	Area
Redatto da	eGovernment

Versione	Data	Modifiche
1.0	10.03.2017	Versione iniziale

Firma digitale: Concetti generali e linee guida

Indice

Indice delle figure

PREMESSA

Con la diffusione dell'uso dei documenti informatici, sono sempre più numerose le richieste di chiarimento sul corretto utilizzo della firma digitale, con particolare riferimento al valore giuridico della firma digitale, ai formati di firma, ai casi in cui sia necessario apporre più firme su un medesimo documento, ai diversi strumenti che in Ateneo sono disponibili per l'apposizione della firma su un documento informatico.

Il CSI ha quindi predisposto un Manuale è dunque quello di offrire all'utilizzatore della firma digitale una panoramica sulla tematica, con l'obiettivo di rendere noti alcuni aspetti normativi e tecnologici di carattere generali, la cui conoscenza è fondamentale per operare in modo valido e corretto.

In dettaglio, il Manuale è organizzato in tre parti:

Parte I – Concetti generali e quadro normativo

Parte II – I formati e le modalità di firma

Parte III – Applicazioni per la firma digitale

Parte IV – Riferimenti normativi e glossario

PARTE I – CONCETTI GENERALI E QUADRO NORMATIVO

La presente parte tiene conto dell'attuale normativa nazionale e del Regolamento (UE) n. 910/2014 del Parlamento Europeo e del Consiglio del 23 luglio 2014 "in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE", (c.d. Regolamento eIDAS). Tale regolamento sancisce i principi per il mutuo riconoscimento delle firme elettroniche qualificate in tutti gli stati membri dell'UE.

Di seguito, si ritiene utile inquadrare il contesto più ampio delle firme elettroniche, con particolare riguardo alla firma digitale.

1. LE TIPOLOGIE DI FIRMA ELETTRONICA

Con l'avvento delle firme elettroniche si deve modificare il modo di intendere il concetto di sottoscrizione.
Le firme elettroniche non riproducono infatti il nome e il cognome del firmatario, non sono costituite da parole, né da simboli grafici, ma sono piuttosto una serie di informazioni digitali apposte o collegate ad un documento (in senso lato) che, in forma di bit, conferiscono determinati effetti a un dato documento informatico.
In generale, la sottoscrizione elettronica, analogamente a quanto accade per la firma autografa sui documenti cartacei, è l'elemento (informatico) che permette di attribuire all'autore la paternità giuridica del documento. Il Codice dell'Amministrazione Digitale (CAD), il d.lgs 82/2005, individua caratteristiche e condizioni di operatività delle diverse tipologie di firma, in accordo con la citata normativa europea.

Nello scenario normativo attuale sono previste quattro tipologie di firma, che assicurano differenti livelli sicurezza, alle quali sono riconosciuti differenti effetti giuridici: conseguentemente ad ogni tipologia di firma viene ricondotto un diverso valore probatorio.
In generale, ai sensi dell'art. 21 commi 1 e 2 del CAD, il documento informatico, cui è apposta una firma elettronica, soddisfa il requisito della forma scritta e sul piano probatorio è liberamente valutabile in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità e immodificabilità. Inoltre, il documento informatico sottoscritto con firma elettronica avanzata, qualificata o digitale, formato nel rispetto delle regole tecniche per la formazione, per la trasmissione, la conservazione, la copia, la duplicazione, la riproduzione e la validazione dei documenti informatici, nonché quelle in materia di generazione, apposizione e verifica di qualsiasi tipo di firma elettronica, ha altresì l'efficacia prevista dall'articolo 2702 del codice civile.

1.1. FIRMA ELETTRONICA (FE)

Con l'espressione firma elettronica s'intende un insieme di dati in forma elettronica, riconducibili all'autore (anche di tipo: log identificativo, indirizzo mail, ecc.), allegati oppure connessi ad atti o fatti giuridicamente rilevanti contenuti in un documento informatico, utilizzati come metodo di identificazione informatica. La firma elettronica quindi, più che a una vera e propria firma, dà vita ad un processo di autenticazione cui sono riferibili minori requisiti di sicurezza rispetto alle altre tipologie di firma.

La normativa riconosce alla firma elettronica un valore probatorio: la firma è liberamente valutabile dal giudice in fase di giudizio, in base a caratteristiche oggettive di qualità e sicurezza. E' ripudiabile dal sottoscrittore e, ai sensi dell'art. 21 comma 2-bis del CAD, non può essere utilizzata per la sottoscrizione di atti da parte di un pubblico ufficiale.

1.2. FIRMA ELETTRONICA AVANZATA (FEA)

È un particolare tipo di firma elettronica che, allegando oppure connettendo un insieme di dati in forma elettronica a un documento informatico, garantisce integrità (consentendo di rilevare se i dati sono stati successivamente modificati), autenticità del documento sottoscritto. La sua creazione presuppone l'utilizzo di mezzi sui quali il firmatario mantiene il controllo esclusivo. Quest'ultimo elemento assicura la connessione univoca con il firmatario e quindi la paternità giuridica del documento.
La firma elettronica avanzata presenta dei caratteri peculiari che la differenziano marcatamente rispetto alle altre tipologie di firma. In primo luogo, la normativa non vincola la firma elettronica avanzata a particolari standard tecnici o determinati *software*. Conseguentemente non esiste uno standard di firma elettronica avanzata, ma sono ipoteticamente possibili soluzioni di firma anche molto diverse tra loro, purché rispettino i requisiti richiesti dalla legge:

1. connessione unicamente al firmatario;
2. idoneità a identificare il firmatario;
3. creazione mediante dati per la creazione di una firma elettronica che il firmatario può, con un elevato livello di sicurezza, utilizzare sotto il proprio esclusivo controllo;
4. collegamento ai dati sottoscritti in modo da consentire l'identificazione di ogni successiva modifica di tali dati.

