Introduzione alla Firma Digitale

Aspetti Tecnici

Riferimenti	
Oggetto:	Firma Digitale
Modello Documento:	FIRMA-MO-001
Nome File:	**FIRMA-MO-001 rel 5.1BOZZA.doc**
Versione:	5.01
Ultimo aggiornamento:	31 marzo 2011
Data creazione:	26 settembre 2005
Autore:	Segreteria Tecnica Consorzio CBI

Il contenuto del presente documento costituisce materiale riservato ed il documento è sottoposto alla disciplina del Marchio CBI

Revisioni

Revisioni			
Vers.	Data	Autore	Descrizione
1.00	26/09/2005	ACBI	Allegato 3 alla Circolare CBI 6/2005
2.00	13/07/2006	ACBI	Allegato 1 alla Circolare CBI 6/2006 (Aggiunte precisazioni nei paragraf1 4.2, 4.3.1, 4.3.2 e 5.1.1.1)
3.00	04/05/2007	ACBI	Modifiche a seguito di quanto concordato dal GdL Firma Digitale nell'incontro tenuto a Milano in data 16 Aprile 2007 (Riorganizzazione del capitolo 4 ed in particolare del paragrafo 4.4 nel quale sono state esplicitate le regole di strutturazione dei messaggi e di gestione della firma per i Nuovi Servizi CBI)
4.00	23/07/2009	Segreteria Tecnica CBI	Modifiche a seguito della decisione di adottare dal 1° febbraio 2010 la solo firma attached monobusta nell'ambito dei nuovi servizi. Introduzione della possibilità di supportare da schema XSD eventuali limitazioni nell'uso della firma
5.00	07/07/2010	Segreteria Tecnica CBI	Modifiche a seguito della deliberazione CNIPA n°45 del 21 maggio 2009 e dell'incontro tecnico del GdL Standard, Architettura e GPA tenuto in data 30 giugno 2010. Estensione a tutti i servizi CBI del principio di controllo del mittente fisico dei flussi firmati (cfr. par. 4.8)
5.01	24/03/2011	Segreteria Tecnica CBI	Aggiunte precisazioni nei paragrafi 4.1 e 4.4 a seguito delle segnalazioni pervenute alla Segreteria Tecnica a fronte dei test di sistema 21 febbraio – 15 marzo 2011.

Indice dei Contenuti

1 INTRODUZIONE 4

1.1 Finalità del documento 4

1.2 Struttura del documento 4

2 Inquadramento generale 5

2.1 Quadro normativo di riferimento 5

2.2 Premessa 5

2.3 La Firma elettronica/digitale 6

2.3.1 Il processo di Firma 6

2.3.2 Interoperabilità 7

3 Soggetti e ruoli 7

3.1 Cliente 7

3.2 Banca Proponente 7

3.3 Banca Passiva 8

3.4 Titolare 8

4 Standard di Firma 9

4.1 Introduzione 9

4.2 Struttura logica della busta PKCS#7 10

4.3 Struttura logica della busta CADES-BES 11

4.4 Informazioni sulla firma nei messaggi CBI 12

4.5 Porting 13

4.6 Nuovi Servizi 15

4.6.1 Regole di gestione della firma digitale 15

4.6.2 Controlli in carico al soggetto ricevente 18

4.6.3 Restrizioni d'uso della firma digitale per i nuovi servizi 19

4.7 Tabella riepilogativa 20

4.8 Soggetti abilitati all'invio di flussi firmati 21

5 Processi ed attività 22

5.1 Tratta Cliente => Banca Passiva 22

5.2 Tratta Banca Passiva => Cliente 24

5.3 Tratta Cliente => Cliente 25

6 APPENDICE 26

6.1 Appendice A: documentazione tecnica di riferimento 26

1 INTRODUZIONE

Tenendo conto:

- dei sistemi di firma elettronica e/o digitale distribuiti da soggetti bancari e non;
- della diffusione del Servizio CBI – Corporate Banking Interbancario (di seguito solamente Servizio) presso la clientela;
- dell'evoluzione al Nuovo Servizio CBI, basato su una Nuova Architettura Tecnologica;
- delle richieste provenienti dal Mercato;

il Gruppo di Lavoro "Firma Digitale" (GdL) ha verificato l'opportunità di veicolare sul Nuovo CBI anche flussi[1] firmati digitalmente.

A tal fine sono state prese in considerazione diverse soluzioni di firma elettronica e/o digitale. Tuttavia, alla data, l'unico sistema di firma in grado di offrire un quadro di interoperabilità a livello tecnico e normativo, sia pure in ambito "domestico"[2], risulta essere quello definito dalle deliberazioni "CNIPA" in tema di firma digitale.

1.1 FINALITÀ DEL DOCUMENTO

Il presente documento fornisce una descrizione delle modalità di veicolazione, sul circuito CBI, di flussi sottoscritti con Firma, individuando i criteri di trattamento dei flussi firmati, in particolare per gli eventuali soggetti facilitatori che le banche vorranno incaricare per l'interconnessione con l'infrastruttura di rete.

1.2 STRUTTURA DEL DOCUMENTO

Il documento è strutturato come segue:

- inquadramento generale;
- architettura, soggetti e loro sintetica descrizione;
- definizione dello standard di firma previsto;
- processi ed attività.

[1] Con il termine "flussi" si intenderanno genericamente informazioni potenzialmente oggetto di firma digitale.
[2] A livello normativo, la soluzione CNIPA compliant, essendo sviluppata in aderenza alle disposizioni europee, assicura validità anche nei confronti degli altri paesi, pur se non automaticamente interoperabile dal punto di vista tecnico.

2 INQUADRAMENTO GENERALE

2.1 QUADRO NORMATIVO DI RIFERIMENTO

Il quadro normativo di riferimento, sul quale si basano le regole tecniche di gestione della firma digitale sul circuito CBI, è determinato dalle deliberazioni DigitPA (già CNIPA, Centro Nazionale per l'Informatica nella Pubblica Amministrazione) in tema di firma digitale e, più in generale, di "Regole per il riconoscimento e la verifica del documento informatico".

Ai fini di una ottimale comprensione di quanto riportato nel presente documento sono di seguito riportate le deliberazioni DigitPA di pertinenza, alle quali si rimanda qualora si desideri acquisire informazioni di dettaglio sull'argomento:

- ***Deliberazione 4 del 17 febbraio 2005:*** è la deliberazione in vigore fino al 30 agosto 2010. Prevede l'apposizione della firma nel formato PKCS#7 attached (buste .p7m);
- ***Deliberazione 34 del 18 maggio 2006 e relativo allegato:*** anch'essa in vigore fino al 30 agosto 2010, riguarda le regole tecniche per la definizione del profilo di busta crittografica per la firma digitale in linguaggio XML. Sul CBI ad oggi si è scelto di non gestire la firma digitale con busta in formato XML;
- ***Deliberazione 45 del 21 maggio 2009 ((Pubblicata sulla Gazzetta Ufficiale n. 282 del 3 dicembre 2009):*** è la deliberazione in vigore dal 30 agosto 2010 (3 dicembre 2009 + 270 giorni ART. 29 commi 1,3). Si passa dallo standard PKCS#7 allo standard CAdES-BES. Per quanto riguarda la busta XML si fa riferimento allo standard XAdES.

2.2 PREMESSA

Sui motivi dell'introduzione della Firma si ritiene opportuno riepilogare le considerazioni che ne hanno determinato i presupposti :

- già oggi molte Banche offrono alla clientela servizi di Remote Banking che utilizzano in vario modo la Firma;
- gli uffici legali di molte Banche hanno sempre individuato nei sistemi di riconoscimento (utente e dati/utente) oggi in essere nel Servizio "margini di rischio", accettati solo in quanto l'operatività attuale è coperta da una prassi diffusa ed "avallata" dal CBI; per contro, la normativa italiana e la normativa europea in materia di Firma sono elementi che conferiscono "certezze di diritto" ben gradite;
- la Firma è oggetto di diffusione presso le Aziende clienti attraverso canali non bancari (p.e. Camere di Commercio), con tutto quello che ne consegue dal punto di vista tecnico[3] se le Aziende stesse dovessero chiederne il suo utilizzo nei colloqui telematici con le Banche;
- la Firma ha iniziato a coinvolgere alcune procedure o a manifestarsi come esigenza/prerequisito per la veicolazione di dati diversi da quelli CBI, ma logicamente a loro strettamente collegati;
- per la prima volta, utilizzando flussi elettronici, è possibile smaterializzare tutti i documenti che, per obbligo di forma o per esigenze probatorie, devono essere scritti e sottoscritti. A tal proposito deve essere considerato, inoltre, il nuovo quadro normativo circa la rispondenza dei flussi elettronici firmati ai requisiti di validità formale e sostanziale (D.LGS. 82 del 7/3/05 – Codice della PP.AA digitale – CAD);
- l'adozione della Firma Digitale rende obsoleti i sistemi/algoritmi di sicurezza attualmente in uso;

[3] Le valutazioni commerciali circa gli impatti della Firma esulano dalle competenze del GdL; i giudizi sono espressi solo in chiave puramente tecnologica.

- la realizzazione di Nuovi Servizi CBI ad elevato valore aggiunto per le aziende rende opportuno prevedere anche la funzionalità di Firma Digitale quale elemento performante dell'offerta bancaria verso la propria clientela;
- l'esistenza di nuove funzioni CBI per le quali, a livello di sistema, è previsto l'utilizzo della Firma Digitale (es. fatture elettroniche, ecc.).

