ITALIAN PATENT OFFICE

Document No.

102012902088514A1

Publication Date

20140402

Applicant

BIT4ID S.R.L.

Title

METODO PER EFFETTUARE UNA FIRMA DIGITALE

DESCRIZIONE

Campo di applicazione

La presente invenzione si riferisce ad un metodo per effettuare una firma digitale. In particolare, l'invenzione si riferisce ad un metodo del tipo sopra citato in cui un firmatario di un documento in formato digitale applica una propria chiave di crittografia in un procedimento di firma digitale la cui corretta esecuzione è determinata da almeno un altro parametro, ad esempio da un algoritmo di crittografia selezionato per il procedimento di firma.

In particolare, la presente invenzione si riferisce alla definizione di uno schema per agevolare un processo di firma digitale di un documento.

Arte nota

Come noto, per effettuare la firma digitale su un documento elettronico è previsto inserire una chiave di crittografia di un firmatario in un'applicazione di firma che riceve in input il documento elettronico da firmare.

In particolare, per apporre una firma digitale sul documento elettronico è necessario fornire all'applicazione di firma un certificato digitale associato al firmatario e applicare la chiave di crittografia (chiave privata) mediante un dispositivo sicuro, ad esempio una smartcard.

Il certificato digitale è un documento elettronico che attesta l'associazione univoca tra una chiave pubblica e l'identità di un soggetto (una persona, una società, un computer, etc) che dichiara di utilizzarla

nell'ambito delle procedure di cifratura asimmetrica e/o autenticazione tramite firma digitale. Tale certificato è fornito da un ente terzo fidato e riconosciuto come autorità di certificazione (CA) ed è a sua volta autenticato per evitarne la falsificazione sempre attraverso firma digitale ovvero cifrato con la chiave privata dell'associazione, la quale fornisce poi la rispettiva chiave pubblica associata per verificarlo.

La firma digitale è ad esempio eseguita come passo necessario per l'espletamento di un servizio fornito ad un indirizzo Internet, presso il quale è anche reperibile il documento da firmare. Il servizio ed il documento da firmare sono ad esempio memorizzati su un server collegato in rete, come la rete Internet, e raggiungibile tramite un dispositivo elettronico del firmatario, ad esempio un palmare, un personal computer e simili, anch'essi collegati in rete e dotati di un navigatore o browser, per accedere all'indirizzo Internet.

In altre parole, l'apposizione della firma digitale è richiesta per la fruizione di un servizio erogato attraverso la rete Internet e per il quale è necessario sottoporre un documento elettronico firmato. In un simile scenario, il servizio è erogato da un server web sul quale è reperibile il documento al quale apporre la firma.

Nei metodi noti, per una corretta applicazione della firma digitale, non è sufficiente che il firmatario applichi la sua chiave di crittografia ma è indispensabile che svolga correttamente alcune operazioni come lo scaricamento (download) del documento da firmare ed associato al servizio richiesto, la selezione di un algoritmo di firma al quale applicare la propria chiave di crittografia e l'inserimento di uno o

più altre informazioni che sono generalmente richieste al firmatario e che possono ad esempio includere l'inserimento da tastiera di un codice di verifica del firmatario oppure l'invio di un consenso al trattamento dei dati, senza i quali il procedimento di firma non può essere accettato o completato correttamente.

In sostanza, per la corretta applicazione della firma digitale è necessario che l'utente disponga di ulteriori informazioni accessorie che qualificano l'operazione, ad esempio potrebbe essere necessario conoscere la tipologia di certificato da utilizzare (e.g. certificato di autenticazione, certificato di sottoscrizione) oppure l'algoritmo di firma da utilizzare. Per la fruizione di un servizio web è inoltre spesso richiesto all'utente di conoscere il formato di file da utilizzare per la firma (e.g. pdf firmato) e la modalità con la quale deve essere inviata all'ente erogatore (e.g. spedizione a mezzo mail, attraverso http POST).

Queste operazioni, che incombono sul firmatario, rendono il procedimento di firma digitale soggetto a svariati errori e ne impediscono una vera e propria diffusione.

Si pensi ad esempio al seguente caso d'uso.

Un utente apre il navigatore nel proprio dispositivo elettronico, ad esempio nel personal computer o notebook, ed accede ad un servizio tramite un indirizzo Internet, presso il quale può scaricare un documento da compilare e firmare, salvandolo ad esempio in una cartella del dispositivo, in formato .doc, .pdf, .docx o .txt. L'utente può ricevere il documento da compilare e firmare tramite e-mail e salvarlo, come sopra detto.

Tuttavia, in entrambi i casi è possibile che l'utente modifichi l'estensione del file da firmare, ad esempio da .doc a .pdf, la qual cosa impedisce una corretta prosecuzione del procedimento di firma digitale.

