



HL7 Italia

www.hl7italia.it

La Firma Digitale di CDA

(IT Realm)

White Paper

Versione 1.1

Febbraio 2012

Questo documento¹

Titolo (dc:title):	White Paper Titolo
Data (dc:date):	08/02/2012
Status/Versione (hl7italia:version):	v1.1
Sostituisce (dc:relation.replaces):	n/a
Diritti di accesso (dc:right.accessRights):	Documento pubblico
Nome File (hl7it:fileName):	HL7Italia-FirmaCDA-1.1-WP
Approvato da (hl7it:isRatifiedBy):	Gruppo di Progetto HL7 Italia Firma Digitale CDA
Emesso da (dc:publisher):	[HL7 Italia]

¹ I metadati del documento sono conformi allo standard Dublin Core 1.1 (ISO 15836:2003)

Partecipanti alla redazione:

	Nome	Organizzazione
Autore (dc:creator):	Riccardo Ranza	Lombardia Informatica
Autore (dc:creator):	Mario Martinelli	Lombardia Informatica
Autore (dc:creator):	Pierluigi Valenti	Lombardia Informatica
Autore (dc:creator):	John Mason	Lombardia Informatica
Contributore (dc:contributor):	Stefano Micocci	CUP2000
Contributore (dc:contributor):	Giorgio Cangiolì	Consulente
Contributore (dc:contributor):		
Responsabile (hl7it:responsible):		
Responsabile (hl7it:responsible):		

Hanno inoltre partecipato alle attività del *Gruppo di Progetto*: Giorgia Galamini, Data Processing; Libero Maesano, Simple Engineering; Renato Calamai, eHealthTech; Giovanni Sarbia, Adobe.

REGISTRO DELLE MODIFICHE

Versione	Stato	Data	Commenti
0.1	Bozza	20/04/2011	
0.2	Bozza	05/07/2011	Inserito par. "Impatti" Modificato par. "Scopo del Documento" Modifiche editoriali minori
0.3	Bozza	14/09/2011	Recepimento di osservazioni di CUP2000 Inserimento del par. "Struttura del Documento" Ristrutturazione per abilitare l'inserimento futuro di altri profili Riformulazione dei par. "Conclusioni" e "Interoperabilità"
1.0	Finale	19/09/2011	Versione Proposta per pubblicazione
1.09	Bozza	18/01/2012	Introdotte precisazioni nei cap. 2.1.1, 2.1.5 e 2.2.7
1.1	Finale	08/02/2012	Versione Proposta per pubblicazione



Rispetta l'ambiente.

Non stampare questo documento se non è strettamente necessario.

Sommario

1	INTRODUZIONE	5
1.1	SCOPO DEL DOCUMENTO	5
1.2	STRUTTURA DEL DOCUMENTO	6
2	PROFILI DI INTEROPERABILITÀ.....	7
2.1	L'APPROCCIO SPONTANEO (FIRMA XAdES DEL CDA2).....	7
2.1.1	Contesto	7
2.1.2	Fruizione.....	9
2.1.3	Formato di firma	9
2.1.3.1	<i>Firma XAdES Enveloping</i>	9
2.1.3.2	<i>Firma XAdES Detached</i>	9
2.1.3.3	<i>Firma XAdES Enveloped</i>	9
2.1.4	Vantaggi	10
2.1.5	Svantaggi	10
2.2	UN APPROCCIO DIFFERENTE (FIRMA DI DOCUMENTI PDF CON CDA2 INIETTATO)	11
2.2.1	Contesto	12
2.2.2	Fruizione.....	13
2.2.3	Formati di firma	13
2.2.3.1	<i>Firma XAdES</i>	13
2.2.3.2	<i>Firma PAdES</i>	13
2.2.3.3	<i>Firma CAdES</i>	14
2.2.4	Vantaggi	14
2.2.5	Svantaggi	14
2.2.6	Osservazione	14
2.2.7	Impatti.....	15
2.3	UN ALTRO APPROCCIO	16
3	CONCLUSIONI.....	17
3.1	INTEROPERABILITÀ.....	17
3.2	NORMALIZZAZIONE	18

1 INTRODUZIONE

Nell'ambito dei processi di dematerializzazione della Sanità, si avverte una forte spinta verso l'impiego degli standard HL7-CDA2 per la rappresentazione informatica dei documenti clinici (referti, lettere di dimissione, verbali di pronto soccorso, ecc.)