2.3 LA FIRMA ELETTRONICA / DIGITALE

2.3.1 Il processo di Firma[4]

Per firmare un documento il titolare, dopo essersi fatto rilasciare un certificato elettronico, deve poter attivare le seguenti procedure:

1. generare l'impronta del documento elettronico da firmare (Hash: condensato di lunghezza fissa del documento. Esso risulta unico per uno specifico documento e non è possibile risalire al documento a partire dall'hash medesimo);
2. cifrare, con la propria chiave privata, l'impronta del documento elettronico;
3. creare una "busta elettronica" (busta crittografica) che contiene il documento (se si utilizza lo standard PKCS#7 o CAdES-BES in modalità attached), la Firma e il certificato. Il certificato è un documento (elettronico) nel quale un'entità (Certificatore) dichiara che una specifica chiave pubblica appartiene ad un determinato individuo identificato con certezza.

Il destinatario del documento elettronico firmato deve essere posto in grado di:

1. aprire la "busta crittografica";
2. aprire il certificato e:
   - leggere l'identità del Titolare e la validità temporale del suo certificato;
   - estrarre la chiave pubblica del mittente;
3. decifrare l'impronta del documento elettronico con la chiave pubblica del Titolare;
4. calcolare l'impronta del documento elettronico e verificare il valore ottenuto con quello firmato ai fini dell'integrità del messaggio;
5. verificare (al momento della ricezione del documento, o successivamente) la validità del certificato utilizzato per la Firma. Possono essere seguite due modalità:
   - l'accesso tramite protocollo LDAP alle speciali liste (CRL – Lista dei Certificati Revocati e CSL – Lista dei certificati sospesi) redatte da ogni Certificatore, con verifica di presenza del certificato all'interno di tali liste. In caso negativo, il certificato deve essere considerato valido e, conseguentemente, anche il documento elettronico può essere considerato valido a norma di legge;
   - verifica tramite protocollo OCSP (Online Certificate Status Protocol – purché supportato dalla Certification Authority di riferimento), in grado di fornire "in tempo reale" l'informazione sulla validità del certificato, o di una sua eventuale revoca/sospensione.

Gli step descritti sono normalmente svolti da specifici prodotti software che possono apporre, in modo semplice, una firma per ogni singolo documento o da procedure in grado di firmare singolarmente interi flussi di documenti (es. fatture). Analoga procedura può essere utilizzata nell'ambito dei processi connessi alla verifica.

[4] Le note che seguono sono inserite a scopo divulgativo e descrivono, senza pretese "scientifiche", il processo di Firma così come previsto dalla normativa italiana.

2.3.2 Interoperabilità

La presenza di molteplici Certificatori, ciascuno con le proprie soluzioni tecnologiche, può sollevare un problema d'interoperabilità in fase d'apposizione della Firma da una parte e di verifica dei documenti firmati dall'altra.
In ogni caso oggi la capacità di riconoscere e verificare buste firmate utilizzando strutture, dati e tecnologie di differenti Certificatori è ampiamente diffusa - grazie anche ai lavori di enti tecnici come Assocertificatori, (recepiti normativamente con Crc. 19 giugno 2000 n. CNIPA/CR/24 e successive Deliberazione CNIPA n. 4/2005 del 17 febbraio 2005 e n. 45/2009 del 21 maggio 2009) - le modalità per garantire l'interoperabilità delle singole componenti di un sistema di firma (carte a microprocessore, lettori di carte, applicazioni) sono allo studio.

La componente di riconoscimento e verifica delle buste firmate è considerata interoperabile se sono garantiti i seguenti passi:

1. riconoscere il formato di una "busta elettronica";
2. aprire ed estrarre le informazioni contenute nella busta elettronica;
3. "leggere" il contenuto del certificato ed estrarre correttamente l'identità della persona che ha firmato e la relativa chiave pubblica;
4. verificare la Firma riconoscendo l'algoritmo utilizzato per ottenere l'impronta del documento elettronico e applicare lo stesso algoritmo al documento estratto dalla busta elettronica onde verificare la corrispondenza delle due impronte;
5. verificare la validità del Certificato mediante la modalità prevista dal Certificatore allo scopo.

Benché gli attuali standard internazionali garantiscano i precedenti cinque punti in modo automatico, non tutte le applicazioni di verifica delle firme li realizzano in maniera adeguata.

La costituzione di un apposito Elenco CBI dei Certificatori si pone quindi quale base per una piena interoperabilità delle soluzioni di mercato nell'utilizzo della Firma ed è garanzia altresì di uno sviluppo coordinato e sicuro dei sistemi di Firma all'interno del Servizio CBI.

3 SOGGETTI E RUOLI

Si evidenziano di seguito i compiti di ciascun soggetto presente nell'ambito del Servizio CBI relativamente alla funzionalità della firma digitale.

3.1 CLIENTE

Il Cliente è la persona fisica o giuridica che ha sottoscritto il contratto CBI con una Banca Proponente e con una o più Banche Passive

3.2 BANCA PROPONENTE

È il soggetto che, nell'ambito del Servizio CBI, offre la funzione di Firma al Cliente.

Al fine di rendere disponibile tale funzione, la Banca deve organizzarsi per:

- rendere disponibili al Cliente gli idonei strumenti (kit di firma: dispositivo sicuro di Firma e software per l'apposizione/validazione della Firma) rilasciati da Certificatori iscritti all'Elenco CBI ovvero,
- verificare l'idoneità di eventuali strumenti già in possesso dei Titolari (v. oltre per la relativa nozione), accertando che:
  - il Certificatore sia presente nell'Elenco dei certificatori abilitati dal CBI (elenco disponibile sul sito consortile www.cbi-org.eu nella sezione "Adesioni al CBI") ;
  - il rilascio del Certificato Digitale sia avvenuto ai sensi della legge 197/91, delle norme del Regolamento del Marchio CBI – Sezione "Certificatori" – nonché della relativa Circolare CBI prot. 3/2004;
- veicolare verso il sistema flussi firmati esclusivamente:
  - con Certificati che rispettino i requisiti indicati ai punti precedenti;
  - verificando la Firma e controllando la validità del Certificato utilizzato per la firma nel caso in cui detto controllo del Certificato non sia già stato effettuato al momento dell'apposizione della Firma;
  - conservando evidenza dell'esito di tali verifiche in associazione all'istante temporale in cui sono state completate, valorizzando l'apposito tag presente nel messaggio xml denominato "riferimento temporale"[5];
- mettere a disposizione del Cliente i contenuti dei flussi firmati di cui il Cliente stesso è destinatario.

3.3 BANCA PASSIVA

È il soggetto che si pone in grado di archiviare i flussi firmati e procedere al trattamento degli stessi. La Banca Passiva non ha l'obbligo di effettuare il controllo del Certificato che accompagna la Firma apposta ai supporti, che grava invece - per espressa disposizione delle Norme del Servizio - sulla Banca Proponente.

La Banca Passiva è obbligata a ricevere, verificare la firma e confermare la ricezione dei flussi ad essa inviati, anche nel caso in cui l'eventuale ulteriore controllo del Certificato effettuato dalla medesima Banca Passiva desse esito negativo.

La segnalazione dell'anomalia riscontrata nel supporto logico firmato – qualora un Certificato od una Firma non dovessero risultare validi – potrà essere effettuata tramite canali CBI utilizzando codici d'errore specifici. L'eventuale scarto dovrà essere effettuato anche nel caso in cui, in presenza di Firme multiple, una Firma non dovesse risultare valida.

Le fasi di verifica della Firma (e, quindi, la loro autenticità ed integrità) ed archiviazione possono essere delegate ad altra struttura, esterna alla Banca.

Nel caso in cui la Banca Passiva decida di avvalersi della facoltà di apposizione della Firma sui propri flussi, è tenuta a dotare un proprio Titolare (Cfr. paragrafo successivo) di un Certificato per la Firma rilasciato da uno dei Certificatori convenzionati ed eventualmente degli apparati necessari (kit di firma o sistemi informatici) per l'apposizione di firme automatiche massive.

3.4 TITOLARE

Considerate:
- le caratteristiche della Firma ed in particolare quella della titolarità dei poteri di firma attribuibile esclusivamente a persone fisiche;

[5] L'apposizione del "riferimento temporale" attesta sia l'avvenuta ricezione del flusso firmato da parte della Banca Proponente sia la regolarità del procedimento di firma, anche per quanto riguarda i relativi controlli.

– le finalità del presente documento;

per Titolare si intende il firmatario, cioè la persona fisica a cui sono attribuiti poteri di Firma e che ha accesso ad un dispositivo sicuro per la creazione della medesima Firma.

4 STANDARD DI FIRMA

4.1 INTRODUZIONE

Da un punto di vista strettamente tecnico lo scambio dei flussi sulla rete CBI può essere assistito da firma digitale apposta secondo i seguenti standard:

- **PKCS#7** v.1.5 (Public-Key Cryptography Standards) definito dalle specifiche RFC 2315;
- **CAdES-BES** definito nella norma ETSI TS 101 733 V1.7.4 e basato sulle specifiche RFC 3852 e RFC 2634 e successive modificazioni.

Entrambi gli standard permettono di lavorare utilizzando due modalità tecniche alternative, denominate "attached" e "detached".
Con la modalità attached i dati sottoposti a firma sono inseriti nella busta, mentre nella detached sono esterni alla stessa e possono pertanto essere veicolati separatamente.