Inoltre, se il dispositivo digitale non è un personal computer ma un dispositivo mobile, ad esempio con sistema iOS o Android, è necessario che sia dotato di un'applicazione in grado di ricevere dal navigatore il documento da firmare, dal momento che in tali sistemi non è previsto un preliminare salvataggio in cartelle (folder) dei documenti. In questo caso, l'utente deve quindi accertarsi che il suo dispositivo elettronico sia dotato di un'applicazione in grado di leggere il documento da firmare e, se non ne è già dotato, deve individuare un'applicazione adatta ed installarla sul dispositivo.

In ogni caso, per la firma del documento, l'utente non solo deve disporre dell'applicazione di firma appropriata ma deve anche selezionare uno o più parametri da inserire nell'applicazione di firma, oltre alla propria chiave di crittografia. E' evidente che anche nello svolgimento di queste operazioni possono verificarsi errori.

Supponendo ad esempio che il documento da firmare sia un file in formato .pdf, è possibile che l'applicazione di firma sia impostata di "default" per applicare un certo formato di firma, ad esempio il formato CAdES (CMS Advanced Elecronic Signatures) che genera un file firmato con estensione .p7m. Tuttavia, è possibile che per il corretto espletamento del servizio sia richiesto applicare un diverso algoritmo formato di firma, come il formato PAdES (PDF Advanced Electronic Signatures); quindi, se l'utente non modifica l'impostazione di "default"

dell'applicazione di firma, la firma digitale risulta errata, pur fornendo una chiave di crittografia valida.

Naturalmente, tra i vari possibili errori è possibile che l'utente/firmatario applichi una propria chiave ma che la chiave non è sia quella effettivamente richiesta, ad esempio potrebbe erroneamente essere inserire una chiave di autenticazione anziché una chiave di sottoscrizione.

Gli errori quindi possono essere molteplici: l'utente acquisisce il file da firmare dall'entità richiedente scaricandolo usando il proprio Internet browser o ricevendolo come allegato di una mail inviatagli automaticamente. Il file presenta un'estensione classica come .pdf, .doc, .docx, .txt al quale è associato un software installato sul sistema ospite che consente la sua elaborazione.

Attraverso il riconoscimento dell'estensione del file, MIME type, il sistema ospite dell'utente lancerà in esecuzione l'applicazione necessaria alla visualizzazione del suo contenuto. Sui sistemi desktop solitamente un browser consente il salvataggio del file trasmesso dalla applicazione web sul file system in una cartella a scelta dell'utente (e.g. Desktop, Download). Una volta ricevuto il file l'utente potrà interagire con esso in maniera agevole, ad esempio con un doppio click potrà lanciare il software che ne permette la visualizzazione o la modifica. Successivamente il file scaricato può essere inviato all'applicazione di firma digitale usando la procedura prevista da quest'ultima, ad esempio trascinando l'icona rappresentativa del file su quella dell'applicazione di firma. Sui sistemi mobile o almeno sulle piattaforme più diffuse come

iOS e Android, il file viene inviato direttamente dal browser ad un software installato che si è registrato come gestore per quella particolare estensione/MIME type. E' necessario che quindi l'applicazione di firma si registri come ulteriore gestore per la tipologia di file proposta dalla web application.

L'utente appone la firma al documento utilizzando un client di firma conforme alla normativa vigente e solitamente ulteriori istruzioni sui parametri di configurazione da utilizzare sono comunicati all'utente dall'applicazione web attraverso un messaggio in linguaggio naturale.

Apposta la firma, l'utente trasmette il documento firmato all'entità richiedente attraverso un canale da essa predisposto, ad esempio mediante e-mail oppure attraverso un upload con un'applicazione web. Solitamente il documento firmato digitalmente è un file con estensione .p7m oppure .pdf (i file PDF firmati digitalmente con il loro formato nativo hanno la medesima estensione dei file PDF privi di firma digitale). Sui sistemi mobile il file firmato digitalmente resta di proprietà dell'applicazione di firma digitale che deve prevedere in maniera autonoma un meccanismo di trasmissione compatibile con quello previsto dall'applicazione web o quanto meno l'applicazione di firma digitale deve prevedere ad una modalità di trasmissione del file firmato ad un'altra applicazione in grado di procedere alla sua trasmissione.

Lo scenario proposto dimostra che per l'apposizione della firma ad un documento, l'utente non solo deve disporre dell'applicazione di firma appropriata ma deve anche utilizzare i

parametri corretti per l'esecuzione della procedura, ed è evidente che nello svolgimento di queste operazioni possono verificarsi errori.

