforme allo standard RFC 3494 e successive modificazioni.

Art. 2.
Ambito di applicazione e contenuto

1. La presente deliberazione stabilisce, ai sensi dell'art. 40, comma 4 delle regole tecniche, le regole per il riconoscimento e la verifica del documento informatico cui i certificatori accreditati devono attenersi al fine di ottenere e mantenere il riconoscimento di cui all'art. 28, comma 1 del testo unico.

2. Le disposizioni di cui al titolo II definiscono il formato dei certificati qualificati e le informazioni che in essi devono essere contenute.

3. Le disposizioni di cui al titolo III definiscono il formato dei certificati elettronici di certificazione e le informazioni che in essi devono essere contenute, generati ai sensi dell'art. 13, comma 2, delle regole tecniche, e il formato dei certificati elettronici di marcatura temporale e le informazioni che in essi devono essere contenute.

4. Le disposizioni di cui al titolo IV definiscono 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.

5. Le disposizioni di cui al titolo V definiscono i formati e le modalità di accesso alle informazioni sulla revoca e la sospensione dei certificati, ai sensi dell'art. 29, comma 1, delle regole tecniche.

6. Le disposizioni di cui al titolo VI definiscono i formati delle buste crittografiche destinate a contenere gli oggetti sottoscritti con firma digitale.

7. Le disposizioni di cui al titolo VII definiscono i requisiti delle applicazioni di verifica della firma digitale di cui all'art. 10 delle regole tecniche.

PROFILO DEI CERTIFICATI QUALIFICATI

Art. 3.
Norme generali

1. Il profilo dei certificati è, se non diversamente indicato, conforme alla specifica RFC 3280, capitolo 4, recante «Profilo dei certificati e delle liste di revoca dei certificati nell'infrastruttura a chiave pubblica» e, se non diversamente

indicato, conforme alla specifica ETSI TS 101 862 V1.3.2, recante «Profilo dei certificati qualificati».

PROFILO DEI CERTIFICATI DI CERTIFICAZIONE E MARCATURA TEMPORALE

Art. 5.
Profilo dei certificati di certificazione e marcatura temporale

1. Se non diversamente previsto, il profilo dei certificati è conforme alla specifica RFC 3280.

Art. 6.
Uso delle estensioni nei certificati di certificazione

1. I certificati di certificazione contengono 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 relative URL del CPS. Può contenere l'OID generico previsto dall'RFC 3280 (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/CSL. 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. L'estensione non è marcata critica.

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

Art. 7.
Uso delle estensioni nei certificati di marcatura temporale

1. I certificati di marcatura temporale contengono 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 il valore keyPurposeId=timeStamping. L'estensione è marcata critica;

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

d) authorityKeyIdentifier (OID 2.5.29.35), contiene almeno un keyIdentifier. L'estensione non è marcata critica;

e) subjectKeyIdentifier (OID 2.5.29.14), contiene almeno un keyIdentifier. L'estensione non è marcata critica.

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

REGOLE PER LA VALIDAZIONE TEMPORALE

Art. 8.
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 di 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, se non definito a livello nazionale od europeo, è definito e reso pubblico dal certificatore.

INFORMAZIONI SULLA REVOCA E SOSPENSIONE DEI CERTIFICATI

Art. 9.
Verifica dei certificati - CRL

1. Le informazioni sulla revoca e sospensione dei certificati, pubblicate dai certificatori e disponibili pubblicamente tramite liste di revoca e sospensione, hanno un formato conforme alla specifica RFC 3280, capitolo 5, esclusi i paragrafi 5.2.4 e 5.2.6.

2. Le liste di certificati revocati e sospesi sono accessibili al pubblico tramite protocollo HTTP o LDAP.

Art. 10.
Verifica in tempo reale dei certificati - OCSP

1. Fermo restando quanto prescritto dall'art. 9, 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 alle specifica RFC 2560 e successive modificazioni.

Art. 11.
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 se ciò è compatibile con la tecnologia utilizzata.

FORMATI DI FIRMA

Art. 12.
Busta crittografica di firma

1. La busta crittografica destinata a contenere l'oggetto sottoscritto è conforme, salvo i casi previsti dai commi 8 e 9, alla specifica RFC 2315 (PKCS7 ver. 1.5).

