Allegato alla deliberazione n. 34/2006

REGOLE TECNICHE PER LA DEFINIZIONE DEL PROFILO DI BUSTA CRITTOGRAFICA PER LA FIRMA DIGITALE IN LINGUAGGIO XML

Sommario

1 Definizioni

1. Fatte salve le definizioni contenute nell' articolo 1 del decreto legislativo 7 marzo 2005, n. 82, e successive modificazioni, ai fini delle presenti regole si intende per:
   a) 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 sulla G.U. 27 aprile 2004, n.98;
   b) FIRME MULTIPLE, firme digitali apposte da diversi sottoscrittori allo stesso documento;
   c) CAMPO, unità informativa contenuta nel certificato. Può essere composta da diverse unità informative elementari dette "attributi";
   d) ESTENSIONE, metodo utilizzato per associare specifiche informazioni (attributi) alla chiave pubblica contenuta nel certificato allo scopo di fornire ulteriori informazioni sul titolare del certificato e per gestire la gerarchia di certificazione;
   e) ATTRIBUTO, informazione elementare contenuta in un campo di un certificato elettronico, come un nome, un numero o una data;
   f) MARCA TEMPORALE, un'evidenza informatica che consente la validazione temporale;
   l) 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);
   m) 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;
   n) HTTP, (Hypertext Transfer Protocol) protocollo per il trasferimento di pagine ipertestuali e risorse in rete conforme allo standard RFC 2616 e successive modificazioni;
   o) TAG, un elemento inserito nel file XML che specifica come una porzione di documento debba essere elaborata;
   p) W3C, (World Wide Web Consortium), un consorzio internazionale di compagnie che operano in Internet e con il Web, con lo scopo di sviluppare standard aperti per l'evoluzione del Web;
   q) TSP, (Time Stamp Provider), il componente o il server che fornisce il servizio di marcatura temporale;
   r) XML, (eXtended Markup Language) insieme di regole per strutturare in formato testo i dati oggetto di elaborazione.

2 XML – Sintassi e elaborazione delle sottoscrizioni

In questo capitolo vengono selezionate le tipologie di firme XML e gli algoritmi da utilizzare nell'ambito delle possibilità offerte dalla specifica RFC 3275.

Le buste crittografiche devono essere, ove non diversamente indicato, conformi a tale specifica.

2.1 Tipologie di firme

Le XML Signature si presentano in tre forme base di modalità di imbustamento:

1. Enveloped
   http://www.w3.org/TR/xmldsig-core/#def-SignatureEnveloped
2. Enveloping
   http://www.w3.org/TR/xmldsig-core/#def-SignatureEnveloping
3. Detached
   http://www.w3.org/TR/xmldsig-core/#def-SignatureDetached

L'utilizzo della modalità *Enveloped* può presentare problemi implementativi nel caso di apposizione di firme successive. Per tale motivo, quando viene utilizzata tale modalità, deve essere utilizzata la trasformazione descritta nel paragrafo 2.5.2 del presente documento.

Le applicazioni di apposizione della firma possono quindi realizzare le buste crittografiche in una qualsiasi delle modalità consentite. Conseguentemente, le applicazioni di verifica devono essere in grado di verificare le firme in una qualsiasi di queste modalità, fatte salve le caratteristiche, in termini di algoritmi e trasformazioni, definite nel seguito.

Nel caso si utilizzi la modalità *Detached*, le applicazioni di verifica conformi al presente profilo devono assicurare la corretta apertura delle buste crittografiche nel caso gli oggetti firmati siano contenuti nello stesso file che contiene la firma (elemento signature).

Gli elementi Manifest e SignatureProperties di cui al paragrafo 5.1 della specifica RFC 3275 non devono essere utilizzati.

Per consentire la visualizzazione da parte dell'applicazione di verifica dei dati precedentemente firmati, le applicazioni di firma devono valorizzare, nel caso di busta *Enveloping*, l'attributo MimeType e l'attributo Encoding dell'elemento <Object.>. Negli altri casi devono identificare il MimeType dei dati che si stanno firmando utilizzando un apposito attributo.