Supponendo ad esempio che il documento da firmare sia un file in formato .pdf, è possibile che l'applicazione di firma sia impostata di "default" per applicare un certo formato di firma, ad esempio CAdES (CMS Advanced Elecronic Signatures) che genera un file firmato con estensione .p7m. Tuttavia, è possibile che per il corretto espletamento del servizio sia richiesto applicare un diverso formato, ad esempio PAdES (PDF Advanced Electronic Signatures); quindi, se l'utente non modifica l'impostazione di "default" dell'applicazione di firma, la firma digitale risulta errata, pur avendo eseguito un processo di firma formalmente corretto. Altro possibile errore in cui l'utente potrebbe imbattersi è l'utilizzo di un certificato non idoneo all'operazione di firma, l'utente/firmatario potrebbe ad esempio utilizzare un certificato di autenticazione in luogo di uno di sottoscrizione.

Sono anche noti metodi per firmare digitalmente un documento e che guidano l'utente tramite l'utilizzo di "oggetti web attivi" come controlli ActiveX ed Applet Java. Il controllo ActiveX ad esempio è una tecnologia sviluppata dalla Microsoft® per estendere le funzioni di un'applicazione, ad esempio del navigatore, aggiungendo nuovi comandi.

Analogamente le Applet sono programmi scritti in linguaggio Java che possono essere eseguiti da un Web browser. Le applet sono utilizzate per creare pagine dotate di funzioni interattive, ad esempio per guidare le operazioni di firma dell'utente.

Anche l'utilizzo di "oggetti web attivi" presenta alcune problematiche insite nella soluzione tecnologica stessa come la difficoltà di realizzazione gli stessi oggetti per diverse piattaforme, in grado quindi di operare in ambienti eterogenei. Molte soluzioni attualmente in uso non riescono ad essere indipendenti dal:

- sistema Operativo.
- browser.
- tecnologia utilizzata per la protezione delle chiavi asimmetriche di firma digitale (e.g. tipologia di smart card, di firma remota).

Altra problematica inerente l'adozione di "oggetti web attivi" è che sono stati spesso utilizzati per attacchi informatici. Infine tra le limitazioni di tale soluzione vi è l'impossibilità di utilizzo degli stessi in uno scenario mobile in quanto i Web Browser installati sui dispositivi mobile, basati su sistemi operativi iOS ed Android, non ne consentono l'uso.

Il problema tecnico alla base della presente invenzione dunque è quello di escogitare un metodo di automazione della firma digitale che consenta di evitare errori nella firma, semplificando notevolmente il procedimento richiesto e rendendolo sostanzialmente disponibile a qualsiasi utente e su qualsiasi dispositivo elettronico, superando dunque tutte le limitazioni che tutt'ora affliggono i metodi secondo l'arte nota.

Sommario dell'invenzione

L'idea di soluzione alla base della presente invenzione è quella di incorporare tutte le informazioni necessarie per la corretta esecuzione

di una firma digitale all'interno di un file formattato, e di dare il file formattato in input ad un'applicazione di firma atta ad estrarre le informazioni e a ricevere ulteriormente in input una chiave di crittografia da un firmatario, per completare il procedimento di firma digitale.

Vantaggiosamente, secondo questa idea di soluzione, la possibilità di errore durante il procedimento di firma è sostanzialmente annullata, poiché al firmatario è solo richiesto di dare la propria chiave di crittografia in input all'applicazione di firma e poiché tutte le altre informazioni necessarie per l'esecuzione del procedimento sono incorporate nel file formattato. Vantaggiosamente, tale file formattato può comprendere anche il file da firmare.

Il vantaggio di un siffatto metodo è evidente quanto un servizio, ad esempio un servizio fornito da un server presso un determinato indirizzo Internet, è espletato solo a valle di una specifica firma digitale, cioè una firma richiedente parametri specifici.

Infatti, diversamente dai metodi noti, il servizio non invia al firmatario il documento da firmare ma bensì il file formattato che incorpora sia le informazioni o i parametri necessari per effettuare firma digitale, sia il documento da firmare. Quando il dispositivo elettronico del firmatario riceve il file formattato, esegue automaticamente l'applicazione di firma, estraendo dal file formattato il documento da firmare e le informazioni per la sua corretta firma digitale, ad esempio uno specifico algoritmo di crittografia da utilizzare.

Il firmatario è liberato da ogni controllo o azione necessaria

nel procedimento di firma e può vantaggiosamente concentrarsi sulla lettura del documento da firmare e sull'inserimento della sua corretta chiave di crittografia, per la firma.

In altre parole, l'idea di soluzione alla base della presente invenzione è quella di: creare una struttura dati che incorpori il documento da firmare e tutte le informazioni necessarie per la corretta apposizione della firma digitale in maniera conforme alle specifiche del richiedente la firma.

