FIRMA DIGITALE – SPECIFICHE TECNICHE

1 ABBREVIAZIONI E TERMINI

- XML: eXtensible Markup Language
- SHA: Secure Hash Algorithm
- XAdES: XML Advanced Electronic Signature

2 INTRODUZIONE

Scopo del documento è la descrizione delle specifiche tecniche inerenti la firma digitale adottata per i documenti CDA nell'ambito del progetto Medir. Quanto proposto rientra nell'adozione dello standard XML Digital Signature (http://www.w3.org/TR/xmldsig-core/) a cui si riferisce la normativa sulla firma digitale deliberazione CNIPA, e all'adozione dello standard XAdES-BES (XML Advanced Electronic Signature) come stabilito dalla deliberazione CNIPA 45 del 9 novembre 2009.

La firma digitale può riferire a una trasformazione XSLT, e cioè a un foglio di stile per la renderizzazione pre-firma del documento CDA, ottenendo in tal modo una firma del tipo "ciò che si vede".

3 LA NORMATIVA SULLA FIRMA DIGITALE

Nella definizione per l'implementazione della firma digitale dei documenti CDA in MEDIR, si può fare riferimento a

- Specifiche XML Digital Signature (http://www.w3.org/TR/xmldsig-core/)
- Best Practices per la firma XML riportate in (http://www.w3.org/TR/xmldsig-bestpractices/) nonché
- Deliberazione CNIPA n.34 18 maggio 2006 per le trasformazioni XSLT
- Specifiche XAdES-BES - ETSI TS 101 903 V1.4.2
- Deliberazione CNIPA n.45 9 novembre 2009 – Regole per il riconoscimento e la verifica del documento informatico

La specifica **XML Digital Signature**, documenta la sintassi e le modalità per rappresentare la firma digitale di documenti XML. Sono previste

- firme enveloped o enveloping che riguardano dati all'interno dello stesso documento
- firme detached che riguardano dati esterni al documento XML rappresentante la firma stessa.

La Deliberazione non impone l'utilizzo di una modalità di firma ma indica gli algoritmi che le applicazioni di firma devono specificare.. La tipologia di firma digitale XML adottata in MEDIR è di tipo Enveloped (http://www.w3.org/2000/09/xmldsig#enveloped-signature). Tale tipologia, prevede che essa sia inserita all'interno del documento XML firmato. In particolare, in Medir è previsto che la firma XML sia contenuta all'interno del tag LegalAuthenticator del documento CDA e dopo il tag assignedEntity.

In particolare, l'algoritmo di digest da applicare all'oggetto da firmare è la funzione SHA-256 (http://www.w3.org/2001/04/xmlenc#sha256) mentre l'algoritmo di signature per la generazione e la validazione della firma digitale è lo RSA-SHA256 (http://www.w3.org/2001/04/xmldsig-more#rsa-sha256).

Al fine di normalizzare il documento da firmare, prima di apporre la firma stessa, la delibera consente l'utilizzo di due algoritmi di canonicalizzazione:

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

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

L'uso della trasformazione XSLT (http://www.w3.org/TR/1999/REC-xslt-19991116) è consentita inserendo all'interno della stessa, il foglio di stile da utilizzare in modo che anche in fase di verifica, si possa disporre di tutte le informazioni

necessarie al recupero dei dati firmati dal documento trasformato. Inoltre dalla delibera, risulta essere obbligatorio l'utilizzo di una trasformazione di canonicalizzazione dopo l'utilizzo della trasformazione XSLT.

Per la normalizzazione degli oggetti da firmare, la delibera consente quindi l'utilizzo degli algoritmi di canonicalizzazione http://www.w3.org/2006/12/xml-c14n11# e http://www.w3.org/2006/12/xml-c14n11#WithComments.

4 L'IMPLEMENTAZIONE MEDIR

La tipologia di firma digitale XML adottata in Medir è enveloped (http://www.w3.org/2000/09/xmldsig#enveloped-signature) e prevede che essa sia inserita all'interno del documento XML firmato.