2.2 Algoritmo di digest

La funzione di *hash* che le applicazioni di firma devono specificare e, quindi, applicare all'oggetto da firmare è la funzione SHA-1 (ISO/IEC 10118-3:1998).
L'URI che deve essere indicata nell'attributo *Algorithm* dell'elemento *DigestMethod* è:

http://www.w3.org/2000/09/xmldsig#sha1

Le applicazioni di verifica devono gestire almeno questo algoritmo.

2.3 Algoritmo di signature

L'algoritmo per la generazione e la validazione della firma digitale (*SignatureValue*) che le applicazioni di firma devono specificare e, quindi, applicare all'elemento *SignedInfo* è l'algoritmo RSA-SHA1.

L'URI che deve essere indicata nell'attributo *Algorithm* dell'elemento *SignatureMethod* è:

http://www.w3.org/2000/09/xmldsig#rsa-sha1

Le applicazioni di verifica devono gestire almeno questo algoritmo.

2.4 Algoritmi di canonicalizzazione

L'applicazione di firma può usare quale algoritmo di canonicalizzazione dell'elemento *SignedInfo* uno tra quelli identificati dalle URI seguenti:

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

Questa URI deve essere riportata nell'attributo *Algorithm* dell'elemento *CanonicalizationMethod.*

Le applicazioni di verifica devono gestire almeno questi algoritmi di canonicalizzazione.

2.5 Algoritmi di trasformazione

I paragrafi seguenti riportano l'insieme minimo di trasformazioni che le applicazioni di verifica devono essere in grado di gestire.

L'URI che identifica la trasformazione, come specificato nella specifica RFC 3275, deve essere riportata nell'attributo *Algorithm* dell'elemento *Transform.*

2.5.1 Base 64

L'URI che rappresenta questa trasformazione è:

http://www.w3.org/2000/09/xmldsig#base64

2.5.2 Enveloped Signature

Nella modalità *enveloped*, è necessario assicurare che tutte le firme successive alla prima vengano applicate sugli stessi dati sui quali è stata calcolata la prima firma, il che non accade in modo automatico; pertanto, si deve fare in modo che siano gestite opportunamente le strutture *ds:Signature* dai dati originali, sia in fase di generazione che in fase di verifica della firma.

La soluzione consiste nell'uso di una opportuna trasformazione XPath da specificare nel tag <*ds:Transforms*> all'interno del tag <*ds:SignedInfo*>.

La trasformazione seguente si basa sulla sintassi descritta nella raccomandazione XPath Filter 2.0 pubblicata dal W3C all'indirizzo http://www.w3.org/2002/06/xmldsig-filter2 (cfr. anche la sintassi XPath v2.0 definita in http://www.w3.org/TR/xpath20). Il filtro proposto elimina, dai dati sottoposti a firma, tutti gli elementi di tipo *ds:Signature* all'interno del documento XML, a partire dal nodo root (escluso) a scendere.

```
<ds:SignedInfo>
        <ds:CanonicalizationMethod
                Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315" />
        <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />
        <ds:Reference URI="">
                <ds:Transforms>
                        <ds:Transform Algorithm="http://www.w3.org/2002/06/xmldsig-filter2">
                                <dsig-xpath:XPath Filter="subtract"
                                                xmlns="http://www.w3.org/2002/06/xmldsig-filter2">
                                        /descendant::ds:Signature
                                </dsig-xpath:XPath>
                        </ds:Transform>
                        <ds:Transform Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315" />
                </ds:Transforms>
                <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"  />
                <ds:DigestValue >f/Rcq6wu9gORMioxAxaof7pZux8=</ds:DigestValue>
        </ds:Reference>
</ds:SignedInfo>
```

Le applicazioni di firma e di verifica devono supportare la trasformazione sopra descritta.