Tali documenti clinici (detti documenti clinico-elettronici: DCE) sono quindi particolari "documenti informatici", che il processo organizzativo richiede tipicamente di sottoscrivere applicando la firma elettronica qualificata (cfr. D.Lgs.n.235/2010, "Codice dell'Amministrazione Digitale"), che a sua volta applica la logica "what you see is what you sign".

Il formato dei documenti basati su HL7-CDA2 è –come è noto- XML. Tale formato deve poter soddisfare le seguenti esigenze specifiche:

- Fruibilità dell'informazione da parte dell'utente umano: l'utente "umano" che opera in base a quello che "vede", cioè alla rappresentazione intelligibile delle informazioni del documento sottoscritto a cui, comunque, è associato il meccanismo "non ripudio" della firma elettronica qualificata;
- Fruibilità dell'informazione da parte dell'utente programmatico: l'utente "programmatico" (es. una Cartella Clinica) che deve fruire della componente strutturata navigando in modo deterministico il documento nel suo formato nativo CDA2 per fare pieno uso delle informazioni strutturate in esso contenute.

Si osserva che ai documenti sottoscritti con firma elettronica qualificata è naturalmente applicabile il processo di conservazione sostitutiva previsto dalla normativa vigente.

1.1 SCOPO DEL DOCUMENTO

La Deliberazione n.45 del 21/05/2009, in Gazzetta ufficiale del 3-12-2009 e attualmente in vigore, intitolata "Definizione delle regole per il riconoscimento e la verifica del documento informatico", indica la possibilità di realizzare una sottoscrizione "in linguaggio XML" di un documento informatico (sottoscrizione XAdES). Ne consegue che questa modalità di sottoscrizione sia naturalmente applicabile ad un documento clinico-elettronico CDA2 che è in formato XML.

Il presente documento si pone l'obiettivo di individuare le eventuali problematiche che possono insorgere nell'apposizione di una firma elettronica qualificata in formato XAdES, individuando possibili scenari conformi alla normativa in vigore, che consentano una più agevole gestione della firma del documento in formato strutturato CDA2 e della sua rappresentazione interpretabile dall'utente umano, individuando così gli opportuni profili di interoperabilità.

La condivisione di un numero contenuto di profili, normati in ambito HL7 Italia, coniuga le specificità e le esigenze dei processi dei singoli domini applicativi (p.e le Regioni) con le esigenze di interoperabilità a livello nazionale dei DCE sottoscritti.

In questa analisi, si è tenuto conto delle seguenti considerazioni:

- I tempi e l'onere elaborativo necessari per l'apposizione della firma e per la verifica/fruizione del documento devono essere accettabili per l'utente finale e per i sistemi coinvolti, con riferimento al contesto operativo di utilizzo (p.e. interattivo o meno);
- In fase di generazione della componente di presentazione i sottoscrittori (soprattutto quando si tratta di organizzazioni) hanno l'esigenza di introdurre componenti distintive (es. un logo aziendale);
- Il documento deve portare con sé quanto necessario per la sua presentazione all'utente sottoscrittore e all'utente fruitore nel modo più agevole possibile, in quanto la presentazione "nativa" del formato XML non è intelligibile dall'utente umano;
- Il formato prescelto deve consentire anche la marcatura temporale del documento sottoscritto;
- Il documento con la sua firma può produrre un unico file o più file;
- La dimensione dei documenti prodotti, per quanto sia un aspetto sempre meno rilevante, può avere impatti sui tempi di trasmissione e fruizione in rete.

1.2 STRUTTURA DEL DOCUMENTO

Il documento presenta:

- il capitolo di Introduzione (questo);
- il capitolo Profili di Interoperabilità, dove i vari profili sono enunciati e discussi. Tale capitolo è già predisposto a future estensioni, con l'inclusione di altri profili;
- il capitolo di Conclusioni.

2 PROFILI DI INTEROPERABILITÀ

2.1 L'approccio spontaneo (firma XAdES del CDA2)

La scelta spontanea per la sottoscrizione di documenti CDA2 è il formato XAdES che, essendo a sua volta un formato XML basato su specifiche del W3C (XML-DSig), coniuga in modo naturale la firma del documento clinico-elettronico con il trasporto di informazioni strutturate facilmente navigabili ed importabili da parte di applicazioni terze quali le Cartelle Cliniche.