L'algoritmo di digest utilizzato è la funzione SHA-256, mentre quello per la generazione e la verifica della firma è il RSA-SHA256, così come definito della Deliberazione CNIPA n.45 del 9 novembre 2009.

Il documento da firmare deve essere prima normalizzato utilizzando l'algoritmo di canonicalizzazione http://www.w3.org/2006/12/xml-c14n11#WithComments il quale consente di preservare i commenti presenti.

Poiché, come già detto, Medir prevede l'utilizzo della tipologia di firma digitale XML Enveloped, la fase di firma prevede la dichiarazione dell'algoritmo di trasformazione http://www.w3.org/2000/09/xmldsig#enveloped-signature, utile al processo di validazione della firma.

Medir prevede opzionalmente l'impiego della trasformazione XSLT per ottenere una firma del tipo "ciò che si vede". In tale ipotesi, come ultima trasformazione da includere nella firma digitale, è necessario specificare una canonicalizzazione di tipo http://www.w3.org/2006/12/xml-c14n11#WithComments, in modo da normalizzare il risultato delle precedenti trasformazioni prima che avvenga l'apposizione della firma.

4.1 Firma digitale: <Signature>

Per la firma del documento, è prevista l'adozione dello standard XML-Signature nella modalità enveloped. La firma viene quindi accolta all'interno della classe <legalAuthenticator> in un elemento <signature> esterno allo standard CDA.

L'elemento <signature> contiene i dati necessari per la verifica della firma apportata al documento. Questo include le direttive indirizzate dallo standard XML-Signature come riscontrabile al sito web: http://www.w3.org/2000/09/xmldsig#.

Si utilizza il namespace http://www.w3.org/2000/09/xmldsig#

La deliberazione CNIPA n.45 del 9 novembre 2009 definisce inoltre l'adozione della specifica **XAdES-BES**, estendendo in questo modo lo standard XML Digital Signature con alcuni attributi; tali attributi vengono aggiunti all'elemento <signature> attraverso l'elemento <qualifyingProperties>.

La struttura di base di una sezione di firma del documento è la seguente, con l'indicazione della cardinalità degli elementi opzionali:

```
<Signature ID [0…1]>
  <SignedInfo>
    <CanonicalizationMethod/>
    <SignatureMethod/>
     (<Reference URI [0…1] >
       (<Transforms>) [0…1]
        <DigestMethod>
        <DigestValue>
       </Reference>) [1…*]
  </SignedInfo>
  <SignatureValue>
  (<KeyInfo>)[0…1]
```

```
 (<Object ID [0…1]>) [0…*]
 <Object>
  <QualifyingProperties>
   <SignedProperties>
    <SignedSignatureProperties>
     (<SigningTime>) [0…1]
    </SignedSignatureProperties>
   </SignedProperties>
  </QualifyingProperties>
 </Object>
</Signature>
```

Il formato si personalizza nel modo seguente:

Campo	Cardinalità	Scelta	Descrizione
Signature ID	0..1	0	Non utilizzato
Reference	1..*	1	Specificare algoritmo e valori di digest
Reference URI	0..1	0	Non utilizzato
Transforms	0..1	1	Indicazione dell'algoritmo Enveloped Signature
KeyInfo	0..1	1	Codifica Base64 del certificato digitale X.509 da utilizzare per il riscontro della firma
Object	0..*	0	Nessun object definito
Object ID	0..1	1	Oggetto contenente attributi aggiuntivi
SigningTime	0..1	1	Indicazione della data/ora di applicazione della firma nell'elemento *SigningTime*

Procedura di firma del documento

Il document source deve elaborare il flusso XML da firmare per calcolarne l'impronta. Quindi viene creato un elemento di tipo <Reference>, includendo l'algoritmo utilizzato e il valore del digest ottenuto. A questo punto viene creato un elemento <SignedInfo> con il <SignatureMethod>, il <CanonicalizationMethod> e la <Reference> appena calcolata.

A questo punto si costruisce l'elemento <KeyInfo>, contenente le informazioni relative al certificato X.509 da utilizzare per la verifica della firma stessa, secondo quanto stabilito dalla specifica XAdES-BES. Infine viene generato l'elemento <object> all'interno del quale deve essere specificata la data e l'ora di applicazione della firma nell'elemento <SigningTime>.