2. La busta crittografica di cui al comma 1 è di tipo signedData (OID: 1.2.840.113549.1.7.2).

3. Per la codifica della busta crittografica possono essere utilizzati i formati ASN.1-DER (ISO 8824, 8825) o BASE64 (RFC 1421).

4. Il documento da firmare è imbustato nel formato originale, senza aggiunte in testa o in coda al formato stesso.

5. Il nome del file firmato, ossia della busta, assume l'ulteriore estensione «p7m».

6. Le buste crittografiche di cui al comma 5 possono contenere a loro volta buste crittografiche. In questo caso è 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'art. 14.

8. Il CNIPA Può stabilire, con apposito provvedimento, ulteriori formati standard di busta crittografica, riconosciuti a livello nazionale o internazionale, conformi a specifiche pubbliche (Publicly Available Specification-PAS).

9. 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 precedente;

c) la disponibilità di ogni modifica inerente a quanto indicato alla lettera a) con un anticipo di almeno 90 giorni rispetto alla data del rilascio di nuove versioni del prodotto che implementa 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 del formato oggetto del protocollo d'intesa e visualizzare il documento informatico oggetto della sottoscrizione;

e) la capacità di utilizzare le informazioni contenute nell'elenco pubblico dei certificatori di cui all'art. 41 delle regole tecniche e nelle liste di revoca di cui all'art. 29 del citato provvedimento nel prodotto di verifica di cui al comma precedente.

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 essi consentono di soddisfare;

b) alla possibilità di assicurare un idoneo supporto e un'adeguata diffusione sul mercato nazionale ed internazionale dei prodotti che realizzano la struttura informatica del documento sottoscritto, tali da 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 indica 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 informa tempestivamente il soggetto interessato e, nel caso lo stesso non ottemperi rapidamente alla piena osservanza di quanto previsto, revoca il protocollo d'intesa dandone pubblicità nell'elenco di cui al comma 13 ed informandone tempestivamente le pubbliche amministrazioni di cui al comma 11.

Art. 13.

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 alla specifica RFC 2315.

3. L'apposizione di firme multiple di cui al presente articolo non comporta l'applicazione di ulteriori estensioni al file firmato, oltre alla prima.

APPLICAZIONI DI VERIFICA DELLA FIRMA

Art. 14.

Requisiti delle applicazioni di verifica

1. Le applicazioni di verifica della firma digitale indicate o distribuite dai certificatori accreditati, ai sensi dell'art. 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'art. 12, commi da 1 a 7, e all'art. 13.

3. Le applicazioni di cui al presente articolo gestiscono correttamente il processo di verifica delle firme digitali prodotte precedentemente all'entrata in vigore della presente deliberazione che non perdono la loro specifica validità.

DISPOSIZIONI FINALI E TRANSITORIE

Art. 15.
Operatività

1. La presente deliberazione entra in vigore a decorrere da nove mesi dalla data di pubblicazione nella Gazzetta Ufficiale.

2. L'obbligo di utilizzo della codifica UTF-8, previsto nella RFC 3280, ha effetto a decorrere da nove mesi dall'entrata in vigore della presente deliberazione.

3. L'obbligo di cui all'art. 4, comma 5, lettera f) ha effetto a decorrere da nove mesi dall'entrata in vigore della presente deliberazione. Fino a tale data, se il certificato non contiene nell'estensione qcStatement i valori id-etsi-qcs-QcCompliance e id-etsi-qcs-QcSSCD, almeno una delle policy indicate nel certificato indica esplicitamente che il certificato è un certificato qualificato e che la chiave privata, corrispondente alla chiave pubblica presente nel certificato qualificato, è memorizzata su un dispositivo sicuro per la generazione della firma conforme alle normative vigenti.

4. Durante il periodo di proroga di cui al comma 3, se il certificato non contiene nell'estensione qcStatement il valore id-etsi-qcs-QcLimitValue, gli eventuali limiti di negoziazione sono inseriti nell'attributo explicitText del campo userNotice.

5. Le disposizioni di cui all'art. 14 hanno effetto a decorrere da nove mesi dall'entrata in vigore della presente deliberazione.

6. I certificati elettronici emessi precedentemente all'entrata in vigore della presente deliberazione rimangono validi fino alla scadenza prevista al momento dell'emissione, salvo precedente revoca o sospensione.

Roma, 17 febbraio 2005

Il presidente: Zoffoli