2.1.1 Contesto

La legislazione italiana richiede che il firmatario di un documento informatico debba avere la possibilità di visionarne preventivamente il documento da sottoscrivere (art. 35 comma 2 del CAD) in modo tale che il processo assicuri il non ripudio della firma garantendone sia la piena integrità che la piena consapevolezza del contenuto da parte del sottoscrittore (what you see is what you sign).

I documenti in formato XML pur essendo in formato testuale hanno una struttura tale che la loro rappresentazione come semplice testo può essere insufficiente a garantirne l'intelligibilità; il particolare caso dei documenti XML-CDA2 è emblematico il quanto la struttura estremamente articolata, la definizione dei nomi degli elementi in lingua inglese e la presenza di informazioni codificate lo rendono totalmente inadatto ad essere presentato direttamente della sua forma nativa.

Lo standard XML-DSig, così come specificato dal W3C, tiene conto di tale tipologia di documenti complessi prevedendo che la presentazione al sottoscrittore sia in tal caso prodotta tramite una trasformazione basata sull'impiego di un foglio di stile XSLT che, quando applicato dal toolkit di firma, generi un output XHTML da utilizzare per presentare all'utente i dati da sottoscrivere. La firma è poi apposta sull'Hash del documento XHTML risultante dalla trasformazione.

Il foglio di stile utilizzato durante la sottoscrizione può essere incluso nella signature XML con lo scopo di rendere il processo di verifica della firma indipendente da informazioni non contenute nel file prodotto dal processo di sottoscrizione.

Lo standard XAdES infine estende XML-DSig, definendo l'obbligatorietà di alcune estensioni che in questo sono opzionali.

L'implementazione del processo di firma XAdES e la corrispondente componente di verifica, sono demandate al "client di firma" che, facendo uso delle informazioni contenute nel file firmato o ad esso crittograficamente correlate, è in grado di presentarne il contenuto all'utente senza aver nessuna conoscenza del dominio applicativo a cui questo appartiene. Questo aspetto è estremamente importante in quanto un documento normalmente viene sottoscritto digitalmente quando deve essere messo a disposizione di altri domini di responsabilità, all'interno dei quali la presentazione delle informazioni in esso contenute deve essere univoca, standardizzata e non mediata da componenti

applicative che potrebbero mostrare le informazioni in una forma diversa da quella percepita dal sottoscrittore. Un caso emblematico è quello della visione del documento CDA2 da parte di un cittadino il quale può ottenere e conservare un documento firmato e ha il diritto di visionarne il contenuto con strumenti standard non verticalizzati sulla specifica natura del contenuto.

In altre parole, il processo di firma e verifica deve fornire garanzia di vedere esattamente quanto visionato dal sottoscrittore, sia a utenti diversi, sia agli stessi utenti in tempi diversi.

L'impiego della trasformazione XSLT nell'ambito della firma XAdES ha diverse conseguenze:

1. Solo i nodi "catturati" dalla trasformazione XSLT sono presentati all'utente e, di fatto, coinvolti nel meccanismo di integrità della firma;
2. Poiché il foglio di stile è per sua natura testuale, l'inclusione di elementi grafici nel documento XHTML prodotto per la presentazione (ad esempio loghi o simili) complica il processo di apposizione della firma e di fruizione del documento sottoscritto;
3. L'inclusione del foglio di stile nel documento sottoscritto pur semplificando il processo di verifica ne può far aumentare considerevolmente le dimensioni, questo è vero il particolar modo per i documenti CDA2, i quali possono essere associati ad un foglio di stile molto complesso.

Si noti che il punto 1) può essere mitigato inserendo in sottoscrizione un ulteriore nodo "reference" a copertura dell'intero documento al fine di assicurare l'integrità di tutti gli elementi presenti, anche quelli non coinvolti nell'output XHTML su cui si basa il non ripudio del sottoscrittore.