2.5.3 Xpath

L'URI che rappresenta questa trasformazione è:

http://www.w3.org/TR/2002/REC-xmldsig-filter2-20021108/

2.5.4 XSLT

L'URI che rappresenta questa trasformazione è:

http://www.w3.org/TR/1999/REC-xslt-19991116

Questa trasformazione va sempre seguita dalla canonicalizzazione.

Il foglio di stile utilizzato deve essere incluso nel file firmato.

Poiché, in fase di verifica, è necessario che l'utente disponga del documento che è stato firmato, i meccanismi automatici di verifica e utilizzo dei dati firmati devono prelevarli dal documento trasformato e non dal file XML precedente alla trasformazione. Tale obbligo deve essere rispettato anche per la canonicalizzazione.

2.5.5 Canonicalizzazione

L'URI che rappresenta questa trasformazione è:

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

oppure

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

L'uso della canonicalizzazione è obbligatorio dopo ogni trasformazione XSLT.

2.6 KeyInfo

L'elemento KeyInfo, opzionale nella RFC 3275, deve essere sempre presente nella busta crittografica.

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 firmatario.

L' applicazione di verifica deve gestire almeno l'elemento *X509Data.*

L'applicazione di verifica deve utilizzare il certificato contenuto nella busta per le operazioni di verifica della firma.

3. XML Advanced Electronic Signatures (XAdES)

Con riferimento alla specifica ETSI TS 101 903 V1.2.2 (2004-04) XadES le applicazioni di verifica devono gestire i formati XAdES-BES e XAdES-T come indicato nei paragrafi successivi.

3.1 XAdES-BES

Il formato di firma XAdES-BES è descritta nel capitolo 4.4.1 della specifica ETSI TS 101 903 V1.2.2 (2004-04) XadES.
Le applicazioni conformi al presente profilo devono gestire un elemento *ds:object* nel modo seguente:

```
<ds:Signature ID>
.....
<ds:Object>
        <QualifyingProperties>
                <SignedProperties>
                        <SignedSignatureProperties>
                                (SigningTime)?
                        </SignedSignatureProperties>
                </SignedProperties>
                <UnsignedProperties>
                        <UnsignedSignatureProperties>
                                (CounterSignature)*
                        </UnsignedSignatureProperties>
                </UnsignedProperties>
        </QualifyingProperties>
</ds:Object>
....
</ds:Signature >
```

- *l'elemento ds:Object* deve contenere un solo elemento figlio *QualifyingProperties* (*direct incorporation*);
- la firma deve essere apposta all'oggetto da firmare e ai suoi attributi firmati se presenti; nell'elemento *ds:signature* va aggiunto un *ds:reference* per l'elemento *SignedProperties.*

L'elemento *SigningTime* specifica il momento in cui il firmatario termina il processo di firma. Questo elemento deve essere firmato.

L'elemento *CounterSignature* (controfirma) indica la firma applicata ad un'altra firma. Sostanzialmente il *CounterSignature* contiene un nuovo elemento *Signature* il cui *Reference* è l'elemento *ds:SignatureValue* dell'elemento padre *ds:Signature*.
Questa proprietà non deve essere firmata.

La sintassi dell'elemento *QualifyingProperties* è descritta nel capitolo 6 della specifica ETSI TS 101 903 V1.2.2 (2004-04) XadES .

La sintassi dei suoi attributi è descritta nel capitolo 7.2 della medesima specifica.

3.2 Associazione di una Marca Temporale alla firma

La marca temporale è ottenuta inviando un'impronta di un documento ad un TSP che firma con un certificato emesso da una TSA (Time Stamping Authority) di cui ha disponibilità un certificatore accreditato iscritto nell'elenco pubblico tenuto dal Centro nazionale per l'informatica nella pubblica amministrazione.

Il risultato (TimeStampToken) è un oggetto di tipo *signed-data* ottenuto firmando l'hash + alcuni altre informazioni tra cui la data e ora secondo la specifica RFC 3161.

Quella che intendiamo prendere in considerazione è la marcatura della sola firma. Questa. viene inserita tra gli attributi qualificati non firmati. Il formato che descrive il requisito è lo XAdES-T.