Si applica la procedura di canonicalizzazione e viene calcolato il <SignatureValue> dell'elemento <SignedInfo> e dell'elemento <KeyInfo> tramite l'algoritmo specificato in <SignedInfo> stesso. In questo modo anche gli algoritmi utilizzati risultano firmati, prevenendo la possibilità di attacchi sostenuti sostituendo gli algoritmi utilizzati con altri notoriamente più vulnerabili.

Si costruisce l'elemento <Signature> sulla base degli elementi appena costruiti (<SignedInfo> e <SignatureValue>), includendo anche l'elemento <KeyInfo>.

Si inserisce la sezione <Signature> all'interno del documento stesso.

Procedura di verifica della firma

Il document consumer applica l'algoritmo di canonicalizzazione specificato nella sezione <CanonicalizationMethod> alla sezione <SignedInfo> ed estrae la sezione <Reference> memorizzata.

Sulla base dell'algoritmo in essa specificato, viene calcolato il digest del documento.
Si verifica che il digest calcolato sia uguale a quello memorizzato. Se così non è, la procedura fallisce.
Se la procedura precedente termina con successo, occorre estrarre dalla sezione <KeyInfo> le informazioni sulla chiave di firma.
Si applica l'algoritmo di canonicalizzazione all'elemento <signatureMethod> e si utilizza il risultato per confermare il valore che è memorizzato nell'elemento <signatureValue>.

L'elemento <signature> relativo alla firma digitale è aggiunto all'interno della classe <legalAuthenticator>.

Sulla base di quanto detto, l'esempio precedente di rappresentazione della classe <legalAuthenticator> comprensivo di firma digitale diventa:

```
<legalAuthenticator>
  <!-- time: value= Data e ora di firma del documento -->
  <time value="20080708192030+0200"/>
  <signatureCode code="S"/>
  <Signature Id="xmldsig-fcea150a-756a-4c6c-8d84-7b4dba0edd33" xmlns="http://www.w3.org/2000/09/xmldsig#">
    <SignedInfo>
      <CanonicalizationMethod
        Algorithm=" http://www.w3.org/2006/12/xml-c14n11#WithComments "/>
      <SignatureMethod
        Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
      <Reference Id="xmldsig-0f2d8b6e-dfd9-4337-93b5-1e9d962d1516" URI="#xpointer(/)">
        <ds:Transforms>
                    <ds:Transform    Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
        </Transforms>
        <DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
        <DigestValue>j6lwx3rvEPO0vKtMup4NbeVu8nk=</DigestValue>
      </Reference>
      <Reference Id="xmldsig-96e21a1f-8bfe-4019-9a91-703353f6f680" URI="#idKeyInfo">
        <DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />
        <DigestValue>ZhSpFkc=…</DigestValue>
      </Reference>
      <Reference Id="xmldsig-32d7165f-dc21-4a0f-9e3e-57f69785e873" URI="#idSignedProperties"
Type="http://uri.etsi.org/01903#SignedProperties">
        <DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />
        <DigestValue>TKsaJT5p=…</DigestValue>
      </Reference>
    </SignedInfo>
    <SignatureValue>MC0CFFrVLtRlk=...</SignatureValue>
    <KeyInfo Id="#idKeyInfo">
      <X509Data>
        <X509Certificate>MIICXTCCA..</X509Certificate>
      </X509Data>
    </KeyInfo>
    <Object Id="idObject">
      <QualifyingProperties Target="#xmldsig-fcea150a-756a-4c6c-8d84-7b4dba0edd33"
xmlns="http://uri.etsi.org/01903/v1.3.2#">
        <SignedProperties Id="idSignedProperties" xmlns:voc="urn:hl7-org:v3/voc"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
          <SignedSignatureProperties>
            <SigningTime>2008-07-08T17:20:30Z</SigningTime>
          </SignedSignatureProperties>
        </SignedProperties>
      </QualifyingProperties>
```

```
    </Object>
  </Signature>
  <assignedEntity>
    <id
      root="2.16.840.1.113883.2.9.4.3.2"
      extension="RSSMRA70C07F284U"/>
    <id
      root="2.16.840.1.113883.2.9.2.200.4.2"
      extension="000000568942"/>
    <assignedPerson>
      <name>
        <prefix>Dott.</prefix>
        <given>Mario</given>
        <family>Rossi</family>
      </name>
    </assignedPerson>
    <representedOrganization>
      <!--
        tag id (OBBLIGATORIO):
          - root = OID root HL7 (Italia) per gli identificativi delle
                strutture di ricovero
          - extension = ID della struttura (AO) da codifica Min Salute
      -->
      <id
        root="2.16.840.1.113883.2.9.4.1.2"
        extension="200904"
        assigningAuthorityName="SSN-MIN SALUTE"/>
      <!--
        name= nome della struttura presso cui è il documento è stato firmato
      -->
      <name>AO G. Brotzu</name>
      <addr>
        <city>Cagliari</city>
        <postalCode>09100</postalCode>
        <streetName>via Ospedale</streetName>
        <houseNumber>46</houseNumber>
        <country>Italia</country>
      </addr>
    </representedOrganization>
  </assignedEntity>
</legalAuthenticator>
```