Relativamente all'affermazione del punto 2) si noti che è tecnicamente possibile realizzare una trasformazione con un output XHTML che riferisca ad elementi grafici, però tale approccio ha consistenti controindicazioni in quanto ciascuno dei file grafici deve essere oggetto di uno specifico nodo "reference" per assicurarne l'integrità. La costruzione delle URL per i file esterni deve essere tale da garantire che il processo di verifica sia indipendente dall'ambiente operativo del fruitore che, in ogni caso, deve ricevere e gestire una molteplicità di file. Queste complicazioni tecnico gestionali, in aggiunta alle difficoltà per il fruitore di assicurarsi che la firma del documento sia stata generata in modo tale da assicurare l'integrità di tutti i file a corredo della trasformazione, disincentivano l'impiego di elementi grafici nella trasformazione XSLT.

Per il punto 3) sono possibili degli "escamotage" tecnici al fine di mantenere in un file esterno il foglio di stile (riferimento ad un foglio di stile intermedio contenente la sola "include" di quello reale) al prezzo di una gestione ulteriore dei file XSLT che devono essere disponibili presso sottoscrittore e fruitore, sia in firma che in verifica, e correlati al documento sottoscritto generando le medesime problematiche espresse per il punto 2).

2.1.2 Fruizione

La fruizione del contenuto da parte dell'utente "umano" richiede l'impiego di un comune web browser, una volta prodotta la componente XHTML da parte dello strumento di verifica della firma.

La fruizione del contenuto da parte dell'utente "programmatico", in funzione del formato di firma utilizzato, richiede al più di ignorare elementi Signature iniettati nella struttura XML del documento CDA2.

2.1.3 Formato di firma

Come accennato precedentemente la scelta spontanea per la firma di un documento CDA2 è il formato XAdES, il quale a sua volta prevede tre modalità di "imbustamento" della firma:

- Enveloping, elemento Signature che "ingloba" il contenuto sottoscritto (indispensabile per la firma di documenti non XML);
- Detached, con il file XML contenente la Signature fisicamente distinto dal file del documento sottoscritto;
- Enveloped, elemento Signature "iniettato" nel documento XML sottoscritto.

2.1.3.1 Firma XAdES Enveloping

Per la firma di documenti CDA2 non si ritiene di particolare interesse il formato Enveloping in quanto, trattandosi della firma XML di documenti XML, non sembra dare alcun valore aggiunto rispetto ad una tradizionale firma CAAdES.

Si suggerisce perciò di restringere la scelta ai formati di tipo Detached ed Enveloped.

2.1.3.2 Firma XAdES Detached

Il formato di firma Detached ha il vantaggio di non alterare in alcun modo il documento sottoscritto per cui limita le problematiche di interoperabilità alla sola firma XML. Per contro devono essere mantenuti, e correlati, due file rendendo più complicata la gestione documentale dei documenti firmati.

Ai fini dell'interoperabilità, anche le modalità di correlazione devono essere condivise e pertanto normalizzate.

2.1.3.3 Firma XAdES Enveloped

Il formato di firma Enveloped produce tendenzialmente un unico file XML. Si osserva che lo schema XML del CDA2 deve essere esteso –quantomeno a livello nazionale italiano-

per prevedere la presenza opzionale del nodo della firma (o più nodi di firma nel caso di firma multipla).

2.1.4 Vantaggi

Utilizzando il formato Detached il documento sottoscritto resta inalterato (si devono però gestire due file distinti).

Utilizzando il formato Enveloped è possibile mantenere il documento firmato in un unico file.

La componente CDA2 del documento è fruibile senza alcuna elaborazione a meno, nel caso di firma Enveloped, del nodo Signature iniettato nel documento CDA2; tale nodo infatti deve essere ignorato.

Il documento XHTML prodotto in sede di verifica della firma è direttamente rappresentabile in un browser web.

2.1.5 Svantaggi

Indipendentemente dal formato di firma utilizzato (Detached o Enveloped), per presentare il documento all'utente in sede di verifica della firma occorre ripetere ogni volta la trasformazione XSLT, cioè fare uso di uno specifico client XAdES.

L'apposizione e la verifica della firma sono estremamente onerose sia in termini di tempo di elaborazione sia di risorse di calcolo (almeno un ordine di grandezza superiore ad una firma CAdES) a causa delle numerose e complesse trasformazioni richieste dallo standard XML-DSig; il problema è aggravato dal fatto che mentre la firma è eseguita una volta la verifica è potenzialmente eseguita numerose volte. In sede di pura fruizione l'onere computazionale è riferito al processo di verifica della firma XAdES, da effettuare almeno una volta quando il documento è acquisito da un diverso dominio di responsabilità (p.e. il cittadino o il medico che consultano il Fascicolo Sanitario Elettronico), e non al semplice atto di fruizione dei contenuti strutturati CDA2.