L'uso di una specifica modalità, unitamente alle regole di obbligatorietà/facoltatività di apposizione della firma digitale è demandata alle norme tecniche che regolano l'erogazione dei singoli servizi.

Vale la pena osservare che le deliberazioni di DigitPA prevedono l'utilizzo della sola modalità "attached". Tuttavia l'esigenza di ottimizzazione delle fasi di veicolazione di talune tipologie di flussi sul circuito CBI rendono opportuno prevedere anche l'utilizzo della modalità "detached". Ciò non pone problemi di compliance con le direttive di DigitPA poiché è possibile passare in modo biunivoco da una firma "attached" a una "detached".

Per quanto riguarda i criteri di applicazione della firma, i controlli, la verifica della validità dei certificati nonché le attività delle Certification Authority si rinvia alle apposite norme del Servizio CBI. Nel seguito del documento verranno descritte la tipologia di firma prescelta nonché modalità concernenti l'applicazione della firma digitale sui flussi oggetto di porting e sui flussi relativi ai Nuovi Servizi CBI.

Si osserva che con l'entrata in vigore della deliberazione n° 45 del 21 maggio 2009 il documento informatico dotato di firma apposta secondo lo standard PKCS#7 non viene più inteso – stante i chiarimenti forniti per le vie brevi da DigitPA – quale documento sottoscritto con firma digitale, ma come "documento informatico cui è apposta una firma elettronica" in quanto tale "liberamente valutabile in giudizio" (art. 21, comma 1 del CAD Codice dell'Amministrazione Digitale).

L'affiancamento del nuovo formato CAdES-BES al formato PKCS#7 (e non la sua sostituzione) rappresenta pertanto una scelta puramente tecnica ed essenzialmente legata alla gestione del pregresso (flussi firmati prima dell'entrata in vigore della deliberazione n° 45 del 21 maggio 2009 e veicolati successivamente).

Analogamente, una busta CAdES-BES che utilizzi SHA-1 invece che SHA-256 è tecnicamente valida e quindi i flussi firmati utilizzando tale algoritmo non devono essere scartati, ancorché la loro validità sul piano legale possa essere individuata ad un livello inferiore rispetto a quello proprio dei flussi generati con SHA-256.

In conclusione, a prescindere dalla valenza giuridica stabilita dalla ricordata deliberazione n° 45 del 21 maggio 2009, la verifica che la busta rispetti le indicazioni della stessa non rientra nella sfera di attività della Rete CBI e non deve dunque generare scarti.

4.2 STRUTTURA LOGICA DELLA BUSTA PKCS#7

Rimandando al RFC2315 per i dettagli tecnici in merito allo standard PKCS#7 v.1.5 e per la descrizione esaustiva della busta in sintassi ASN.1, di seguito sono riportate alcune figure che illustrano la struttura logica della busta PKCS#7 nei due casi di firma attached e detached.

Struttura logica della busta PKCS#7 v.1.5 con firma attached

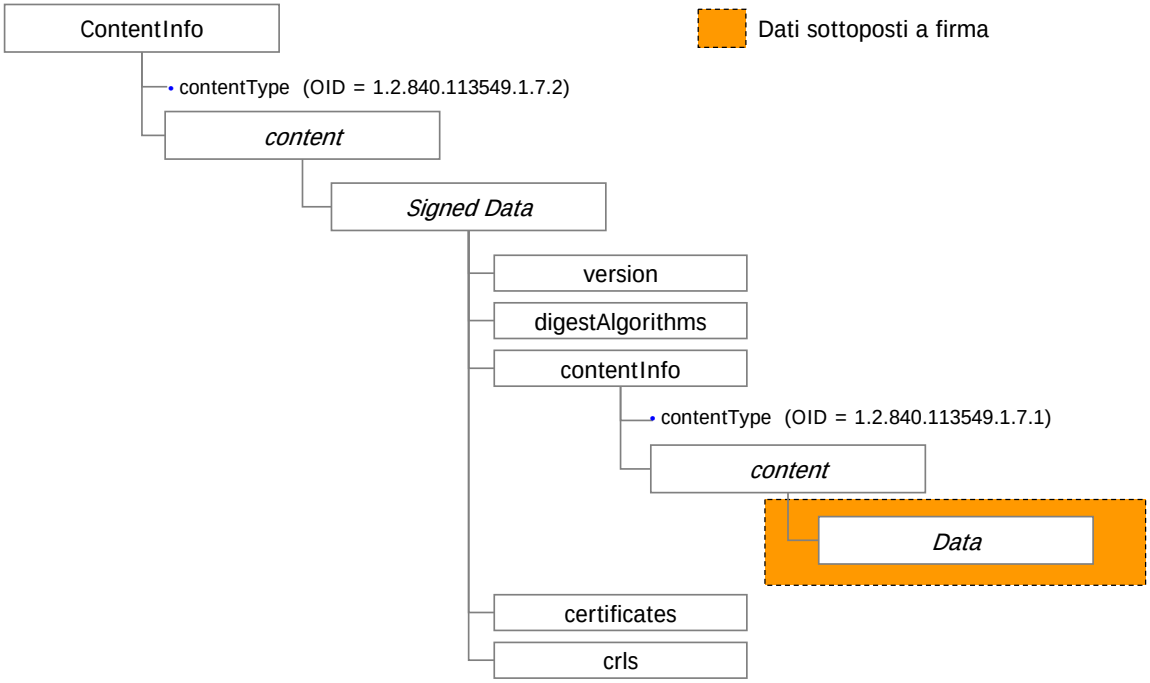


Figura 1

Struttura logica della busta PKCS#7 v.1.5 con firma detached

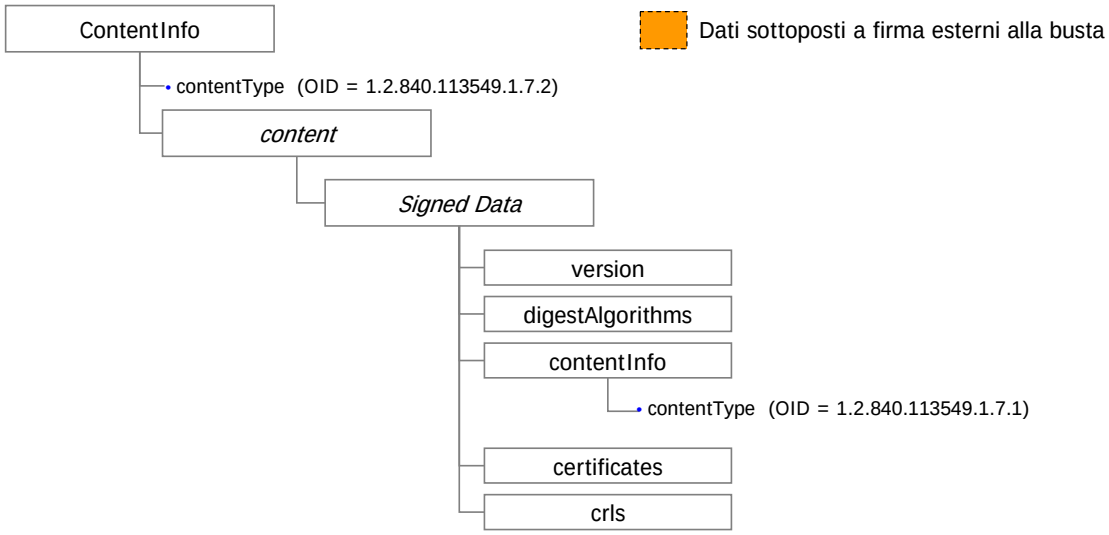


Figura 2

4.3 STRUTTURA LOGICA DELLA BUSTA CADES-BES

La struttura della busta CAdES-BES è analoga a quella della busta PKCS#7. Rimandando al RFC 3852 per i dettagli tecnici in merito allo standard CAdES-BES e per la descrizione esaustiva della busta in sintassi ASN.1, di seguito sono riportate alcune figure che illustrano la struttura logica della busta CAdES-BES nei due casi di firma attached e detached.