4.2 Trasformazione XSLT: <stylesheet>

L'utilizzo della trasformazione XSLT non è obbligatorio; la trasformazione XSLT andrebbe impiegata quando è necessario realizzare una firma del tipo "ciò che si vede". Negli altri casi in cui questo non è necessario, tale trasformazione può essere omessa e si possono firmare direttamente i dati rappresentati nel documento XML.

Attraverso l'utilizzo di tale trasformazione, il firmatario del documento è in grado di specificare come è stato ottenuto l'oggetto della firma a partire dai dati XML di partenza. Un client integrato al sistema Medir, prima di inviare un documento, compone un CDA xml e propone al firmatario una renderizzazione dello stesso ottenuta applicando un foglio di stile che poi sarà incluso all'interno della firma digitale nell'opportuno tag relativo all'algoritmo di trasformazione XSLT.

Procedura di firma del documento

A seguire la trasformazione xmldsig#enveloped-signature viene specificato l'algoritmo di trasformazione XSLT, indicando in-line il foglio di stile adottato, utilizzando in maniera interoperabile l'uso della trasformazione XSLT http://www.w3.org/TR/1999/REC-xslt-19991116.

Infine, come ultima trasformazione da includere nella firma digitale, è necessario specificare una canonicalizzazione di tipo http://www.w3.org/2006/12/xml-c14n11#WithComments, in modo da normalizzare il risultato della precedente trasformazione.

Pertanto il contenuto di <Signature> del documento CDA che prevede trasformazione XSLT risulta arricchito nella sola sezione <Transforms> delle trasformazioni necessarie.

Procedura di verifica della firma
Corrisponde alla procedura descritta nel caso di CDA privo di trasformazione XSLT.

