Documento di Specifiche di definizione del CDA 2 per Interoperabilità FSE

LAZIOcrea S.p.A. – Società a Socio unico Regione Lazio – Cap. Soc. € 924.400,00
Sede legale e amministrativa: Via del Serafico, 107 00142 Roma - T +39 06 515631 F +39 06 51563611
Uffici: Via Adelaide Bono Cairoli, 68 – Roma 00145 – T +39 06 51689800 – F +39 06 51892207
C.F./P.IVA 13662331001 – R.E.A. RM-1464288
PEC Azienda: laziocrea@legalmail.it
www.laziocrea.it - www.regione.lazio.it

Data	Ver	Descrizione Modifica
20/03/2018	**1**	**Prima emissione**
17/02/2022	**2**	**Iniezione rappresentazione pdf**

Indice

1 INTRODUZIONE 4
1.1 Scopo del Documento 4
1.2 Riferimenti 4
1.3 Convenzioni 4
1.4 Requisiti di Conformità 4
1.5 Notazioni specifiche 4
1.6 Convenzioni di obbligatorietà e opzionalità. 5
1.7 Propedeuticità 5
1.8 Acronimi e definizioni 5
2 Iniezione rappresentazione PDF. 7
3 Applicazione firma digitale XADES. 9

1 INTRODUZIONE

1.1 Scopo del Documento

L'obiettivo del presente documento è quello di offrire una guida rapida riguardante l'inclusione di un documento non strutturato come ad esempio un documento PDF all'interno del CDA e l'applicazione della firma digitale XADES in modalità enveloped.

1.2 Riferimenti

Rif.1 - HL7 Implementation Guide: CDA Release 2 – Continuity of Care Document (CCD) - **http://www.hl7.org**

1.3 Convenzioni

Nel presente documento sono adottate le convenzioni descritte nei paragrafi seguenti.

1.4 Requisiti di Conformità

I requisiti di conformità a questa guida sono indicati nel seguente formato:

CONF-xy: esempio di un requisito di conformità
CONF-xy-zw: esempio di un sottolivello di requisito di conformità
CONF-xy-zw-ji: esempio di un ulteriore sottolivello di requisito di conformità

dove la numerazione è sequenziale eventualmente a tre livelli.

In particolare i requisiti di conformità a questa guida sono espressi in un linguaggio "technology-neutral". È possibile utilizzare il linguaggio di validazione Schematron per l'implementazione delle regole di conformità definite nella presente guida.

1.5 Notazioni specifiche

Nel documento vengono utilizzate le seguenti notazioni specifiche:

- i valori costanti assunti dagli attributi sono indicati in *font corsivo*;
- le classi, gli elementi e le componenti degli elementi del modello CDA sono indicati con *font corsivo*;

- per l'identificazione degli elementi, sia all'interno del testo narrativo che all'interno dei requisiti di conformità, viene utilizzata la notazione XPath (es. *ClinicalDocument / typedId, relatedDocument / @typeCode, etc.*).

1.6 Convenzioni di obbligatorietà e opzionalità.

Nella definizione dei requisiti, delle specifiche e delle regole descritte nel seguente documento sono utilizzate le parole chiave **DEVE, NON DEVE, OBBLIGATORIO, VIETATO, DOVREBBE, CONSIGLIATO, NON DOVREBBE, SCONSIGLIATO, PUÒ, OPZIONALE** che devono essere interpretate in conformità con RFC 2119.