Struttura logica della busta CADES-BES in modalità attached

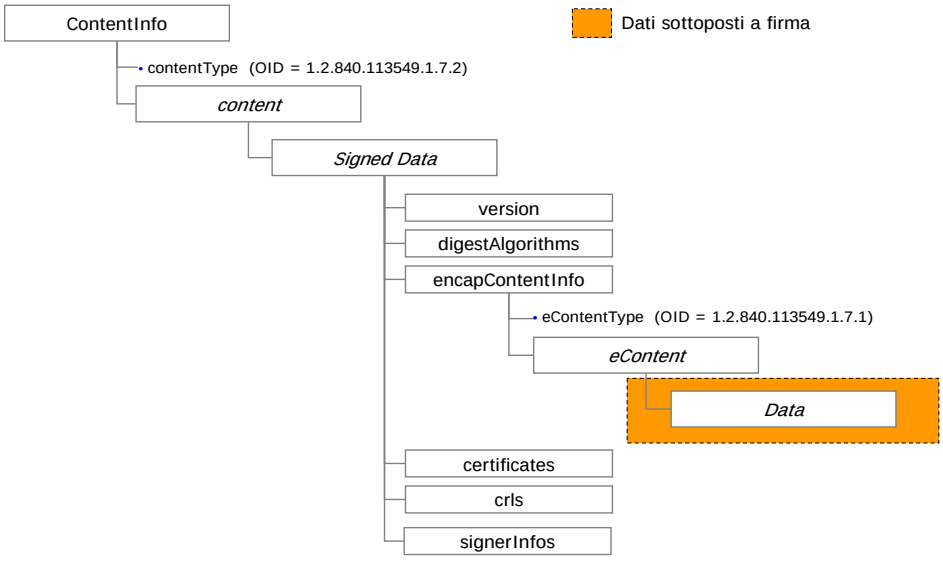


Figura 3

Struttura logica della busta CADES-BES in modalità detached

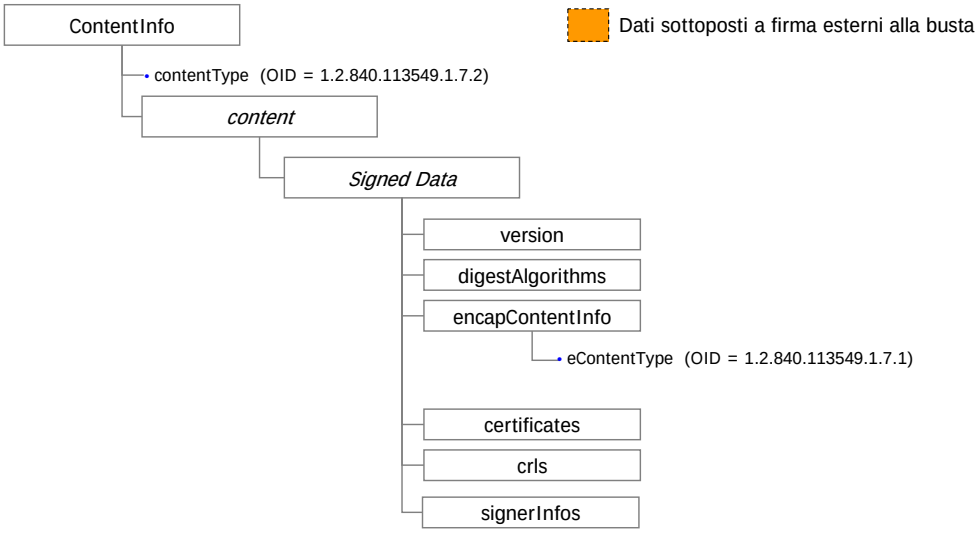


Figura 4

4.4 INFORMAZIONI SULLA FIRMA NEI MESSAGGI CBI

Per tutti i Servizi CBI che prevedono l'uso della firma digitale, la struttura XML dei messaggi è definita in modo da consentire l'inserimento di tutte le informazioni relative alla firma in un blocco strutturato come segue:

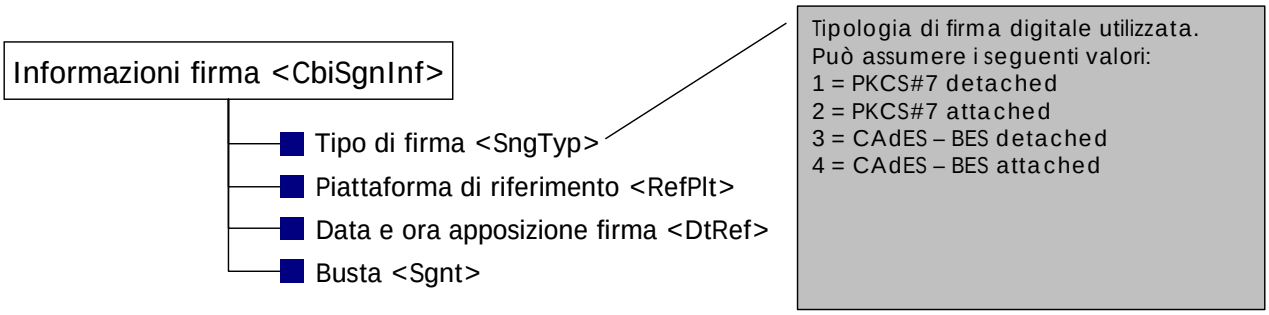


Figura 5

Le informazioni contenute in questo blocco sono le seguenti:

- Tipo firma; può assumere i seguenti valori:
  - 1 = PKCS#7 detached
  - 2 = PKCS#7 attached
  - 3 = CAdES-BES detached
  - 4 = CAdES-BES attached
- Piattaforma di riferimento: è la piattaforma su cui è stata generata la firma; può assumere il seguente valore:
  - A=ASCII/UTF-8
- Data e ora apposizione firma

- Firma/Busta: tag che contiene il file **codificato in Base64**[6]

Si osserva come il blocco così strutturato consente una valorizzazione potenzialmente ambigua che consiste nel dichiarare – tramite il campo "Tipo di firma" – la tipologia di firma non congruente all'effettiva modalità utilizzata per la generazione della busta.

Si rende pertanto necessario presentare un criterio univoco che permetta di valutare la modalità con la quale la firma è stata apposta sul flusso.
Ciò in considerazione del fatto che per ogni servizio CBI possono essere definite specifiche limitazioni relative alla modalità con la quale è consentito apporre la firma.

Si afferma quindi che il tipo di firma apposta è definito dal valore assunto dal campo "Tipo di firma", indipendentemente dall'effettivo contenuto del campo "Busta" <Sgnt>.

A titolo di esempio, qualora una firma venga dichiarata attached nel tag "Tipo di firma" nell'ambito di un servizio CBI che non preveda tale modalità di apposizione, l'entità logica firmata deve essere fatta oggetto di scarto.

Inoltre, qualora il valore assunto dal campo "Tipo di firma" non risulti coerente con l'effettiva tipologia di firma presente nella Busta, l'entità logica firmata deve essere fatta oggetto di scarto.

Alla luce delle possibilità offerte dagli standard PKCS#7 e CAdES-BES si precisa infine che:

- è possibile inserire più firme "parallele" nella stessa busta;
- l'introduzione da parte del mittente di firme annidate in una busta fornisce al ricevente il diritto allo scarto dei dati firmati, secondo le modalità previste dal servizio in esame.

4.5 PORTING

Per la definizione dei criteri e delle modalità con le quali deve essere realizzato il "porting" degli attuali Servizi CBI sulla Nuova Architettura, si veda apposito documento tecnico PORTING-MO-001.

Relativamente alla veicolazione delle attuali funzioni firmate digitalmente sulla Nuova Architettura CBI, si è condivisa la seguente modalità:

- Il file (contenente i supporti logici) viaggia in chiaro
- La modalità di firma prescelta è la detached
- Per la codifica della busta crittografica deve essere utilizzato il formato alfanumerico ottenuto applicando la trasformazione BASE 64 (RFC 1421, RFC 2045) al formato ASN.1 (ISO/IEC 8824) in rappresentazione binaria (ISO/IEC 8825, BER - DER)
- I dati sottoposti a firma sono:
  - Intero supporto logico, inclusi record di testa e record di coda
- La busta detached viene veicolata all'interno del messaggio XML che accompagna il file contenente i supporti logici

Pertanto i flussi relativi al porting firmati digitalmente saranno veicolati sulla Nuova Architettura CBI come di seguito rappresentato.

---

[6] *Pertanto il processo di generazione della firma prevede i seguenti step:*
- *produzione della busta con codifica binaria*
- *codifica della busta così ottenuta in Base64*
- *inserimento della stringa ottenuta nel tag firma/busta.*

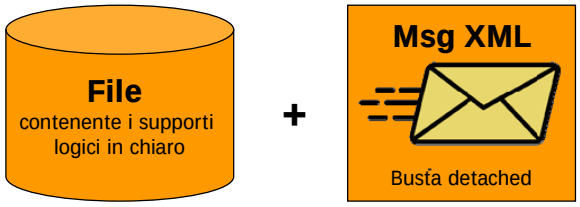


Figura 6

La seguente Figura rappresenta il flusso logico del processo di firma, finalizzato alla generazione della busta detached.