Gli strumenti più diffusi sono quelli che utilizzano nei processi di sottoscrizione le parole d'ordine temporanee (*one time password* - OTP) e i dati biometrici, tra cui assumono un posto di rilievo le soluzioni di firma grafometrica, oppure, la Posta Elettronica Certificata che ottemperi alle regole tecniche in materia di identificazione del titolare della casella.

Il documento informatico sottoscritto con firma elettronica avanzata, formato nel rispetto delle regole tecniche, è riconosciuto valido fino a querela di falso. Pertanto, questa tipologia di firma comporta l'inversione dell'onere della prova: chi intende disconoscere la sottoscrizione di un documento dovrà provare che l'apposizione della firma è riconducibile ad altri e che tale apposizione non è imputabile a sua colpa.

Appare importante sottolineare come il legislatore abbia deciso di limitare l'ambito di validità della firma elettronica avanzata ai soli rapporti intercorrenti tra il sottoscrittore e il soggetto l'erogatore della

soluzione di firma (art. Art. 60 (Limiti d'uso della firma elettronica avanzata), comma 1 del DPCM "Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali" del 22.02.2013.
La firma elettronica avanzata, ai sensi dell'art. 21 comma 2-bis del CAD, non è valida per la sottoscrizione di atti da parte di pubblico ufficiale.

1.3. FIRMA ELETTRONICA QUALIFICATA (FEQ)

È un particolare tipo di firma elettronica avanzata basato su un certificato "qualificato" (che garantisce l'identificazione univoca del titolare, rilasciato da certificatori accreditati) e realizzato mediante un dispositivo sicuro per la generazione della firma che soddisfa particolari requisiti di sicurezza.
In dettaglio, la firma qualificata si basa sui seguenti elementi:

- ✓ Certificato qualificato emesso da Enti Certificatori accreditati
- ✓ Standard tecnologico ben definito
- ✓ Richiesto l'utilizzo di un dispositivo sicuro di firma (smart card, token usb, HSM)
- ✓ Interoperabilità

I documenti informatici sui quali è apposta una firma qualificata, hanno l'efficacia prevista dall'art. 2702 del codice civile ai sensi del quale la scrittura privata fa piena prova fino a querela di falso della provenienza delle dichiarazioni di chi l'ha sottoscritta. L'utilizzo del dispositivo di firma si presume riconducibile al titolare, salvo che questi dia prova contraria si configura quindi l'inversione dell'onere della prova.

1.4. FIRMA DIGITALE (FD)

La firma digitale, ai sensi dell'art. 1, comma 1, lettera s) del Codice dell'Amministrazione Digitale, è un particolare tipo di firma qualificata basata su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare tramite la chiave privata (custodita dal titolare) e al destinatario tramite la chiave pubblica (contenuta nel certificato), rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici.

La coppia di chiavi asimmetriche è lo strumento rilasciato da un Certificatore autorizzato, che svolge un ruolo di garanzia di autenticità dell'origine del documento firmato. Le chiavi sono, appunto, due: una privata, a conoscenza del solo titolare, e una pubblica, conoscibile da tutti. Quest'ultimo elemento fa, della firma digitale, un'Infrastruttura a Chiave Pubblica (Public Kei Infrastructure – PKI). Le due chiavi si dicono

"asimmetriche" in quanto il documento potrà essere cifrato sia con chiave pubblica che con quella privata, sortendo due effetti differenti:

La procedura di firma digitale di un documento elettronico prevede la siglatura del documento (firma) da parte dell'emittente tramite chiave privata e l'apertura (verifica della firma) da parte del destinatario tramite la corrispondente chiave pubblica.

Ovviamente, la coppia di chiavi asimmetriche sono attribuite a un solo titolare.

La firma digitale ha la stessa efficacia probatoria della firma qualificata, ma, a differenza di quest'ultima, si avvantaggia della sicurezza e della facilitata comunicazione tra gli utilizzatori dei documenti firmati offerte dall'infrastruttura a chiave pubblica PKI. Assieme alla firma qualificata è lo strumento a norma per la sottoscrizione di atti da parte di pubblico ufficiale.

Per tale motivo, nel prosieguo del Manuale, si farà riferimento alla firma digitale quale strumento per la sottoscrizione dei documenti informatici rilevanti ai fini dei procedimenti amministrativi dell'Ateneo.

2 IL CERTIFICATO QUALIFICATO PER LA FEQ O PER LA FD

I certificati qualificati per la firma qualificata (FEQ) o digitale (FD) sono emessi da enti accreditati, le Certifcation Authority e contengono le informazioni anagrafiche del titolare, i dati sull'eventuale terzo interessato (ad esempio, l'Università) per conto del quale il certificato viene emesso, nonché la chiave pubblica.

La chiave pubblica è associata in modo univoco alla chiave privata del titolare del certificato qualificato e custodita nel dispositivo sicuro di firma.

Di seguito una rappresentazione grafica del contenuto del certificato.

Figura 1 – La struttura di un certificato di firma

Il certificato del titolare ha un periodo di validità limitato, nel nostro Ateneo **pari a 6 anni**, ma può anche essere revocato o sospeso prima della naturale scadenza. La revoca sopravviene in diversi casi, quali il guasto, la sottrazione o lo smarrimento del dispositivo di firma, quando il titolare ha perso il controllo esclusivo del dispositivo o quando il titolare abbia il ragionevole dubbio che i certificati qualificati possano essere utilizzati da altri.

3 L'APPOSIZIONE E LA VERIFICA DELLA FIRMA DIGITALE

3.1. L'APPOSIZIONE DELLA FIRMA DIGITALE

La sottoscrizione elettronica non è semplicemente un atto ma si tratta di un processo informatico basato su algoritmi crittografici che permettono di rappresentare un insieme di dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici (documento informatico), utilizzati come metodo di identificazione informatica.