NOTA: Il confronto delle prestazioni tra firma CAdES e XAdES è stato effettuato utilizzando un toolkit crittografico in linguaggio Java ed un Personal Computer di fascia media. Per i test dei due formati di firma è stato utilizzato il medesimo toolkit. Si osserva, inoltre, che le prestazioni della firma XAdES, comportando numerose trasformazioni, sono influenzate in modo significativo dalla dimensione del documento XML, dalla sua complessità e dalla complessità delle trasformazioni richieste, prima fra tutte la trasformazione XSLT necessaria per produrre la componente di presentazione per il sottoscrittore.

2.2 Un approccio differente (Firma di documenti PDF con CDA2 iniettato)

A causa dei preoccupanti impatti prestazionali e dell'enorme impegno di risorse di calcolo (almeno un ordine di grandezza superiore ad una firma CADES) si è investigata la possibilità di estendere il profilo di interoperabilità con il supporto di ulteriori formati, più adatti a contesti applicativi:

- che prevedano la generazione di grandi quantità di documenti da parte di attori diversi;
- in cui tali documenti sono destinati ad essere fruiti più volte nel corso del loro ciclo di vita in uno scenario di utilizzo di interattività in tempo reale.

Si sottolinea esplicitamente che questo ulteriore approccio qui proposto **non è alternativo** al precedente, con cui **coesiste**.

Dal punto di vista del processo si è provato a "rovesciare" l'approccio partendo dal punto di vista del fruitore del documento sottoscritto:

- L'utente "umano" per cui la metafora di lavoro naturale è il documento, cioè un file che possa essere fruito nei modi e con gli strumenti di uso quotidiano;
- L'utente "programmatico" (ad es. una Cartella Clinica) che deve fruire della componente strutturata navigando in modo deterministico il documento.

La componente strutturata deve restare in formato XML aderente allo standard CDA2.

A tal fine si propone il seguente processo:

1. Generare il documento clinico-elettronico nel formato CDA2;
2. Produrre un file in formato PDF a partire dal contenuto informativo del documento CDA2 (in linea di principio applicando una trasformazione XSL-FO);
3. Inserire (ovvero "iniettare") il contenuto XML rappresentato dal documento CDA2 originario nel file PDF; tale possibilità è supportata dal formato di Adobe, che è documentato con specifiche pubbliche (si nota che oltre alla realizzazione di Adobe, ne esistono altre di terze parti, oltre alla possibilità di svilupparle autonomamente);
4. Sottoscrivere il file PDF, comprensivo della componente XML inserita.

NOTA: la maggiore criticità di questa soluzione è assicurare che le fasi 3-4 siano svolte attraverso soluzioni tecniche e procedure organizzative tali da assicurare – anche ai fini legali - la coerenza fra il CDA2 iniettato ed il PDF visualizzato e firmato.

Riassumendo, l'approccio qui descritto prevede di iniettare una struttura XML (il documento clinico-elettronico CDA2) all'interno di una struttura binaria secondo standard PDF, che ne costituisce la rappresentazione orientata all'utente umano.

Poichè il prodotto finale è costituito da un documento PDF conforme, la sua sottoscrizione è indipendente dal processo di iniezione e pertanto compatibile con tutte le modalità di firma previste dalla normativa vigente, in particolare CAdES e PAdES.

Questo ulteriore approccio qui proposto richiede che la stazione o il servizio di verifica della firma abbiano la capacità di estrarre il dato CDA2 dal file PDF. In assenza, l'utente ha comunque accesso al documento in formato PDF.

Il processo proposto porta anche alla produzione di un documento (PDF) che veicola entrambi i contenuti in un unico file, semplificandone l'aspetto gestionale.

2.2.1 Contesto

La normativa vigente permette la firma elettronica qualificata di file PDF purché il loro contenuto sia "statico" (p.e. non contenga macro-istruzioni che ne possano alterare dinamicamente il contenuto).