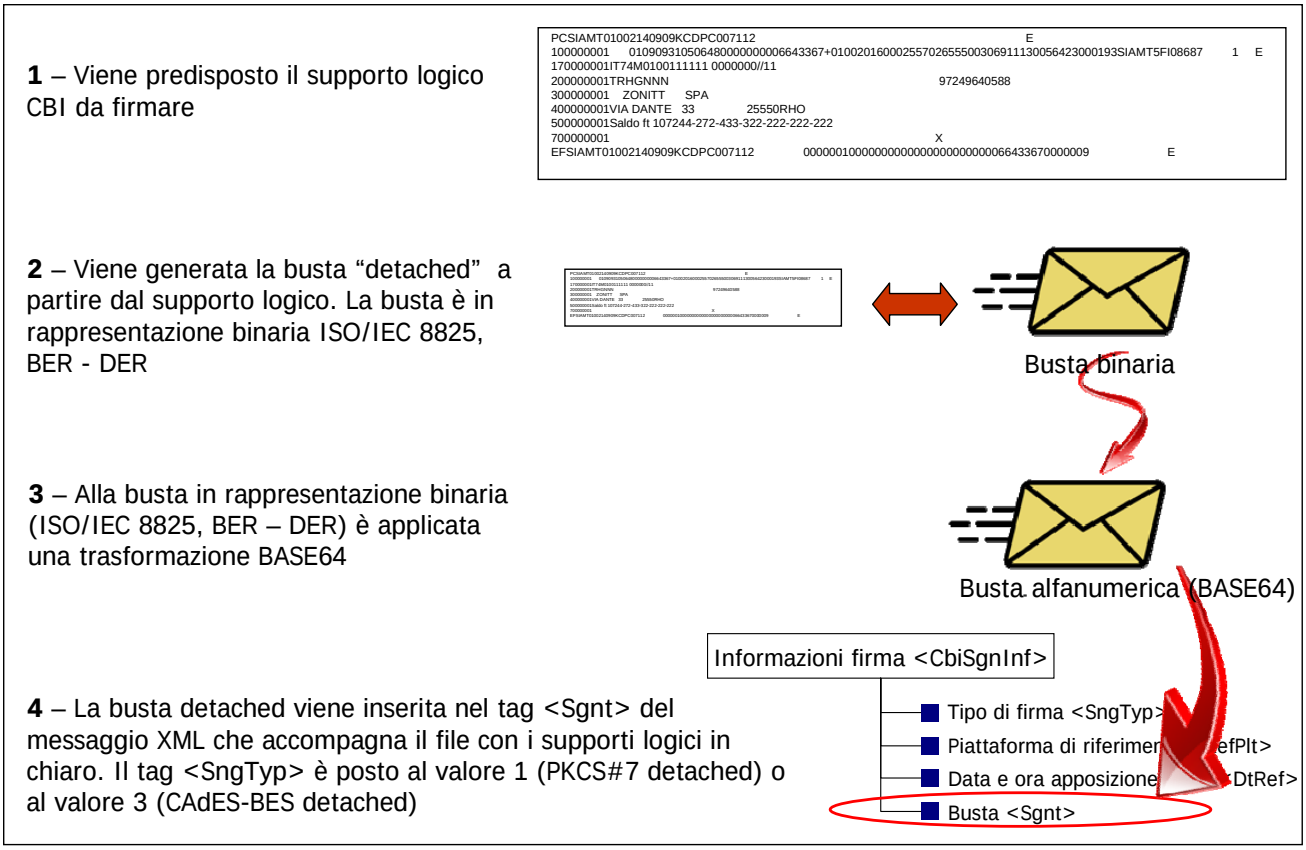


Figura 7

I dati contenuti nella busta PKCS#7 detached sono:
- Hash crittografato del supporto logico (uno per ogni firmatario)
- Certificato (uno per ogni firmatario)

La busta così ottenuta previa codifica in BASE64 prenderà il nome del flusso logico a cui si riferisce ed assumerà l'estensione .p7s, riservata alle buste "detached".

Le informazioni relative alla firma sono inserite in uno specifico blocco contenuto nel messaggio XML di accompagnamento al file, come descritto in Figura.

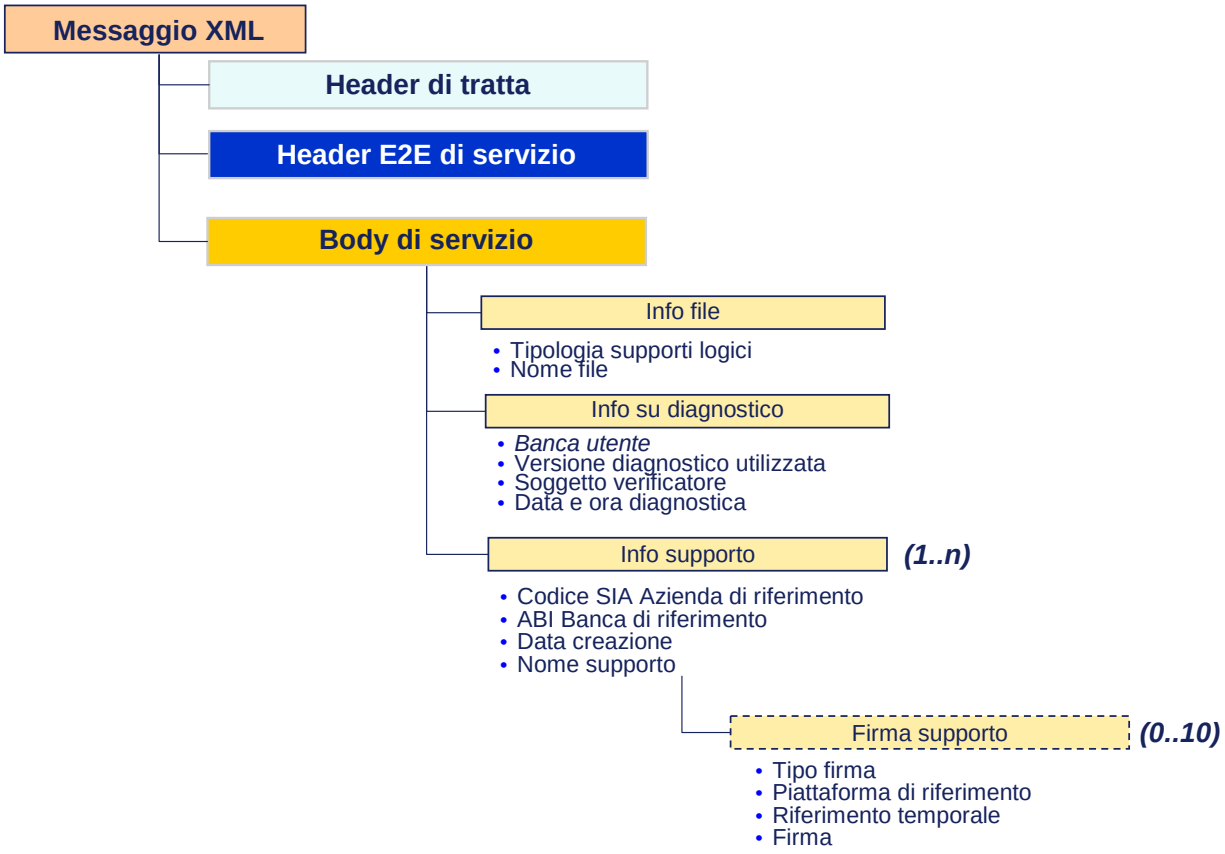


Figura 8

4.6 NUOVI SERVIZI

Dal punto di vista dell'applicazione della firma digitale i Nuovi Servizi CBI si differenziano profondamente dai servizi Porting in quanto i dati sottoposti a firma sono strutturati in formato XML e rappresentano parte integrante del messaggio di richiesta di servizio.

Appare pertanto necessario definire un "framework" costituito da regole valide per la gestione della firma digitale nell'ambito di tutti i Nuovi Servizi CBI.

4.6.1 Regole di gestione della firma digitale

Al fine di garantire la corretta gestione della firma digitale e l'interoperabilità tra i sistemi operanti sul circuito CBI, nel presente paragrafo viene definito un insieme di regole.
Le prime devono essere rispettate in fase di definizione degli standard dei messaggi che caratterizzano ogni Nuovo Servizio; le rimanenti riguardano invece le modalità di composizione dei messaggi contenenti blocchi di informazioni relative alla firma.

Le uniche modalità ammesse per l'apposizione della firma digitale nell'ambito dei nuovi servizi XML CBI sono le seguenti:

- PKCS#7 attached
- CAdES-BES attached

In entrambi i casi non possono essere associate più buste ad uno stesso messaggio logico (cfr. par. 4.6.3).

4.6.1.1 Struttura dei messaggi

Nel presente paragrafo vengono enunciate le regole di strutturazione dei messaggi XML[7] che devono essere rispettate nella definizione dei tracciati associati ad ogni Nuovo Servizio CBI.

Regola 1

All'interno del messaggio XML occorre definire in maniera univoca i dati sui quali è possibile apporre la firma.
Tali dati devono essere contenuti in un unico blocco (tag XML) che rappresenta l'entità logica (messaggio logico) da firmare e verrà - per semplicità - nel seguito indicato come **<DATA>.**
La scelta di racchiudere i dati da firmare in un unico tag root riveste fondamentale importanza in quanto consente di isolarli dal resto del messaggio ottenendo una struttura XML indipendente e "well formed".

Regola 2

Nella struttura del messaggio di richiesta servizio il blocco (i blocchi) con le informazioni sulla firma - di seguito **<SIGINFO>** - deve trovarsi allo stesso livello gerarchico del blocco <DATA> da firmare. Per la composizione di ogni blocco <SIGINFO> si faccia riferimento al paragrafo 4.2 del presente documento.

Regola 3

I dati sottoposti a firma e le informazioni sulla firma devono essere racchiusi in un blocco che rivesta la funzione di "Envelope" – di seguito **<ENVEL>** - in modo da rispettare la seguente struttura:

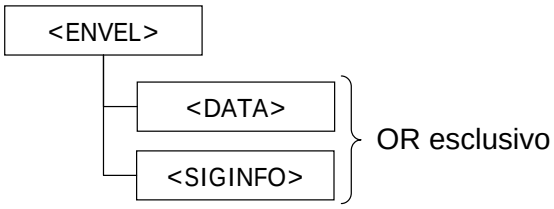


Figura 9

Viene di seguito riportato un esempio di codice XSD con cui è possibile modellare tale struttura:

```
<xs:element name="ENVEL" type="EnvelType"/>

<xs:complexType name="EnvelType">
        <xs:choice>
```

[7] *In generale l'apposizione della firma può essere prevista sia per i messaggi di richiesta servizio che per i messaggi di risposta applicativa*

```
        <xs:element name="DATA" type="DataType"/>
        <xs:element name="SIGINFO" type="SigInfoType"/>
        </xs:choice>
</xs:complexType
```

Si osserva come la struttura fissata dalla **regola 3** non consenta la presenza contemporanea di entrambi i blocchi <DATA> e <SIGINFO>, pertanto **nel caso in cui la firma digitale sia apposta sul messaggio logico, il blocco <DATA> non può essere presente nel messaggio XML.**

Si osserva infine come, in coerenza con le modalità di veicolazione dei flussi previste per i Nuovi Servizi CBI (Cfr. doc. STPG–MO–001 – Nuovi Servizi Parte Generale), il blocco <ENVEL> sia localizzato nel file qualora la richiesta di servizio venga inviata in modalità "file e messaggio".