L'esempio precedente arricchito della sezione di trasformazione diventa:

```
<legalAuthenticator>
  <!-- time: value= Data e ora di firma del documento -->
  <time value="20080708192030+0200"/>
  <signatureCode code="S"/>
  <ds:Signature Id="xmldsig-fcea150a-756a-4c6c-8d84-7b4dba0edd33"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    <ds:SignedInfo>
          <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2006/12/xml-c14n11#WithComments "/>
          <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
          <ds:Reference Id="xmldsig-0f2d8b6e-dfd9-4337-93b5-1e9d962d1516" URI="#xpointer(/)">
            <ds:Transforms>
                  <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
                  <ds:Transform Algorithm="http://www.w3.org/TR/1999/REC-xslt-19991116">
                        <xsl:stylesheet ……..>
                        <xsl:output encoding="UTF-8" indent="no" method="xml" omit-xml-declaration="yes"
                  standalone="yes"/>
                         [stylesheet in-line…]
                        </xsl:stylesheet>
                  </Transform>
                  <Transform Algorithm="http://www.w3.org/2006/12/xml-c14n11#WithComments " />
                </Transforms>
       <DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />
       <DigestValue>Es41FiBh2AtuDkQtwLXaZpqWaVM=</DigestValue>
      </Reference>
      <Reference Id="xmldsig-96e21a1f-8bfe-4019-9a91-703353f6f680" URI="#idKeyInfo">
       <DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />
       <DigestValue>ZhSpFkc=…</DigestValue>
      </Reference>
      <Reference Id="xmldsig-32d7165f-dc21-4a0f-9e3e-57f69785e873" URI="#idSignedProperties"
Type="http://uri.etsi.org/01903#SignedProperties">
```

```
        <DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />
        <DigestValue>TKsaJT5p=…</DigestValue>
      </Reference>
    </SignedInfo>
    <SignatureValue>QSgOslsCJ5yjkUcR9PY5ug2oMLDw=…</SignatureValue>
          <KeyInfo Id="idKeyInfo">
      <X509Data>
        <X509Certificate> ….SEhISEgwMEgwMEgw….MDAwMDA </X509Certificate>
      </X509Data>
    </KeyInfo>
    <Object Id="idObject">
      <QualifyingProperties Target="#xmldsig-fcea150a-756a-4c6c-8d84-7b4dba0edd33"
xmlns="http://uri.etsi.org/01903/v1.3.2#">
        <SignedProperties Id="idSignedProperties" xmlns:voc="urn:hl7-org:v3/voc"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
          <SignedSignatureProperties>
            <SigningTime>2008-07-08T17:20:30Z</SigningTime>
          </SignedSignatureProperties>
        </SignedProperties>
      </QualifyingProperties>
    </Object>
  </Signature>
  <assignedEntity>
    <id
      root="2.16.840.1.113883.2.9.4.3.2"
      extension="RSSMRA70C07F284U"/>
    <id
      root="2.16.840.1.113883.2.9.2.200.4.2"
      extension="000000568942"/>
    <assignedPerson>
      <name>
        <prefix>Dott.</prefix>
        <given>Mario</given>
        <family>Rossi</family>
      </name>
    </assignedPerson>
    <representedOrganization>
      <!--
        tag id (OBBLIGATORIO):
          - root = OID root HL7 (Italia) per gli identificativi delle
                strutture di ricovero
          - extension = ID della struttura (AO) da codifica Min Salute
      -->
      <id
        root="2.16.840.1.113883.2.9.4.1.2"
        extension="200904"
        assigningAuthorityName="SSN-MIN SALUTE"/>
      <!--
```

```
      name= nome della struttura presso cui è il documento è stato firmato
    -->
    <name>AO G. Brotzu</name>
    <addr>
      <city>Cagliari</city>
      <postalCode>09100</postalCode>
      <streetName>via Ospedale</streetName>
      <houseNumber>46</houseNumber>
      <country>Italia</country>
    </addr>
  </representedOrganization>
 </assignedEntity>

</legalAuthenticator>
```

4.2.1 Sicurezza

Al fine di evitare i problemi di sicurezza esplicitati in http://www.w3.org/TR/xmldsig-bestpractices/, Medir impone l'utilizzo di un foglio di stile unico e versionato.

I client integrati dovranno quindi utilizzare solo tale foglio di stile e Medir rigetterà documenti CDA firmati utilizzando trasformazioni XSLT il cui foglio di stile non risulta censito nel sistema. Ciò è realizzato verificando l'hash del foglio di stile presente nella trasformazione XSLT calcolato attraverso un algoritmo MD5. Se l'hash non coincide con quello noto a Medir la firma non sarà considerata valida.

Il foglio di stile (i.e. EXE-DES-Stylesheet_CDA_Medir_V_x.xx.xsl) può essere distribuito ai client integratori, i quali ne possono giudicare l'applicabilità e la esaustività: i client integratori possono proporre eventuali enhancement al foglio di stile per specifiche esigenze (i.e per specifici CDA); la proposta potrà essere valutata da MEDIR, e nel caso di accettazione il nuovo foglio di stile verrà censito.