In dettaglio, il processo prevede:

1. Il calcolo del valore dell'impronta del messaggio (detto hash) applicando un algoritmo di cifratura sull'intero contenuto;

2. La cifratura del valore di hash con la chiave privata del mittente (cioè apporre la firma digitale);

3. L'aggiunta al messaggio originale la firma digitale e la creazione della busta crittografica p7m con l'aggiunta del certificato qualificato del sottoscrittore.

Figura 2 – Il processo di firma

Dal punto di vista tecnico-operativo, le operazioni da compiere per apporre la firma a un documento informatico possono variare in base al *software* di firma utilizzato. I tratti fondamentali, però, sono comuni a tutti gli applicativi utilizzati:

- il software di firma richiede di selezionare il documento da sottoscrivere e di inserire la smart card nel lettore o il dispositivo di firma nella porta USB;
- successivamente il software chiede l'inserimento del codice PIN e salva il documento sottoscritto e pronto per essere utilizzato.

Il documento da firmare è imbustato nel formato originale, senza aggiunte in testa o in coda al formato stesso. Il file firmato, cioè la busta, contiene al suo interno:

- il documento informatico nel formato originale,
- la firma digitale calcolata sull'impronta del documento,
- il certificato qualificato del sottoscrittore.

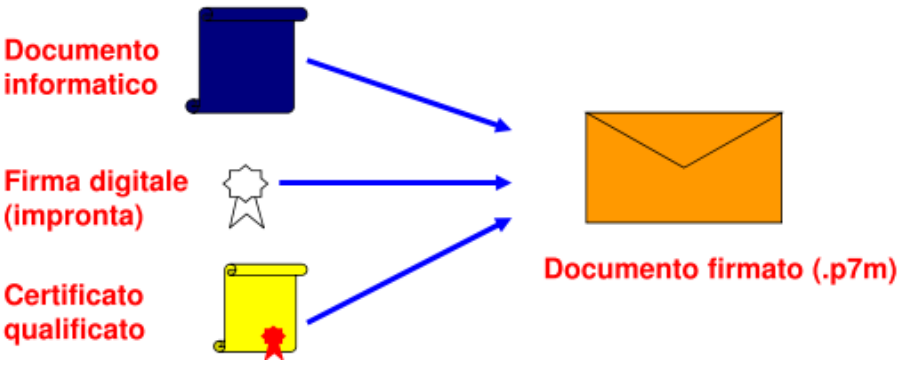

Figura 3 – La busta crittografica in formato Cades

Nel caso in cui il processo di firma interessi un numero elevato di documenti è possibile automatizzare le procedure di sottoscrizione purché l'operazione di firma automatizzata si svolga nel rispetto della

normativa tecnica vigente. La firma digitale deve riferirsi in maniera univoca a un solo soggetto e al documento o all'insieme di documenti cui è apposta o associata.

3.2. LA VERIFICA DELLA FIRMA

Il processo di verifica di un documento firmato digitalmente è complesso e molto importante, in quanto ha l'obiettivo di verificare la validità, l'autenticità e l'integrità del documento.

Il primo passo consiste nel controllo di validità del certificato qualificato del sottoscrittore, mediante un software di verifica tale da accedere (altrimenti l'esito sarà di firma sconosciuta) all'Elenco Pubblico dei Certificatori pubblicato dall'Agenzia per l'Italia Digitale in formato europeo. Un certificato qualificato si può ritenere valido se sono eseguiti e superati i seguenti controlli:

- La validità della firma digitale del certificatore che ha emesso il certificato;
- La data di scadenza , presente all'interno del certificato, della validità del certificato stesso;
- La non presenza del certificato nella lista dei certificati revocati/scaduti (CRL/CSL), emessa e aggiornata dal certificatore.

Il superamento di tali controlli è prerequisito perché siano eseguiti i successivi controlli di autenticità e di integrità del documento che consistono nel:

1. Separare dal messaggio ricevuto la firma digitale;
2. Decifrare la firma digitale con la chiave pubblica del mittente ottenendo così il valore di hash ricevuto;
3. Applicare lo stesso algoritmo di cifratura utilizzato per il calcolo dell'impronta sull'intero contenuto del messaggio ricevuto ottenendo così il valore di hash calcolato;
4. Confrontare il valore di hash ricevuto con quello calcolato;
5. Se sono identici, la verifica ha avuto esito positivo, altrimenti l'esito è da considerare negativo ed il messaggio deve essere rifiutato.

Ai fini del conferimento a un documento firmato digitalmente di valore e validità giuridica, va considerato che:

L'apposizione a un documento informatico di una firma digitale o di un altro tipo di firma elettronica qualificata basata su un certificato elettronico revocato, scaduto o sospeso equivale a mancata sottoscrizione.

La revoca o la sospensione, comunque motivate, hanno effetto dal momento della pubblicazione nella lista pubblica dei certificati revocati o sospesi (CRL/CSL).

Il sottoscrittore deve inoltre accertarsi che il documento su cui appone la firma sia statico, cioè non ne risulti alterato il contenuto alla sua successiva apertura, per la presenza di macro-istruzioni (quali, ad esempio, il campo data).

Rispetto ai documenti informatici su cui è stata apposta firma digitale si pone, quindi, da parte del l'utilizzatore (qualora il documento rechi firme multiple, come specificato più avanti) il problema della verifica della firma digitale. In particolare, occorre accertare che:

- **il documento non sia stato modificato dopo la firma;**
- **il certificato del sottoscrittore sia garantito da una Autorità di Certificazione (CA) inclusa nell'Elenco Pubblico dei Certificatori;**
- **il certificato del sottoscrittore non sia scaduto;**
- **il certificato del sottoscrittore non sia stato sospeso o revocato.**

PARTE II – I FORMATI E LE MODALITA' DI FIRMA

4. I FORMATI DI FIRMA

I formati di firma digitale previsti dalla normativa europea e italiana sono:

4.1 FORMATO CADES

La cui estensione è P7M (PKCS #7 MIME Message). Detto anche "Busta Crittografata". Per leggere il file è necessario un software in grado di interpretare la firma (mediante standard PKCS#7) e poterne estrarre il contenuto.