La costruzione del documento PDF a partire dal documento CDA2 sposta l'elaborazione da una "semplice" trasformazione XSLT ad un vero e proprio servizio di conversione; a tale servizio di conversione è demandata la generazione del documento PDF compresa l'iniezione del documento CDA2 originario all'interno del template PDF, ottenendo un unico file auto-consistente adatto ad essere elaborato senza l'apporto di ulteriori informazioni sia in sede di firma che di verifica della firma.

Questa modalità di generazione del documento da sottoscrivere ha sia punti in comune che differenze rispetto alla firma in formato XML:

1. Anche in questo caso solo i nodi "catturati" dal processo di conversione concorrono alla generazione della componente di presentazione e quindi coinvolti nel meccanismo di "non ripudio" della firma, l'integrità è invece garantita sull'intero documento, grazie alle caratteristiche strutturali della sottoscrizione in modalità CAdES/PAdES;
2. Poiché la conversione è effettuata programmaticamente è possibile inserire nel template PDF elementi grafici distintivi del sottoscrittore o dell'organizzazione in cui opera;
3. Il documento PDF prodotto, pur col vantaggio di essere costituito da un unico file auto-consistente, ha dimensioni considerevolmente superiori al documento strutturato.

2.2.2 Fruizione

La fruizione del contenuto da parte dell'utente "umano" richiede l'impiego di un normale visualizzatore di file PDF. In funzione del formato di firma utilizzato, esso può coincidere con lo strumento di verifica della firma.

La fruizione del contenuto da parte dell'utente "programmatico" richiede l'estrazione della componente XML dal file PDF.

2.2.3 Formati di firma

Come per qualsiasi documento non XML la firma di file PDF può essere effettuata utilizzando uno dei tre formati previsti dalla normativa vigente:

- XAdES;
- PAdES;
- CAdES.

La firma di file PDF comporta delle scelte riguardanti il formato PDF-A concepito per l'archiviazione di documenti PDF per lunghi periodi di tempo.

Per quanto il presente documento non preveda mandatoriamente, come del resto la normativa vigente, che i documenti firmati siano in formato PDF-A, la soluzione tecnica è tale da garantire che i documenti PDF prodotti, qualora fossero in formato PDF-A, non perdano tale conformità con l'inserimento al loro interno della componente CDA2.

2.2.3.1 Firma XAdES

Poichè un file PDF utilizza un formato binario e non testuale i formati utilizzabili per la firma XAdES sarebbero Enveloping e Detached. Nessuno dei due formati è vantaggioso nei confronti dei formati PAdES e CAdES e pertanto la firma XAdES non è presa in considerazione per la casistica in esame.

2.2.3.2 Firma PAdES

Questo formato, anche se non diffuso quanto CAdES, è sicuramente quello più affine al fruitore del documento in quanto con un unico strumento (i.e. Adobe Reader) l'utente "umano" può ottenere la visualizzazione dei contenuti e la verifica della firma, mentre quello "programmatico" può estrarre in modo deterministico la componente strutturata, cioè il documento CDA2. Si osserva che la corretta verifica della firma da parte di un Adobe Reader dipende dalla sua corretta configurazione, in particolare dall'inserimento del plugin reso disponibile da DigitPA.

2.2.3.3 Firma CADES

Il formato CADES, rispetto al precedente PAdES, ha lo svantaggio di richiedere l'impiego di un client di firma per la verifica e rimozione della busta crittografica, per contro questa modalità di apporre e verificare le firme è largamente consolidata e disponibile all'interno di molti tool di mercato.

2.2.4 Vantaggi

Il processo garantisce l'integrità di tutto il documento; naturalmente il non ripudio è relativo alla sola componente di presentazione, esattamente come nel caso dello XAdES.

Il documento firmato è costituito da un unico file.

Nella componente di presentazione del documento è possibile inserire senza difficoltà elementi grafici specifici di un sottoscrittore o di un'organizzazione in cui operano i sottoscrittori in quanto gli elementi grafici sono inglobati nel file PDF e, con la sottoscrizione, se ne assicura l'integrità.

L'onere della conversione è pagato solo in fase di generazione del documento PDF da firmare mentre per l'apposizione della firma e le successive verifiche le prestazioni sono quelle di una firma CADES o PAdES.

La fruizione da parte dell'utente "umano" della componente di presentazione del documento richiede l'utilizzo di un normale visualizzatore di documenti PDF.