In particolare:

- **DEVE, OBBLIGATORIO, NECESSARIO (MUST, REQUIRED, SHALL)** significano che la definizione è un requisito assoluto, la specifica deve essere implementata, la consegna è inderogabile.
- **NON DEVE, VIETATO (MUST NOT, SHALL NOT)** significano che c'è proibizione assoluta di implementazione di un determinato elemento di specifica.
- **DOVREBBE, CONSIGLIATO (SHOULD, RECOMMENDED)** significano che in particolari circostanze possono esistere validi motivi per ignorare un requisito, non implementare una specifica, derogare alla consegna, ma che occorre esaminare e valutare con attenzione le implicazioni correlate alla scelta.
- **NON DOVREBBE, SCONSIGLIATO (SHOULD NOT, NOT RECOMMENDED)** significano che in particolari circostanze possono esistere validi motivi per cui un elemento di specifica è accettabile o persino utile, ma, prima di implementarlo, le implicazioni correlate dovrebbero essere esaminate e valutate con attenzione.
- **PUÒ, POTREBBE, OPZIONALE (MAY, OPTIONAL)** significano che un elemento della specifica è a implementazione facoltativa.

Le parole chiave nel testo sono segnalate in maiuscolo e neretto (es. **DEVE**).

1.7 Propedeuticità

Per la lettura di questa guida si assume che il lettore abbia conoscenza dello standard HL7 V3, in particolare del CDA Release 2, ed accesso alle relative specifiche.

1.8 Acronimi e definizioni

Acronimo/Termine	Definizione
CDA	Clinical Document Architecture
HL7	Health Level 7
ISO	International Organization for Standardization
ISTAT	Istituto Nazionale di Statistica
LOINC	Logical Observation Identifiers Names and Codes
Namespace	Spazio di valori, ambito di intervento di una Autorità Assegnata
OID	ISO Object Identifier
OIDnazionale	ISO Object Identifier di HL7 Italia (2.16.840.1.113883.2.9)
RIM	Reference Information Model
XML	eXtensible Markup Language

Tabella 1 - Acronimi e definizioni

2 Iniezione rappresentazione PDF.

Vi sono diversi modi per includere un contenuto multimediale all'interno di un CDA2. In particolare qui sarà descritto come iniettare la rappresentazione PDF del documento stesso all'interno del CDA.
Quanto descritto vale per tutti i documenti CDA2 i quali hanno la seguente struttura di massima:

```
<ClinicalDocument>

  <recordTarget>
    <patientRole>

    </patientRole>
   </recordTarget>
  <author>

  </author>
  <custodian>

  </custodian>

  <inFulfillmentOf typeCode="FLFS">
    <order moodCode="RQO" classCode="ACT">
      <id root="2.16.840.1.113883.2.9.4.3.6" extension="120A24030681576" assigningAuthorityName="Regione
Lazio"/>
    </order>
  </inFulfillmentOf>

  <component>
    <structuredBody>
      <component>
       <section>
       …
       </section>
      </component>
      …
      <component>
       <section>
       …
       </section>
      </component>
    </structuredBody>
  </component>

</ClinicalDocument>
```

CDA Header

Eventuale riferimento al NRE

CDA Body

Come si può osservare il corpo del CDA (*structuredBody*) è composto da componenti (*component*) costituiti dalle sezioni del documento sanitario (*section*).
L'iniezione della rappresentazione consiste nell'aggiungere una sezione caraterizzata dallo stesso codice LOINC relativo alla tipologia del documento con rappresentazione in Base 64 del contenuto all'interno del tag *value* contenuto nel tag *observationMedia*.
Ad esempio nel caso del CDA del referto di laboratorio il cui codice LOINC del documento è 11502-2 occorre aggiungere la seguente sezione:

```
  <component>
    <structuredBody>
      …
      <component>
        <section ID="PDF">
          <code code="11502-2" codeSystem="2.16.840.1.113883.6.1" codeSystemName="LOINC"
displayName="Referto di Laboratorio" />
          <entry>
            <observationMedia classCode="OBS" moodCode="EVN">
              <value mediaType="application/pdf" representation="B64">Base 64 del documento</value>
            </observationMedia>
          </entry>
        </section>
      </component>

    </structuredBody>
  </component>
```

All'interno della sezione (*section*) l'elemento *code* è **OBBLIGATORIO** e **DEVE** riportare lo stesso codice del documento.

L'elemento *value* all'interno del tag *observationMedia* **DEVE** contenere gli attributi *mediaType* con valorizzato il MIME type del documento (application/pdf) e *representation* valorizzato a "B64".