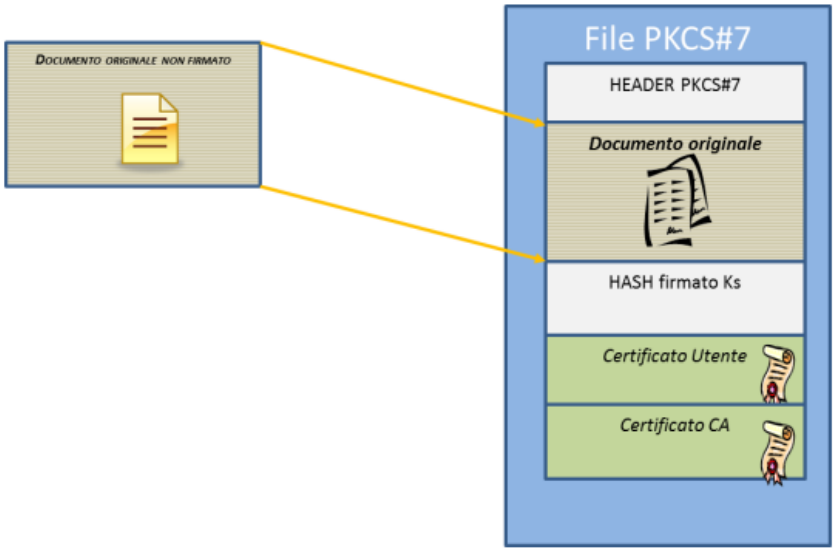

Figura 4 – Struttura di un file Cades

Tutti i formati di file possono essere firmati con questo formato.

Da Regolamento di Ateneo, gli atti amministrativi dell'Università - salvo casi particolari - sono firmati nel formato Cades.

4.2 FORMATO PADES (BASIC E BES)

La cui estensione è PDF. E' uno speciale documento PDF che non può contenere all'interno firme digitali o marche temporali.

Possono essere firmati con questo formato solo file PDF. Alcuni PDF contenenti caratteristiche complesse potrebbero non essere firmabili con questo formato e sarà necessario utilizzare il CAdES.

Esistono due formati diversi di firma Pades descritti di seguito.

4.2.1 *PADES BASIC*

Si tratta della tradizionale firma PDF opportunamente profilata per essere conforme alla normativa Europea. Questo tipo di firma è compatibile con tutte le versioni di Adobe. La firma è valida sul territorio nazionale italiano, ma non può essere utilizzata per il trattamento di documenti a livello europeo

PADES BES

Si tratta di un particolare tipo di firma PDF “avanzata”' opportunamente profilata per essere in linea con alcune particolari restrizioni della normativa europea.
ATTENZIONE: Questo tipo di firma viene riconosciuta correttamente solo dalla versione 10 del software Adobe è però il profilo previsto dalla Decisione della Commissione Europea 2011/130/EU e, quindi, da preferirsi al Basic al fine di garantirne la validità in tutti i paesi dell’UE.

4.3 FORMATO XADES,

L’estensione di tale formato è XML. La sua caratteristica principale è la possibilità di firmare singole parti del documento, cosa di particolare importanza nei caso di documenti scritti da più persone. Tuttavia è uno standard ancora poco usato e richiesto per via di una serie di limitazioni tecniche che non consente la firma di qualsiasi documento.

4.4 MARCA TEMPORALE

Tale formato (MIME-PKCS#7) ha estensione m7m e rappresenta un file firmato digitalmente su cui in seguito è stata apposta la marca temporale.

Questo tipo di file contiene quindi: ["Dati Documento" > "Firma/e" > "Marca temporale"].

Di seguito, si riporta uno schema di confronto tra il formato Cades e quello Pades:

CADES		PADES	
PRO	**CONTRO**	**PRO**	**CONTRO**
Possibilità di firmare tutti i formati.	E' necessario disporre di un visualizzatore per file p7m. Tale problema potrebbe essere ovviato mettendo a disposizione degli utenti una app on line (esempio, quella messa a disposizione da Agid): http://dss.agid.gov.it/validation).	Semplice l'apertura del file.	Si possono firmare solo file in formato PDF.
Indipendenza dal visualizzatore (vanno bene tutti i visualizzatori offerti gratuitamente dalle Certification Authority).	Nell'applicare firme multiple è facile sbagliare apponendo le firme in modalità "enveloped" (c.d. matrioska), invece che in modalità parallela.		Non si capisce se un file pdf è firmato o meno: va aperto (a patto di disporre di un reader Adobe o tale da mostrare le firme.
Estensione che rende identificabili esternamente i file firmati digitalmente da parte degli utilizzatori.			Le firme appaiono solo se si usa Adobe reader: con motli altri sw freeware, non appaiono le informazioni sulle firme (esempio: PDF Creator), ma solo il riquadro di firma: l'utente è quindi portato a ritenere erroneamente che il riquadro di firma "sia" la firma digitale.
			In alcuni casi, se si firma in formato Pades-BES, se la versione Adobe reader non è abbastanza aggiornata, non si riesce ad aprire il file firmato.
			Adobe reader non è più supportato per Linux
			Un file firmato Pades può essere firmato in Cades (il vice-versa non è possibile): si forma così un file

CADES		PADES	
			“eveloped”.