4.6.1.2 Ulteriori regole per facilitare la gestione della firma

Una volta espresse le tre condizioni che concorrono alla determinazione della struttura del messaggio, allo scopo di facilitare la gestione della firma vengono poste altre condizioni di base il cui rispetto è necessario affinché i controlli in carico al ricevente possano essere effettuati secondo quanto espresso nel successivo paragrafo.

Regola 4

La struttura <DATA>, contenente i dati sui quali è possibile apporre la firma, deve soddisfare la seguente condizione:

deve esistere un file di schema xsd nel quale il tipo complesso <DATA> è definito come istanziabile in modalità "stand alone", indipendentemente dal resto del messaggio XML (messaggio fisico).

In altre parole deve essere possibile generare un file XML:

- contenente un'istanza del tipo complesso <DATA>
- validabile utilizzando il file/i file di schema nel quale il tipo complesso <DATA> è stato definito[8]

I dati sottoposti a firma devono quindi rappresentare una struttura interpretabile da un parser XML senza ulteriori aggiunte e con l'ausilio dei file di schema nei quali la struttura stessa è stata definita.

Da un punto di vista strettamente tecnico, la condizione appena esposta si traduce nella seguente:

deve esistere un file di schema nel quale l'elemento complesso <DATA> è definito direttamente al di sotto del tag <xsd:schema> che rappresenta il tag root per l'intero file[9].

Il rispetto della condizione appena espressa si rivela di fondamentale importanza nella gestione delle firme attached poiché permette di validare ed eventualmente conservare[10] i dati sottoposti a firma – contenuti nella busta – in modo totalmente indipendente dal resto del messaggio CBI.

---

[8] *La definizione del tipo complesso <DATA> potrebbe essere "distribuita" su più file di schema*

[9] *cfr. specifiche W3C reperibili all'indirizzo http://www.w3.org/TR/2004/REC-xmlschema-0-20041028/*

[10] *Si ricorda tuttavia che le tematiche inerenti la conservazione dei dati firmati non rientrano nella sfera di competenza del CBI*

4.6.1.3 Dati sottoposti a firma

Vengono in questa sezione definiti nel dettaglio i dati da sottoporre a firma. Le regole di seguito descritte devono essere rispettate da tutto il Sistema poiché l'inclusione o l'esclusione di anche un singolo carattere nello stream dei dati firmati rischia di invalidarne la verifica.

La **regola 4**, esposta nel paragrafo precedente, permette di inserire nella busta PKCS#7 o CAdES-BES un file XML completo, comprensivo di eventuale intestazione indicante l'encoding utilizzato (es. *<?xml version="1.0" encoding="UTF-8"?>*).

Si giunge pertanto a definire la seguente regola:

Regola 5

i dati sottoposti a firma devono rappresentare uno stream (o un file[11]) di dati in formato XML e validabili tramite lo schema (o gli schema) nel quale è definita la struttura <DATA>.

4.6.2 Controlli in carico al soggetto ricevente

La struttura imposta dalla **regola 3** rende in generale possibili i seguenti due casi:

1. presenza del blocco <DATA>
2. presenza del blocco <SIGINFO>

L'OR esclusivo che lega i due blocchi esclude infatti la presenza di entrambi. Nel corso dei seguenti 2 sottoparagrafi sono riportati i controlli in carico al soggetto ricevente in entrambi i casi sopra citati.

4.6.2.1 Presenza del solo blocco <DATA> (entità logica)

In questo caso sui dati non è apposta alcuna firma, pertanto sul blocco <DATA> devono essere applicati i controlli XSD e applicativi previsti dallo specifico Servizio CBI. Qualora il Servizio CBI contempli l'apposizione obbligatoria della firma, deve essere segnalato l'errore secondo le modalità previste dal Servizio stesso.

4.6.2.2 Presenza del solo blocco <SIGINFO> (informazioni firma)

I passi logici da effettuare in questo caso sono di seguito riportati:

- verifica che le firme siano apposte in modalità attached;
- estrazione dell'entità logica firmata dalla busta;
- validazione XSD della struttura o file XML estratto utilizzando lo schema nel quale la struttura sottoposta a firma è definita;
- validazione applicativa della struttura XML estratta applicando i controlli previsti dallo specifico Servizio;

[11] *Da un punto di vista di rappresentazione binaria un file xml può contenere informazioni aggiuntive come ad esempio il BOM (Byte Order Mark). Per i file con codifica UTF-8 il BOM, se presente, è rappresentato da una sequenza di tre byte: 0xEF 0xBB 0xBF*

- verifica di tutte le firme contenute nella busta secondo le modalità stabilite dalla normativa e dallo standard di firma utilizzato.

4.6.3 Restrizioni d'uso della firma digitale per i nuovi servizi

Nel corso del 2009 i competenti Gruppi di Lavoro CBI hanno concordato una apposita revisione delle regole tecniche con le quali apporre la firma digitale sulla totalità dei flussi relativi ai nuovi servizi CBI, interamente strutturati in XML. In particolare è stato deciso di prevedere l'impiego della sola modalità attached nonché l'utilizzo di una sola busta di firma. Le principali motivazioni che hanno condotto a tale decisione sono di seguito riportate:

- la modalità detached potenzialmente pone alcuni problemi tecnici di gestione poiché durante la veicolazione l'insieme dei dati sottoposti a firma potrebbe subire alterazioni sintattiche legate alla gestione ordinaria del formato XML ;
- l'adozione della sola firma attached consente di rendere omogenee le modalità di gestione della firma digitale su tutti i nuovi servizi CBI;
- l'uso di una singola busta permette di semplificare i controlli da applicare ai flussi firmati e ne facilita l'archiviazione;
- l'uso di una singola busta consente di contenere sensibilmente la dimensione media dei flussi firmati da più firmatari, a beneficio della velocità di veicolazione degli stessi.

La seguente Figura riporta il flusso logico del processo di firma dei messaggi logici da applicare nell'ambito dei nuovi servizi XML.

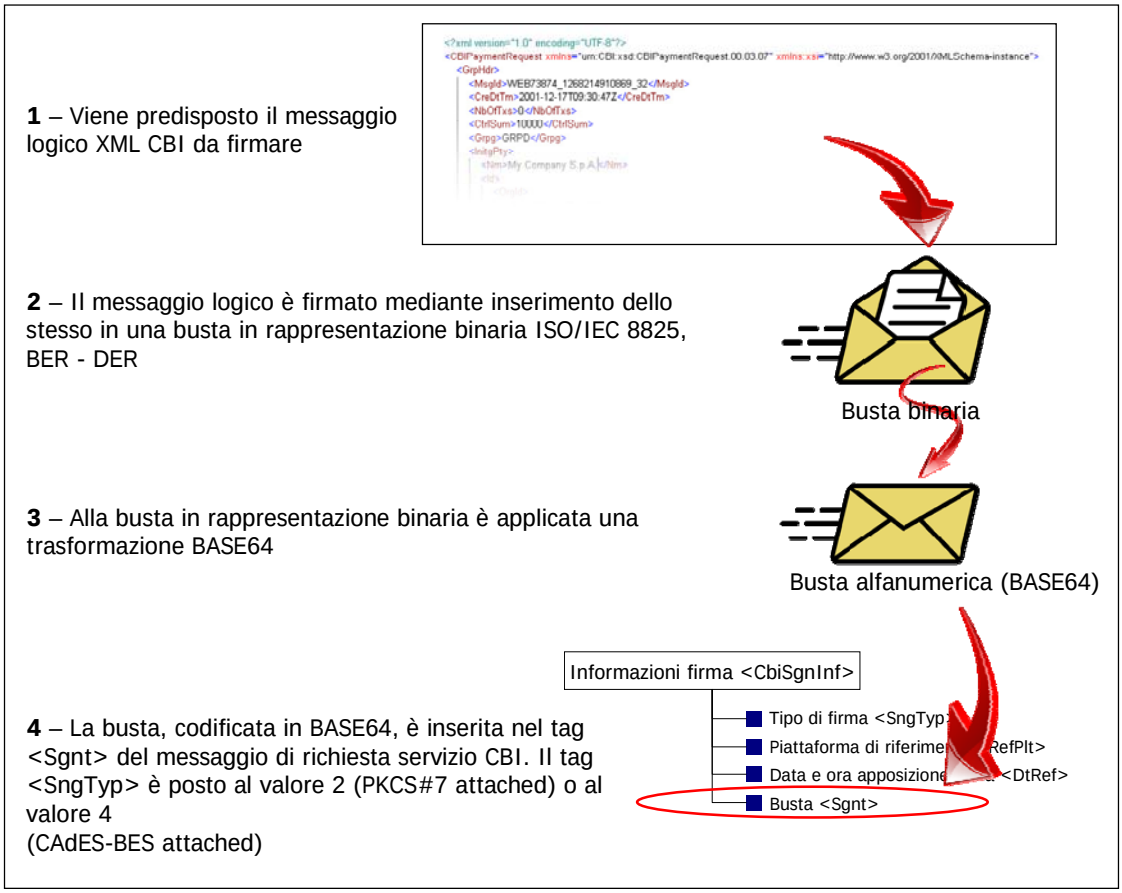


Figura 10

I dati contenuti nella busta PKCS#7 attached sono quindi:

- stream (o un file) di dati in formato XML e validabili tramite lo schema (o gli schema) nel quale è definita la struttura <DATA>;
- Relativo hash crittografato (uno per ogni firmatario);
- Certificato (uno per ogni firmatario).