2.2.5 Svantaggi

Per l'utente "programmatico" l'estrazione del documento CDA2 dal file PDF richiede un passo di elaborazione ulteriore rispetto alla firma XAdES, da demandare o agli strumenti che devono accedere alla componente strutturata o al servizio di verifica della firma, che devono avere la capacità di mettere a disposizione i due contenuti in modo distinto e facilmente fruibile.

A differenza della firma XAdES dove vi è l'obbligo della pubblicazione del foglio di stile, a sua volta sottoscritto con firma elettronica qualificata, la "trasparenza" del processo di generazione dei file PDF e iniezione del relativo CDA2 è di più difficile raggiungimento; si potrebbe pensare alla pubblicazione delle specifiche di trasformazione ed, eventualmente, ad un servizio web tramite cui effettuare la trasformazione di CDA2 in PDF a riprova della correttezza dei servizi utilizzati. L'adozione di questa soluzione richiede quindi la presenza di procedure organizzative ben definite che assicurino la "correttezza" dell'intero processo.

2.2.6 Osservazione

Il programma che realizza la trasformazione da CDA2 a documento PDF (che cioè realizza o emula la trasformazione XSL-FO) è opportuno che "sigilli" il file PDF generato (p.e. con una riga di testo indicante la versione del programma di trasformazione stesso) e

che venga conservato nel sistema di configuration management dell'ente cui fa capo il sottoscrittore, al fine della tracciabilità e futura riproducibilità del processo di trasformazione.

2.2.7 Impatti

E' ragionevole che ogni dominio applicativo possa scegliere quale/i profilo/i realizzare in sede di firma: non necessariamente tutti e in particolare non quello qui proposto (PDF con CDA2 iniettato). D'altra parte tutti i profili devono essere gestiti in sede di verifica a garanzia dell'interoperabilità fra domini differenti.

Nel caso del CDA2 iniettato nel PDF si hanno due casistiche:

- Il profilo di interoperabilità scelto come preferenziale è quello proposto in questo capitolo.

In questo caso le postazioni di firma dovranno essere dotate della funzionalità di iniezione e quelle di verifica di quella di estrazione del CDA2 dal PDF. La modalità architetturale di realizzazione dipenderà dal contesto architetturale applicativo: p.e. funzionalità distribuita sulle postazioni oppure esposta da servizi in rete, a livello di ente/struttura (e.g. ospedale) oppure regionale, ...

Dovrà essere tenuto debito conto anche del fatto che in questo caso la funzionalità di iniezione, ma ben più ancora quella di estrazione, verranno pesantemente invocate e quindi dovranno essere particolarmente efficienti.

- Il profilo di interoperabilità scelto come preferenziale non è quello proposto in questo capitolo.

In questo caso le postazioni di firma non saranno necessariamente dotate della funzionalità di iniezione del CDA2 del PDF. Per le postazioni di verifica invece si avranno due casi:

- Postazioni di verifica non dotate della funzionalità di estrazione. Esse comunque consentiranno la consultazione del DCE solo all'utente umano (in formato PDF), ma non evidentemente rendere disponibile il CDA2 (che resta inserito "invisibile" nel PDF). In questo caso non si hanno accesso e fruizione del CDA2.
- Postazioni di verifica dotate della funzionalità di estrazione. Esse saranno in grado di trattare entrambe le forme del DCE (PDF e CDA2). La modalità architetturale con cui la funzionalità verrà resa disponibile, dipenderà dal contesto architetturale applicativo: p.e. funzionalità distribuita sulle postazioni oppure esposta da servizi in rete, a livello di ente/struttura (e.g. ospedale) oppure regionale, ...

Dovrà essere tenuto debito conto anche del fatto che in questo caso la

funzionalità di estrazione verrà assai raramente invocata e quindi non avrà necessità di essere particolarmente efficiente.

Il formato proposto si basa unicamente su specifiche pubbliche (cfr. ISO 32000) e, pertanto, non implica necessariamente l'acquisto di prodotti o librerie di terze parti.

La scelta di acquisire meta-lavorati dal mercato rispetto ad una realizzazione "ad hoc" è una decisione che sarà presa in autonomia da ogni specifico dominio sulla base di una valutazione costi/benefici.