Figura 5 – I formati Cades e Pades a confronto

5. L’APPOSIZIONE DI FIRME MULTIPLE

Più sottoscrittori possono apporre la propria firma digitale allo stesso documento. In tal caso, si parla di processo di firma multipla. Si possono riconoscere le seguenti tipologie di firma multipla:

– firme “**parallele**”: quando il sottoscrittore successivo al primo firma solo i dati contenuti nella busta crittografica. Un documento con firme parallele produce un file di tipo “nomefile.p7m” nel caso di firma Cades, oppure “nomefile.pdf” nel caso di firma Pades;

– firme “**nidificate**” o “**annidate**” o “**a matrioska**”: in questo caso ogni sottoscrittore successivo firma l’intera busta crittografica generata da un altro sottoscrittore. Un documento con firme annidate produce un file “nomefile.p7m.p7m.p7m….” oppure, “nomefile.pdf.p7m” se il file firmato in Cades era stato precedentemente firmato in Pades;

– “**controfirme**”: in questo caso il sottoscrittore firma una precedente firma apposta da un altro sottoscrittore. Un documento con controfirme produce un file di tipo”nomefile.p7m” “nomefile.pdf”.

In generale, la firma multipla va apposta in modalità parallela, ciò a significare che i sottoscrittori sono a un livello paritetico e che le firme sono congiunte. L’utilizzo della firma nidificata può invece risultare utile per firmare documenti il cui certificato di firma è scaduto, qualora se ne debba - ad esempio – produrre una copia.

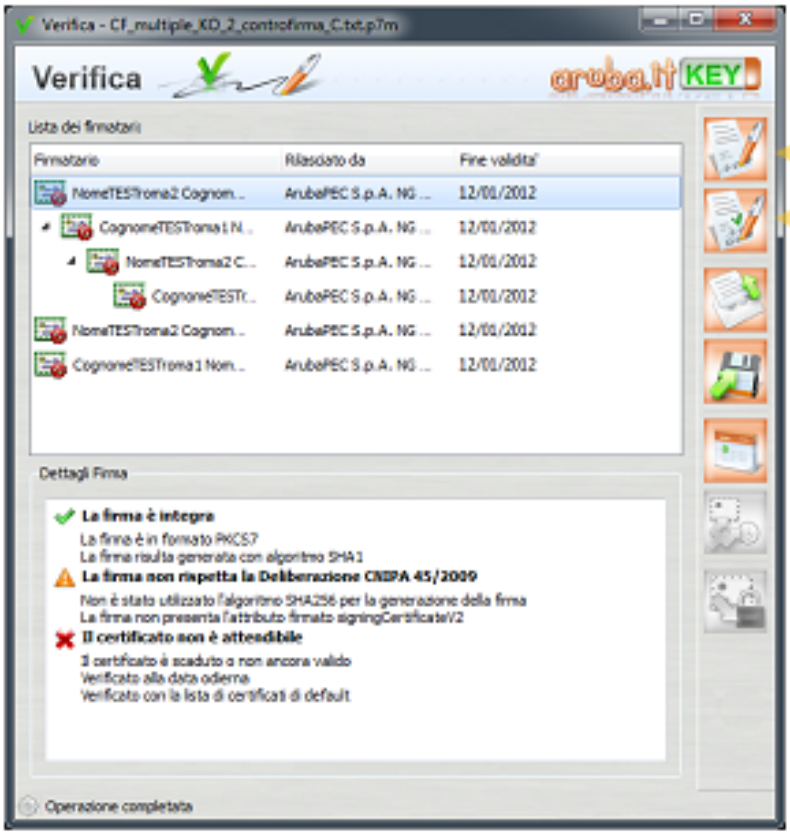

Figura 6 – Un esempio di documento contenente firme parallele e firme nidificate

PARTE III - APPLICAZIONI PER LA FIRMA DIGITALE

In questa sezione vengono forniti i riferimenti alle principali applicazioni per l'apposizione per la verifica dei documenti sottoscritti con firma digitale, fermo restando il rinvio alla documentazione tecnica e ai manuali utente specifici per ciascuna applicazione disponibili, per quanto attiene alle soluzioni istituzionali Federico II, nella sezione Firma digitale all'indirizzo del sito per l'eGovernment: http://www.praxis.unina.it.

6. LE APPLICAZIONI PER LA SOTTOSCRIZIONE

Per i titolari di firma digitale dell'Università, è possibile firmare digitalmente un documento mediante i seguenti prodotti:

- **ArubaKey**: il tool "a bordo" dei token di firma digitale UninaKey
- **ArubaSign**: applicazione disponibile per desktop fornita dalla CA dell'Università
- **Confirma Server**: per la firma dei documenti istituzionali. E' l'applicazione invocata secondo una logica a servizi dalle applicazioni dell'Università: Verbali digitali di esame, Documentale, Protocollo, Convocazione Organi Collegiali.
- **Confirma Client**: è l'applicazione locale della suite Confirma per la apposizione di firme digitali, anche con dispositivi non UninaKey.

I suddetti prodotti consentono di applicare, in base al formato di firma prescelto, firme parallele, annidate o controfirme.

Dettagli operativi, manuali e guide, nonché i link per eventualmente effettuare il download dei predetti sotfware sono disponibili all'indirizzo: http://www.praxis.unina.it/firma-digitale.

7. LE APPLICAZIONI PER LA VERIFICA

I prodotti utilizzabili per l'apposizione della firma ne consentono anche la verifica dei formati **CAdES, PAdES o XAdES**. Una accorttezza va riservata alla configurazione di tali software che devono, ad esempio, essere configurati per indirizzare sempre in modo corretto la lista dei certificati delle CA pubblicata dall'Agenzia per l'Italia Digitale. Altro requisito è che il client dal quale si esegue la verifica sia collegato in rete.

In alcuni casi (ad esempio, Confirma Client), la verifica viene effettuata alla data specificata in input oppure alla data della marca temporale nel caso sia presente.

E' possibile verificare la presenza sul documento di firme parallele o di controfirme.Viene mostrato l'albero delle firme ed indicata la validità della singola firma.