La busta così ottenuta previa codifica in BASE64 assumerà il nome del flusso logico a cui si riferisce ed assumerà, qualora il contenuto venga posto in un file, l'estensione .p7m.

4.7 TABELLA RIEPILOGATIVA

La tabella riepilogativa riportata nel presente paragrafo riassume le modalità di utilizzo della firma digitale nell'ambito dei servizi CBI (porting e nuovi servizi XML) a partire dal 30 agosto 2010.

Servizio	Tipologia di flusso	Modalità di trasporto	Standard di firma	Dove viene inserita la firma[12]	Cosa viene firmato
Porting	Informativo – Banca/Azienda	File e MSG XML	PKCS#7, CAdES-BES, detached, max 10 buste	Apposito blocco contenuto nel Body del MSG	Supporto logico comprensivo di record di testa e di coda. No CR/LF
Porting	Dispositivo – Azienda/Banca	File e MSG XML	PKCS#7, CAdES-BES, detached, max 10 buste	Apposito blocco contenuto nel Body del MSG	Supporto logico comprensivo di record di testa e di coda. No CR/LF
Nuovi servizi XML	Dispositivo - Azienda Banca	MSG XML/ File e MSG XML	PKCS#7, CAdES-BES attached monobusta	Apposito blocco contenuto nel Body	Blocco del body specifico di servizio allo stesso livello gerarchico del blocco Firma (cfr. regola 3)
Nuovi servizi XML	Informativo - Banca Azienda	MSG XML/ File e MSG XML	PKCS#7, CAdES-BES attached monobusta	Apposito blocco contenuto nel Body	Blocco del body specifico di servizio allo stesso livello gerarchico del blocco Firma (cfr. regola 3)
Nuovi servizi XML	End To End – Azienda Azienda	MSG XML/ File e MSG XML	PKCS#7, CAdES-BES attached monobusta	Apposito blocco contenuto nel Body	Blocco del body specifico di servizio allo stesso livello gerarchico del blocco Firma (cfr. regola 3)

4.8 SOGGETTI ABILITATI ALL'INVIO DI FLUSSI FIRMATI

In occasione dell'avvio dell'uso della firma sui flussi dispositivi di Porting (23 febbraio 2009) è stato introdotto un principio di "controllo" dell'immissione in Rete dei flussi dispositivi di Porting firmati da parte dei Gestori di Punto di Accesso (GPA) attestati sull'infrastruttura CBI.
Come descritto nella circolare 6/2008 (alla quale si rimanda per maggiori dettagli) l'istituzione di tale principio è volta a preservare gli investimenti effettuati dalle Banche e dai Soggetti Tecnici CBI nonché, nel contempo, tutelare la corretta operatività del Sistema CBI.

Il citato principio prevede che l'immissione in Rete CBI dei flussi dispositivi di Porting firmati sia consentita alle sole Banche il/i cui GPA abbiano, di concerto con le Banche stesse alle quali prestano il servizio di veicolazione

[12] *Per i dettagli sulle specifiche tecniche di veicolazione del "Blocco firma", descritto al Par. 4.2, si rimanda ai dettagli sulla documentazione specifica descrittiva della struttura della messaggistica per i nuovi servizi CBI (incluso il "Porting").*

dei flussi CBI, preventivamente effettuato apposite sessioni di test di Sistema (test di interoperabilità) mediante invio di flussi firmati.
Pertanto, affinché un mittente fisico possa ricevere tale autorizzazione, allo stesso viene richiesto di effettuare preliminarmente apposite sessioni di test di sistema inviando flussi firmati e verificando in tal modo il grado di interoperabilità con le controparti attestate sulla Rete (riceventi fisici). In caso di esito positivo delle suddette sessioni di test, i mittenti fisici dei supporti logici firmati sono inseriti in una lista ufficiale, resa nota dal CBI, nella quale compaiono i CUC dei mittenti fisici abilitati all'apposizione della firma digitale sui flussi inviati.

A seguito dell'introduzione della firma in standard CAdES-BES i competenti Gruppi di Lavoro CBI hanno concordato di estendere tale principio a tutti i servizi CBI, pertanto è introdotto un documento (da considerarsi come allegato al presente) contenente le informazioni finalizzate ad indicare, per ogni GPA, l'abilitazione selettiva all'invio delle seguenti tipologie di flussi firmati:

- Porting con firma PKCS#7 detached (<SgnTyp> = 1)
- Porting con firma CAdES-BES detached (<SgnTyp> = 3)
- Nuovi Servizi XML con firma PKCS#7 attached (<SgnTyp> = 2)
- Nuovi Servizi XML con firma CAdES-BES attached (<SgnTyp> = 4)

In fase di ricezione di un flusso firmato deve pertanto essere effettuato il controllo del mittente fisico, producendo apposito scarto se il CUC dello stesso non rientra nella lista dei soggetti abilitati all'invio della tipologia di firma ricevuta.

Si precisa a tal proposito che ogni singolo GPA potrebbe essere abilitato solo all'invio di determinate tipologie di firma (es. solo tipo 3 e 4).

Si ricorda infine che per i servizi di Porting l'apposizione della firma rappresenta criterio di omogeneità per l'aggregazione dei supporti logici nei file; pertanto lo scarto per mittente fisico non abilitato deve essere effettuato a livello di intero file (cfr. doc. PORTING-MO-001). Al contrario, per i nuovi servizi XML, tale scarto deve essere effettuato a livello di singoli messaggi logici.

5 PROCESSI ED ATTIVITÀ

Le attività connesse alla creazione e gestione di "informazioni firmate digitalmente"[13] (di seguito - per brevità – oggetto firmato; cfr. par. 4.4 per i dettagli) possono essere ricondotte ai processi sotto riportati.

Nota bene: le attività indicate sono aggiuntive rispetto a quelle previste nell'ambito della normale attività CBI. Tra parentesi [ ] sono riportate le attività ordinarie che precedono o seguono logicamente quelle del processo di Firma.

5.1 TRATTA CLIENTE => BANCA PASSIVA

Il processo è sintetizzato nella figura seguente.

[13] *Con tale termine si intende:*
Il supporto logico CBI, qualora il termine sia riferito al servizio di "Porting"
Il messaggio logico XML, qualora il termine sia riferito ai nuovi servizi CBI

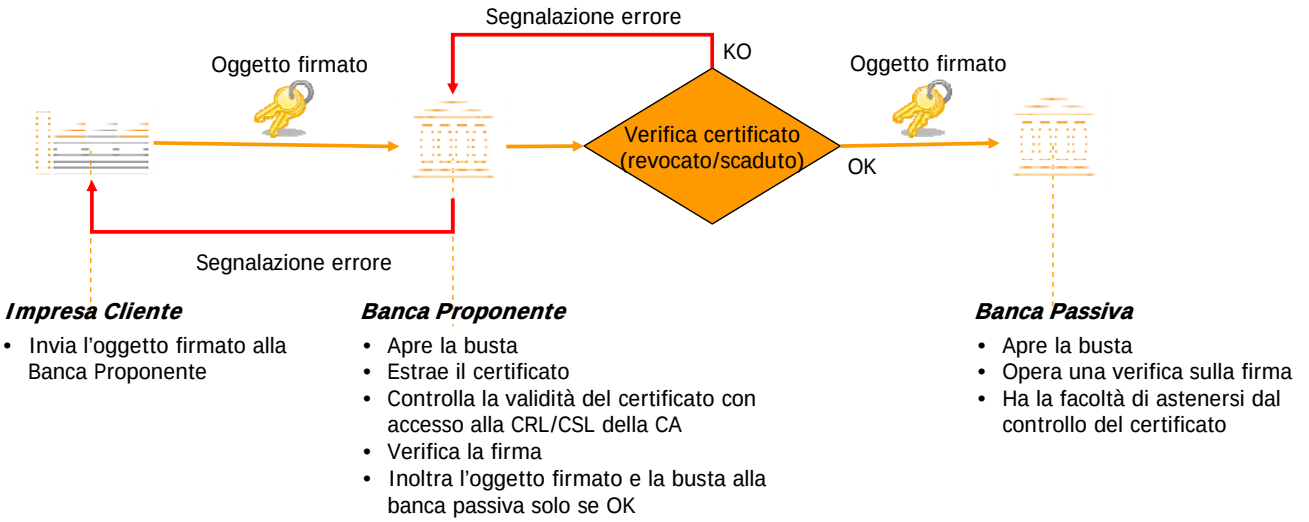


Figura 11: Processo – Tratta Cliente/Banca Passiva

5.1.1.1 Cliente/Titolare

[Generazione dell'oggetto da firmare: il Cliente e/o il Titolare, con l'applicazione e/o le modalità d'utilizzo del Servizio CBI messe a disposizione dalla Banca Proponente, creano l'oggetto sul quale si attiverà il processo di Firma Digitale.]