Comunque, eventuali licenze di prodotti (e.g. librerie) atte a sostenere specificamente le funzionalità di iniezione ed estrazione avranno verosimilmente un costo proporzionale al numero ed alla tipologia di installazioni: e.g. poche licenze se viene esposto un servizio in rete, tante licenze se installate sulle postazioni di lavoro dell'utente.

2.3 Un altro approccio

[In questo capitolo e in altri come questo possono essere inserite ulteriori proposte di profilo per successive estensioni in nuove versioni del documento, seguendo lo schema del capitolo precedente]

3 Conclusioni

I profili di interoperabilità esaminati in questo documento non differiscono in efficacia, cioè sono tutti adeguati alla sottoscrizione di documenti CDA2.

Sono discusse nel seguito le problematiche di interoperabilità e normalizzazione.

3.1 Interoperabilità

Lo sforzo in essere da parte di HL7 Italia è finalizzato a promuovere e consentire la fruizione generalizzata di DCE CDA2, che a loro volta, in quanto referti, hanno la necessità di essere sottoscritti.

Ciò si estrinseca in:

- interoperabilità sintattica e semantica del DCE;
- interoperabilità del documento informatico sottoscritto;
- accessibilità al CDA2.

Interoperabilità sintattica e semantica dei DCE

Questo tema è oggetto dell'attività di standardizzazione di HL7-CDA2 e non è coperto da questo documento.

E' implicito che siano interoperabili DCE realizzati in piena conformità agli standard CDA2.

Interoperabilità del documento informatico sottoscritto

L'interoperabilità dei documenti informatici sottoscritti deriva dall'adozione dei formati definiti dalla normativa vigente (cfr. Deliberazione n.45 del 21/05/2009), che pertanto devono essere rispettati.

Il non ripudio della sottoscrizione implica la rappresentazione intelligibile del documento da sottoscrivere.

Accessibilità al CDA2

Ove non si adotti per il DCE CDA2 il formato XAdES, non viene sottoscritto direttamente il documento CDA2 (p.e. viene sottoscritto il ".pdf" e non il ".xml" che costituisce il CDA2).

In questi casi consegue la necessità di ulteriori normative di interoperabilità (cioè i "profili") che definiscano l'accessibilità al DCE CDA2 a partire dal documento informatico sottoscritto (p.e. l'accessibilità dal PDF al CDA2 iniettato). Il presente documento definisce la cornice entro la quale sviluppare tali normative, in termini di Regole Tecniche emesse da HL7 Italia.

La scelta del profilo di interoperabilità è condizionata dal dominio applicativo che, in funzione delle esigenze del servizio deve dare priorità alla fruizione da parte dell'utente umano piuttosto che a quello programmatico, scegliendo fra i profili normati da HL7 Italia.

A garanzia dell'interoperabilità dei documenti tra i vari domini applicativi, devono comunque essere accettati anche documenti conformi ai profili diversi da quelli utilizzati nel proprio dominio e normati da HL7 Italia.

Qui di seguito una tabella riassume i formati di firma suggeriti, in quanto più adatti al profilo di interoperabilità scelto:

	XAdES			PAdES	CAdES
	Enveloping	Detached.	Enveloped		
XML-CDA2	X	OK	OK	non applicabile	X
CDA2 in PDF	X			OK	OK
<i>R.F.U.</i> (<i>cf. cap. 2.3</i>)

3.2 Normalizzazione

Per semplificare la fruizione dei documenti per l'utente "umano", sarebbe opportuno che anche la presentazione delle informazioni fosse normalizzata. Per realizzare ciò sarebbe necessario che un'organizzazione *super partes* definisse e mettesse a disposizione le regole di presentazione dei documenti CDA2 che, restando al caso della sola firma in formato XAdES, sarebbe rappresentato dai file XSLT firmati da utilizzare per la trasformazione per ciascuna categoria documentale identificata.

Estendendo i profili di interoperabilità dei documenti CDA2 all'impiego di formati alternativi, è sostenibile che l'organizzazione che li adotti faccia uso di un motore di conversione in grado di produrre un "rendering" equivalente, anche se ovviamente non identico, a quello che sarebbe ottenuto applicando il foglio di stile normalizzato al documento CDA2 per la firma in formato XML.

In tal caso, a complemento del foglio di stile associato alla firma XAdES, dovrebbero essere definiti i gradi di libertà per l'inserimento di elementi grafici distintivi del sottoscrittore o della sua organizzazione di appartenenza.