Sono altresì utilizzabili i software di verifica messi gratuitamente a disposizione da tutte le Certification Authority (disponibili all'indirizzo: http://www.agid.gov.it/agenda-digitale/infrastrutture-architetture/firme-elettroniche/software-verifica). In particolare, si segnala che, la Commissione europea ha reso disponibile il

Digital Signature Service (DSS) (url: https://dss.agid.gov.it/home), un software di firma e verifica che può essere gratuitamente scaricato e utilizzato. Il software è reso disponibile dall'Agenzia per l'Italia Digitale per l'uso diretto degli interessati.

PARTE IV - RIFERIMENTI NORMATIVI E GLOSSARIO

Di seguito si riporta l'elenco dei riferimenti normativi rilevanti in materia di firme elettroniche e, a seguire, un glossario dei termini e degli acronimi di uso più frequente.

7. RIFERIMENTI NORMATIVI

- Regolamento (UE) n. 910/2014 del Parlamento Europeo e del Consiglio del 23 luglio 2014 "in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE"
- DECISIONE DI ESECUZIONE (UE) 2015/1506 DELLA COMMISSIONE dell'8 settembre 2015 che stabilisce le specifiche relative ai formati delle firme elettroniche avanzate e dei sigilli avanzati che gli organismi del settore pubblico devono riconoscere, di cui all'articolo 27, paragrafo 5, e all'articolo 37, paragrafo 5, del regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno
- Decreto legislativo n. 82 del 7 marzo 2005, "Codice dell'Amministrazione Digitale"
- DPCM del 22 febbraio 2013, "Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali, ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lettera b), 35, comma 2, 36, comma 2, e 71"

8. GLOSSARIO

A

Algoritmo di hashing

Una firma digitale viene creata facendo passare un documento attraverso un particolare algoritmo, detto di hashing (spezzettamento): il codice prodotto dall'algoritmo, una sorta di "impronta" (hash) del documento, viene poi criptato usando la chiave privata di chi spedisce il messaggio. Si tratta di un algoritmo che partendo da un documento di qualsiasi dimensione lo elabora e produce un codice di dimensione fissa. Il metodo di elaborazione è tale che, se il documento venisse cambiato in qualunque sua parte, questo codice

cambierebbe. Per esemplificare immaginiamo un algoritmo che calcola il numero di lettere, il numero di parole, la frequenza di ogni lettera ecc., se cambia una qualsiasi lettera o parola anche il risultato cambia. Dall'impronta non è possibile risalire al documento, però se il documento cambia, anche solo in minima parte, allora cambia anche l'impronta.

Autenticazione

Nel campo della sicurezza informatica, si definisce autenticazione il processo tramite il quale un computer, un software o un utente destinatario, verifica che il computer, il software o l'utente dal quale esso ha ricevuto una certa comunicazione sia realmente il mittente che sostiene di essere. Uno dei metodi di autenticazione più comunemente adottati prevede l'immissione di un nome e di una password da parte dell'utente. Le forme più evolute sono basate su diversi sistemi di crittografia.

C

Carta a microprocessore - Smart card

Una smart card ("carta intelligente") è essenzialmente un computer delle dimensioni di una carta di credito: incastonato nella plastica della tessera si trova un microprocessore dotato di memoria che può essere letta e, più importante, può essere scritta, nella quale è possibile memorizzare una quantità significativa di informazioni. Contraffare una smart card è estremamente difficile perché il circuito integrato è sepolto nella plastica. In più, il circuito integrato può essere programmato per generare le proprie password e codici, con sofisticate funzioni di crittografia.

Carta Nazionale dei Servizi – CNS: Il documento rilasciato su supporto informatico per consentire l'accesso per via telematica ai servizi erogati dalle pubbliche amministrazioni.

Certificate Policy o Policy: Definizione delle regole generali che indicano in che contesto, a che dominio e con quali modalità di servizio un certificato viene utilizzato. Tutte le regole di servizio vengono poi definite, nel dettaglio, dal documento di Certification Practice Statement (o CPS).

Certificato: Insieme di informazioni utilizzato per distribuire in modo sicuro le chiavi pubbliche degli utenti. Un certificato definisce con certezza la CA che lo ha emesso nonché il periodo di tempo in cui deve essere utilizzato.

Certificazione: Il risultato della procedura informatica, applicata alla chiave pubblica e rilevabile dai sistemi di validazione, mediante la quale si garantisce la corrispondenza biunivoca tra chiave pubblica e soggetto

titolare, si identifica quest'ultimo, si attesta il periodo di validità della predetta chiave e il termine di scadenza del relativo certificato.

Chiavi asimmetriche: Coppia di chiavi crittografiche, una pubblica e una privata, correlate tra loro, utilizzate nell'ambito dei sistemi di validazione.

Chiave privata: Elemento della coppia di chiavi asimmetriche, destinato a essere conosciuto dal soggetto titolare, mediante il quale si appone la firma digitale sul documento informatico o si decifra il documento informatico in precedenza cifrato mediante la corrispondente chiave pubblica.

Chiave pubblica: Elemento della coppia di chiavi asimmetriche destinato a essere reso pubblico, con il quale si verifica la firma digitale apposta sul documento informatico dal titolare delle chiavi asimmetriche o si cifrano i documenti informatici da trasmettere al titolare delle predette chiavi.

Codice di Emergenza (ERC - Emergency Request Code): Codice preimbustato consegnato dall'Ufficio di Registrazione al Titolare per l'autenticazione della richiesta di sospensione di un certificato.

Crittografia: La crittografia, o cifratura, è la tecnica fondamentale per la generazione della firma digitale, e viene utilizzata per assicurare la riservatezza, l'autenticazione e il non ripudio delle informazioni archiviate o inviate attraverso reti di computer. Con la crittografia, un messaggio o, più in generale, un qualunque file di dati (testo, immagini, musica, ecc.) è trasformato in un insieme di segni e simboli assolutamente privi di significato per chi non conosca la "chiave" giusta per decifrarli. Il problema cruciale della crittografia è sempre stato la gestione della chiave. Anche il sistema di cifratura più sofisticato non serve a nulla se non si riesce a garantire la segretezza della chiave. Da questo punto di vista, si parla di due approcci principali alla crittografia: a chiave unica, detto anche a chiave privata o simmetrica; a doppia chiave, detto anche a chiave pubblica o asimmetrica.