Generazione della busta crittografica: predisposto l'oggetto da firmare, il Titolare richiama l'opportuno modulo dell'applicazione CBI da cui si ottiene una busta crittografica e codificata nel formato binario.
Qualora le politiche aziendali del Cliente dovessero prevedere l'apposizione di Firme multiple, l'applicativo dovrà essere in grado di reiterare il processo.

Predisposizione del Msg XML (e, se previsto dal servizio, del file associato) ed inserimento della busta, previa codifica della stessa in Base64, come previsto dagli standard di messaggistica del servizio.

[Invio Msg XML (e, se presente, del file) : invio al CBI mediante i sistemi di trasmissione previsti].

5.1.1.2 Banca Proponente

[Ricezione dell'oggetto firmato mediante i sistemi di trasmissione previsti.]

Riconoscimento del servizio CBI richiesto, identificazione della busta ed estrazione delle informazioni per la verifica della firma (ad es. busta, dati firmati inseriti nella busta nel caso di utilizzo della modalità attached, ecc.).

Archiviazione della busta crittografica.

Apertura della busta crittografica.

Verifica Certificato: la Banca Proponente ha la responsabilità di verificare la validità del certificato utilizzato dal Titolare (o di ogni Certificato, in caso di Firme multiple) accertando che:

- il Certificatore sia iscritto all'Elenco CBI;
- il rilascio del Certificato sia avvenuto ai sensi della legge 197/91;
- il Certificato non sia scaduto, revocato o sospeso mediante consultazione delle CRL/CSL. L'orario e l'esito di tale verifica dovrà essere archiviato e reso disponibile in caso di contestazioni.

Verifica della Firma.

[Diagnostica dell'oggetto firmato, in accordo alle specifiche previste dal CBI[14].

Spedizione alla Banca Passiva dell'oggetto firmato].

5.1.1.3 Banca Passiva

[Ricezione degli oggetti firmati mediante i consueti sistemi trasmissivi.]

Riconoscimento del servizio CBI richiesto ed estrazione della busta per la verifica della firma.

Archiviazione della busta crittografica.

Apertura della busta crittografica.

Verifica, opzionale, della validità del o dei Certificati contenuti.

Verifica d'integrità della busta crittografica / verifica della Firma.

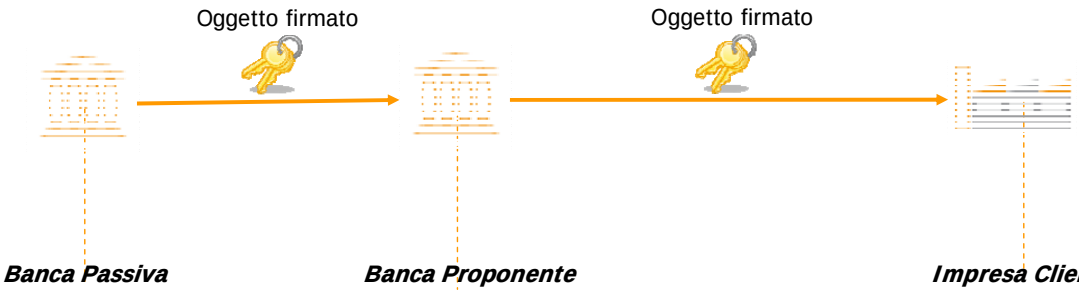
[Diagnostica dell'oggetto firmato e invio conferma di ricezione qualificata/errori rilevati]

Presa in carico delle disposizioni contenute nell'oggetto firmato.

5.2 TRATTA BANCA PASSIVA = > CLIENTE

Il processo è sintetizzato nella figura seguente.

[14] *La diagnostica deve essere conforme ai criteri attualmente in uso.*



Banca Passiva

- Invia l'oggetto firmato al Cliente

Banca Proponente

- Deve mettere a disposizione dei propri clienti il contenuto degli oggetti firmati

Impresa Cliente

- Deve avere a disposizione il contenuto degli oggetti firmati qualora non abbia strumenti adatti a ricevere, aprire la busta e verificare la firma
- Può esercitare la funzione di controllo sul certificato, non necessariamente con strumenti forniti dalla banca per l'accesso diretto alla CRL/CSL

N.B. In questa tratta il processo di verifica di validità del certificato utilizzato non viene effettuato da alcun soggetto, lasciando facoltà al Cliente, eventualmente supportato dalla propria Banca Proponente, di eseguire tale attività

Figura 12: Processo –Tratta Banca Passiva/Cliente

Le attività connesse alla creazione e gestione di oggetti firmati digitalmente possono essere ricondotte a quelle precedentemente illustrate per la tratta Cliente => Banca Passiva.

Occorre sottolineare, tuttavia, che nel caso di Firma apposta da una Banca, il processo di verifica di validità del Certificato utilizzato non viene effettuato da alcun soggetto, lasciando facoltà al Cliente - eventualmente supportato dalla propria Banca Proponente - di eseguire tale attività.

La Banca Proponente, laddove il Cliente non sia in grado di "aprire" gli oggetti firmati, verificarne la Firma (autenticità ed integrità) o procedere ad un'archiviazione delle buste crittografiche, può supportare il Cliente con soluzioni applicative che rientrano nella sfera della propria offerta competitiva.

5.3 TRATTA CLIENTE => CLIENTE

La tratta Cliente-Cliente è prevista unicamente per servizi di Gestione Documentale in cui il mittente ed il destinatario di un flusso sono due aziende utenti del Servizio CBI (es. servizio di Invio end-to-end di fatture elettroniche tra aderenti CBI).

Il processo è sintetizzato nella figura seguente.

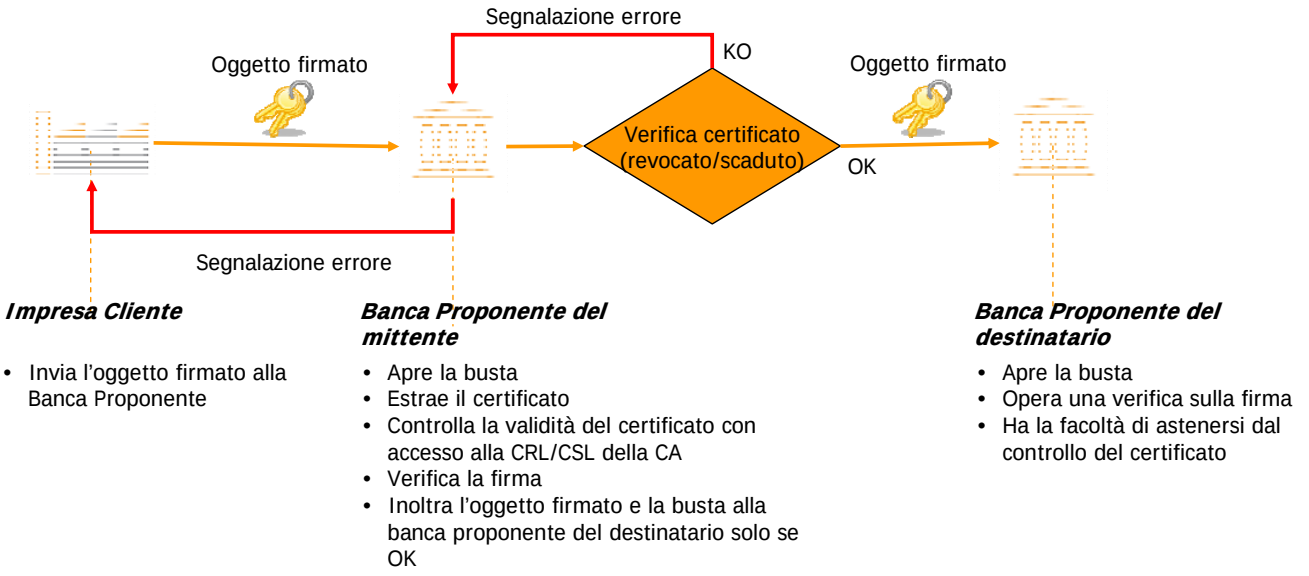


Figura 13: Processo – Tratta Cliente/Cliente

Le attività connesse alla creazione e gestione di oggetti firmati digitalmente possono essere ricondotte a quelle precedentemente illustrate per la tratta Cliente => Banca Passiva, assegnando le attività in carico alla Banca Passiva alla Banca Proponente del Destinatario che dovrà, una volta completate le attività previste, rendere disponibile l'oggetto firmato al Destinatario.

6 APPENDICE

6.1 APPENDICE A: DOCUMENTAZIONE TECNICA DI RIFERIMENTO

[1] RFC 2315 : PKCS #7: Cryptographic Message Syntax Version 1.5

[2] RFC 3852 : Cryptographic Message Syntax (CMS)

[3] ETSI TS 101 733 V1.7.4 : Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES)

Di seguito i riferimenti tecnici per la firma con busta in formato XML. Si precisa tuttavia che l'utilizzo di tale modalità non è al momento previsto nell'ambito del circuito CBI.

[4] ETSI TS 101 903 V1.4.1 : XML Advanced Electronic Signatures (XAdES)

[5] ETSI TS 102 904 V1.1.1 : Profiles of XML Advanced Electronic Signatures based on TS 101 903 (XAdES)

Fine del documento