3.2.1 XAdES-T

Il formato di firma XAdES-T è descritta nel capitolo 4.4.3.1 di ETSI TS 101 903 V1.2.2 (2004-04) XadES.

Le applicazioni conformi al presente profilo devono gestire un elemento *ds:object* nel modo seguente:

```
<ds:Signature ID>
......
<ds:Object>
        <QualifyingProperties>

                <SignedProperties>
                        <SignedSignatureProperties>
                                (SigningTime)?
                        </SignedSignatureProperties>
                </SignedProperties>

                <UnsignedProperties>
                        <UnsignedSignatureProperties>
                                (CounterSignature)*
                                (SignatureTimeStamp)+
                        </UnsignedSignatureProperties>
                </UnsignedProperties>

        </QualifyingProperties>
</ds:Object>
....
</ds:Signature >
```

L'elemento *SignatureTimeStamp* deve contenere contiene il time-stamp calcolato sull'elemento *ds:SignatureValue.*

Il tipo previsto per l'elemento *SignatureTimeStamp* è il *TimeStampType*, l'applicazione deve prevedere un elemento *Include* con un URI relativo al *ds:SignatureValue* che viene marcato come descritto nel par. 7.3 della specifica ETSI TS 101 903 V1.2.2 (2004-04) XadES.

L'elemento *SignatureTimeStamp* non deve essere un attributo firmato.

4 Firme multiple

4.1 Firme Multiple congiunte (parallele)

La realizzazione delle firme multiple congiunte (altrimenti dette contestuali o parallele) sono caratterizzate dal fatto che esse sono apposte in modo indipendente sugli stessi dati di partenza.

Nel caso particolare di XML Signature possiamo evidenziare che:

1. all'elemento *Signature* corrisponde una sola firma e quindi un solo firmatario
2. gli elementi *Reference* che individuano il documento, ovvero i documenti, firmati, sono contenuti nell'elemento *Signature* e contengono anche il DigestValue di ciascuno di essi.

L'attributo *Signature ID* deve essere valorizzato e deve essere univoco per ciascun firmatario.

Se la busta di partenza contiene una firma *enveloping*, le firme successive devono essere apposte in modalità *detached* facendo riferimento ai dati firmati nella busta di partenza presenti nel tag object. Si riporta di seguito un esempio.

```
<?xml version="1.0" encoding="UTF-8"?>
<Envelope>
<Signature Id="Signer-1" xmlns="http://www.w3.org/2000/09/xmldsig#">
        <SignedInfo>
                <CanonicalizationMethod ....."/>
                <SignatureMethod ....."/>
                <Reference URI="#Object1" Type="http://www.w3.org/2000/09xmldsig#object"
                        <DigestMethod ..."/>
                        <DigestValue>....</DigestValue>
                </Reference>
        </SignedInfo>
        <SignatureValue>....</SignatureValue>
        <KeyInfo>  .....  </KeyInfo>
  <Object Id=Object1>
        <data> ... </data>
 </ Object>
 </ Signature>
< Signature Id="Signer-2" xmlns:dsig="http://www.w3.org/2000/09/xmldsig#">
        <SignedInfo>
                <CanonicalizationMethod ....."/>
                <SignatureMethod ....."/>
                <Reference URI="#Object1>
                        <DigestMethod ..."/>
                        <DigestValue>....</DigestValue>
                </Reference>
        </SignedInfo>
        <SignatureValue>....</SignatureValue>
        <KeyInfo>  .....  </KeyInfo>
</ Signature></Envelope>
```

Se la busta di partenza contiene un firma XML in modalità *detached*, le firme seguenti devono essere apposte utilizzando ancora la modalità *detached* facendo riferimento ai dati referenziati dal primo firmatario.

Se la busta crittografica di partenza contiene una firma XML in modalità *enveloped*, le firme seguenti devono essere apposte utilizzando ancora la modalità *enveloped*.

4.2 ControFirme

Le controfirme devono utilizzare quanto stabilito nel paragrafo 31 della specifica ETSI TS 101 903 V1.2.2 (2004-04) XadES.