CRL (Certification Revoke List): Vedere Lista dei certificati revocati o sospesi.

Cross-certification - Accordi di certificazione: La cross-certification si esercita tra Certification Authority che appartengono a domini diversi. In questo processo i Certificatori si certificano l'un l'altro. Condizione necessaria affinché possa avvenire la cross-certification è che essi accettino e condividano regole equivalenti nel Manuale Operativo.

CSP (Cryptographic Service Provider): Software per l'importazione del certificato di autenticazione nello store Microsoft, necessario per la firma della posta elettronica e l'autenticazione su siti Web.

CSR (Certificate Signing Request): E' il file contenente la richiesta di certificazione della chiave pubblica del Web server in formato PKCS#10.

D

Dispositivo di Firma: E' uno dei possibili supporti di memorizzazione della chiave privata del titolare del certificato (protezione software/hardware con password stabilita dall'utente). Possibili supporti sono, ad esempio, una smart card, un dischetto (protezione software con password stabilita dall'utente), o un dispositivo hardware (protezione hardware con password digitata solo sulla tastiera del dispositivo).

Documento informatico: Nella legislazione sulla firma digitale è la "rappresentazione informatica di atti, fatti e dati giuridicamente rilevanti".

E

Ente Emettitore (EE): Ente responsabile della formazione e del rilascio della CNS. E' la Pubblica Amministrazione che rilascia la CNS ed è responsabile della sicurezza del circuito di emissione e del rilascio della carta, garantendo la corretta gestione del ciclo di vita della CNS.

ERC (Emergency Request Code) Vedere Codice di Emergenza.

F

Firma digitale: Un particolare tipo di firma elettronica qualificata basata su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici.

Firma elettronica: L'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di autenticazione informatica.

Firma elettronica qualificata: La firma elettronica ottenuta attraverso una procedura informatica che garantisce la connessione univoca al firmatario e la sua univoca autenticazione informatica, creata con mezzi sui quali il firmatario può conservare un controllo esclusivo e collegata ai dati ai quali si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati, che sia basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma, quale l'apparato strumentale usato per la creazione della firma elettronica.

Firme multiple: Firme digitali apposte da sottoscrittori diversi allo stesso documento. Si suddividono in:

- **firme "parallele"**: quando il sottoscrittore successivo al primo firma solo i dati contenuti nella busta crittografica. Un documento con firme parallele produce un file di tipo "nomefile.p7m";
- **firme "nidificate" o "annidate" o "a matrioska"**: in questo caso ogni sottoscrittore successivo firma l'intera busta crittografica generata da un altro sottoscrittore. Un documento con firme annidate produce un file "nomefile.p7m.p7m.p7m....";

- **"controfirme"**: in questo caso il sottoscrittore firma una precedente firma apposta da un altro sottoscrittore. Un documento con controfirme produce un file di tipo"nomefile.p7m".

G

Giornale di controllo: Il giornale di controllo consiste nell'insieme delle registrazioni, effettuate automaticamente o manualmente, degli eventi previsti dal Regolamento tecnico.

H

Hash: Vedere Algoritmo di Hashing.

I

Incaricati: In materia di protezione dei dati personali, sono le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile.

Infrastruttura a chiave pubblica: Vedere PKI.

IUT - (Identificativo Univoco del Titolare): E' un codice associato al titolare che lo identifica univocamente presso il Certificatore; il titolare ha codici diversi per ogni ruolo per il quale può firmare.

L

LDAP - Lightweight Directory Access Protocol Protocollo utilizzato per accedere alla directory contenente i certificati ed effettuare tutte le operazioni di prelievo certificato, CRL, ecc..

Lista dei certificati revocati o sospesi - CRL (Certificate Revocation List): E' una lista di certificati che sono stati resi "non validi" prima della loro naturale scadenza. L'operazione è chiamata revoca se definitiva,

sospensione se temporanea. Quando un certificato viene revocato o sospeso il suo numero di serie viene aggiunto alla lista CRL, che viene quindi pubblicata nel registro dei certificati.

M

Manuale operativo: - Certification Practice Statement (CPS) Descrizione dettagliata del modo in cui un Ente Certificatore (CA) implementa le procedure di gestione dei certificati e delle regole per lo svolgimento del servizio. Durante la negoziazione di un certificato incrociato (vedi anche Cross-certification), le CA esaminano e confrontano vicendevolmente i propri CPS.

Marca temporale: Evidenza informatica che consente la validazione temporale. Struttura di dati firmata digitalmente che lega in modo sicuro e verificabile un qualsiasi documento informatico ad un riferimento affidabile di tempo (data e ora). In generale, il servizio di marcatura temporale fornito dagli Enti Certificatori, consente di stabilire l'esistenza di un documento informatico prima di un certo istante temporale associando all'evidenza informatica una data e ora certe validandola temporalmente.

P

PCMCIA (Personal Computer Memory Card International Association): Scheda per pc portatile con dimensioni analoghe a quelle di una carta di credito.

PEM (Privacy Enhanced Mail): E' uno standard per la trasmissione di posta sicura sulla rete Internet che si basa su tecniche crittografiche e firma digitale per la protezione dei dati trasmessi.

PIN (Personal Identification Number): Codice segreto associato ad un dispositivo di firma, utilizzato dall'utente per poter accedere alle relative funzioni.