3 Applicazione firma digitale XADES.

Nel presente capitolo sarà descritta l'adozione dello standard XAdES-BES (XML Advanced Electronic Signature) per la firma digitale dei documenti CDA2. La peculiarità di tale standard e che la firma può riferire ad 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".
Nella definizione per l'implementazione della firma digitale dei documenti CDA, 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/);
- 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 come:

- 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 tipologia di firma digitale XML adottata nel FSE 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 la firma XML sarà contenuta all'interno del tag *LegalAuthenticator* del documento CDA e dopo il tag *assignedEntity*.
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.
Di seguito un esempio di applicazione della firma digitale XADES all'interno del CDA2.

```
<ClinicalDocument>

  <recordTarget>
    <patientRole>

    </patientRole>
   </recordTarget>
  <author>

  </author>
  <custodian>

  </custodian>

  <legalAuthenticator>
    <time value="20150507105330+0200" />
    <signatureCode code="S" />

    <Signature Id="xmldsig-9a2c08e0-a01b-4364-91d5-b349c826a882"
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/xmldsig-more#rsa-sha256" />
      <Reference Id="xmldsig-67b39709-f651-411b-867e-26d71e33d825" URI="">
        <Transforms>
          <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
          <Transform Algorithm="http://www.w3.org/2006/12/xml-c14n11#WithComments" />
        </Transforms>
        <DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />
        <DigestValue><!-- Digest codificato Base64 --></DigestValue>
      </Reference>
      <Reference Id="xmldsig-00498038-d117-4a33-b020-21a11676f5b0" URI="#idKeyInfo">
        <DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />
        <DigestValue><!-- Digest codificato Base64 --></DigestValue>
      </Reference>
      <Reference Id="xmldsig-8b217176-3609-42a7-8daf-a207b77d6b44"
Type="http://uri.etsi.org/01903#SignedProperties" URI="#idSignedProperties">
        <DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />
        <DigestValue><!-- Digest codificato Base64 --></DigestValue>
      </Reference>
      </SignedInfo>
      <SignatureValue><!-- Firma codificata Base64 --></SignatureValue>
      <KeyInfo Id="idKeyInfo">
      <X509Data>
        <X509Certificate><!-- Certificato codificato Base64 --></X509Certificate>
      </X509Data>
      </KeyInfo>
      <Object Id="idObject">
      <QualifyingProperties Target="#xmldsig-9a2c08e0-a01b-4364-91d5-b349c826a882"
xmlns="http://uri.etsi.org/01903/v1.3.2#">
        <SignedProperties Id="idSignedProperties" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
        <SignedSignatureProperties>
          <SigningTime>2013-10-03T09:26:58Z</SigningTime>
        </SignedSignatureProperties>
        </SignedProperties>
      </QualifyingProperties>
      </Object>
    </Signature>

    <assignedEntity>
      <id extension="XXXXXX01A01H501X" root="2.16.840.1.113883.2.9.4.3.2" />
      <id extension="cod_operatore" root="2.16.840.1.113883.2.9.2.120.4.2" />
      <assignedPerson>
        <name>
          <prefix>Sig.</prefix>
          <given>NOME_OPERATORE</given>
          <family>COGNOME_OPERATORE</family>
        </name>
      </assignedPerson>
      <representedOrganization>
```

```
        <id assigningAuthorityName="Regione Lazio" extension="120101"
root="2.16.840.1.113883.2.9.2.120.4.11" />
        <name>ASL ROMA A</name>
        <addr>
          <city>Roma</city>
          <postalCode>00185</postalCode>
          <streetName>Via Ariosto</streetName>
          <houseNumber>3</houseNumber>
          <country>Italia</country>
        </addr>
      </representedOrganization>
    </assignedEntity>
  </legalAuthenticator>

  <component>
    <structuredBody>

    </structuredBody>
  </component>

</ClinicalDocument>
```