PKCS (Public Key Cryptography Standards): PKCS è un insieme di standard per la crittografia a chiave pubblica sviluppati dai Laboratori RSA: definiscono la sintassi del certificato digitale e dei messaggi crittografati. In particolare il PKCS#10 definisce la struttura della richiesta per la certificazione della chiave pubblica di una coppia di chiavi asimmetriche; il PKCS#12 descrive una sintassi per il trasferimento di informazioni d'identità personale, tra cui chiavi private e certificati digitali a chiave pubblica, garantendo riservatezza e integrità dei dati trasmessi.

PKI - Infrastruttura di Chiave Pubblica Public Key Infrastructure Insieme di tecnologie, politiche, processi e persone utilizzate per gestire (generare, distribuire, archiviare, utilizzare,revocare) chiavi di crittografia e certificati digitali in sistemi di crittografia a chiave pubblica.

Pubblico ufficiale: Soggetto che, nell'ambito delle attività esercitate, è abilitato in base alla legge di riferimento ad attestare l'identità di persone fisiche.

PUK (Personal Unblock Key): Si riferisce ad un numero utile allo sblocco di un dispositivo (ad esempio una smart card o un token USB) nel caso si sia digitato per più volte in modo erroneo il PIN.

R

Registro dei Certificati (Directory): Il Registro dei Certificati è un archivio che contiene tutti i certificati validi emessi dal Certificatore per i quali sia stata richiesta dal titolare la pubblicazione e la lista dei certificati revocati o sospesi (CRL).

Revoca di un Certificato: E' l'operazione con cui il Certificatore annulla la validità del certificato prima della naturale scadenza. Vedi Lista dei Certificati Revocati o Sospesi - CRL.

Riferimento temporale: Informazione, contenente la data e l'ora, che viene associata ad uno o più documenti informatici.

Ruolo: Il termine ruolo indica genericamente il Titolo e/o Abilitazione professionale in possesso del Titolare del certificato, ovvero l'eventuale Potere di rappresentare persone fisiche o enti di diritto privato o pubblico, ovvero l'Appartenenza a detti enti nonché l'Esercizio di funzioni pubbliche.

S

Sistema di validazione: Sistema informatico e crittografico in grado di generare e apporre la firma digitale o di verificarne la validità.

Smart Card - Carta a microprocessore: Una smart card ("carta intelligente") è essenzialmente un computer delle dimensioni di una carta di credito: incastonato nella plastica della tessera si trova un microprocessore dotato di memoria che può essere letta e, più importante, può essere scritta, nella quale è possibile memorizzare una quantità significativa di informazioni. Contraffare una smart card è estremamente difficile perché il circuito integrato è sepolto nella plastica. In più, il circuito integrato può essere programmato per generare le proprie password e codici, con sofisticate funzioni di crittografia.

S/MIME (Secure Multipurpose Internet Mail Extension): E' il protocollo MIME di posta elettronica per la cifratura e l'invio di messaggi via Internet.

Sospensione di un certificato: E' l'operazione con cui il Certificatore sospende la validità del certificato per un determinato periodo di tempo. Vedi Lista dei Certificati Revocati o Sospesi - CRL.

SSL (Secure Socket Layer): Sistema di trasmissione dati basato su un complesso codice di crittografia che garantisce transazioni sicure sul Web.

Sysgillo CSP: (Cryptographic Service Provider) Vedere CSP.

T

Tempo Universale: CoordinatoVedere UTC.

Terzo Interessato: La persona fisica o giuridica che, ove previsto, presta il proprio consenso all'inserimento nel certificato di sottoscrizione di un Ruolo del Richiedente.

Titolare: La persona fisica identificata nel certificato come il possessore della chiave privata corrispondente alla chiave pubblica contenuta nel certificato stesso; al Titolare è attribuita la firma digitale generata con la chiave privata della coppia.

Token USB: Dispositivo in formato chiave USB, che abbina la funzione di una smart card e del suo lettore.

U

Ufficio di Registrazione Registration Authority (RA): - Entità responsabile dell'identificazione e dell'autenticazione dei soggetti della certificazione, ma che non è una CA e, pertanto, non firma né emette certificati. La RA procede al riconoscimento delle persone che si recano fisicamente ai propri sportelli e ne raccoglie dati anagrafici, tipo di servizio, etc., comunicandoli in modalità protetta alla CA.

USB (**Universal Serial Bus**): Connessione per periferiche di tipo digitale, come tastiere, mouse, scanner e consente la trasmissione dei dati a velocità elevata con prestazioni superiori rispetto alle porte seriali o parallele.

UTC - Tempo Universale Coordinato (Coordinate Universal Time): Scala dei tempi con precisione del secondo come definito in ITU-R Recommendation TF.460-5. E' il fuso orario [PDF - 1,3 MB] di riferimento da cui tutti gli altri fusi orari del mondo sono calcolati e si riferisce all'ora del meridiano di Greenwich (longitudine 0). Per conoscere l'ora in Italia è necessario calcolare +2 nel caso di ora legale e +1 nel caso di ora solare.

V

Validazione temporale (Time stamping)**:** Il risultato della procedura informatica, con cui si attribuisce, ad uno o più documenti informatici, un riferimento temporale opponibile ai terzi.

Validità del certificato: Efficacia e opponibilità al titolare della chiave pubblica, dei dati contenuti nel certificato stesso.

X

X509 Standard: che definisce il formato dei certificati digitali utilizzato per la gestione delle chiavi pubbliche degli utenti. Esso è composto da una serie di informazioni organizzate in campi che specificano: numero del certificato, la Certification Autority (CA) emittente, il nome dell'utente certificato, la sua chiave pubblica, il periodo di validità del certificato, estensioni pubbliche o private. Queste ultime informazioni rappresentano dei campi aggiuntivi e proprietari del certificato. Definisce, inoltre, le caratteristiche di un'Infrastruttura a Chiave Pubblica (PKI).

XML: eXtensible Markup Language **-** è un metalinguaggio per la definizione di linguaggi di markup, ovvero un linguaggio marcatore basato su un meccanismo sintattico che consente di definire e controllare il significato degli elementi contenuti in un documento o in un testo.