Una qualunque applicazione di firma, ricevendo in input la struttura dati suddetta è in grado operare il procedimento di firma in maniera autonoma e corretta. La possibilità di errore nei processi di firma in questo modo è nulla e all'utente è richiesto esclusivamente di concedere l'uso della propria chiave di crittografia all'applicazione di firma che disporrà di tutte le altre informazioni necessarie per l'esecuzione del procedimento.

Il vantaggio di un siffatto metodo è evidente in tutti quelle situazioni in cui per la fruizione di un servizio è necessario apporre una firma con specifici requisiti ad un file scaricabile da un server web. L'utente non procederà più al download del file da firmare per poi applicarvi la firma con i metodi consueti, bensì scaricherà un file contenente la struttura dati descritta che incapsula il documento da firmare e tutte le indicazioni necessarie all'apposizione della firma ed alle operazioni postume di trasmissione verso l'ente richiedente.

Quando il dispositivo elettronico del firmatario riceve il file contenente la struttura dati introdotta, esegue automaticamente

l'applicazione di firma, estraendo dalla stessa il documento da firmare e le informazioni per la sua corretta firma digitale, ad esempio uno specifico algoritmo di crittografia da utilizzare.

Il firmatario è liberato da ogni controllo o azione necessaria nel procedimento di firma e può concentrarsi sulla lettura del documento da firmare e sull'applicazione della sua corretta chiave di crittografia, per completare il processo di firma.

La richiedente ha vantaggiosamente previsto, in termini opzionali, che il file formattato abbia un formato predefinito e che l'applicazione di firma sia automaticamente eseguita quando il file formattato è scaricato nel dispositivo elettronico.

Secondo un aspetto dell'invenzione, tra le informazioni inseribili nel file formattato è anche inclusa un'azione da effettuare dopo la firma del documento, ad esempio un invio di mail ad un indirizzo predefinito ed associato ad un server di firma digitale e/o al server che offre il servizio richiesto dal firmatario.

Il metodo escogitato dal richiedente non è dunque vantaggioso solo per automatizzare una corretta firma digitale di documenti ma anche per automatizzare alcune operazioni richieste da un servizio a monte o a valle della firma digitale. In altre parole, tali operazioni possono essere strettamente inerenti il procedimento di firma digitale, ad esempio relative all'algoritmo di crittografia, o una fase che precede o segue il procedimento di firma, come ad esempio l'invio di un esito della firma digitale.

Sulla base di tale idea di soluzione, il problema tecnico sopra

esposto è risolto da un metodo per l'automazione di una firma digitale comprendente la fase di ricevere su un dispositivo elettronico di un firmatario una richiesta di firma digitale, e caratterizzato dal fatto che la richiesta di firma digitale comprende una trasmissione di un file formattato al dispositivo elettronico, comprendete parametri per una corretta esecuzione della firma digitale, il file essendo associato ad un'applicazione di firma nel dispositivo elettronico atta a rilevare i parametri dal file formattato e a concludere la firma digitale ricevendo in input una chiave di crittografia del firmatario.

Sempre sulla base dell'idea alla base dell'invenzione, il problema tecnico è risolto da un file formattato per l'automazione di una firma digitale, comprendente uno o più parametri per una corretta esecuzione della firma digitale, i parametri comprendono almeno uno tra un algoritmo di crittografia da utilizzare nell'applicazione di firma, un nome di un file da crittografare ed una sua estensione, un file da crittografare, una o più informazioni alfanumeriche per la corretta esecuzione della firma digitale, un'azione da eseguire dopo la firma digitale per la trasmissione di un esito della firma digitale, tale azione comprendendo preferibilmente un invio di e-mail ad un indirizzo predefinito o un'azione HTTP_POST.

Il problema è risolto anche da applicazione di firma digitale atta a rilevare i parametri dal file formattato sopra indicato e a concludere la firma digitale ricevendo in input una chiave di crittografia del firmatario.

La presente invenzione definisce, propone e formalizzare una

metodica per incapsulare tutte le informazioni necessarie all'apposizione della firma all'interno di un'apposita struttura dati che di fatto costituisce la "richiesta di firma" di un dato documento, i.e. una struttura dati che consenta di definire tutte le operazioni da eseguire per firmare un documento e che al suo interno contenga tutte le informazioni necessarie all'apposizione della firma ed alle operazioni che andranno eseguite una volta firmato.

Il problema dell'apposizione di una firma corretta è risolto dall'idea alla base dell'invenzione che vuole l'implementazione della struttura dati comprendente il documento da firmare ed uno o più parametri per l'apposizione di una corretta firma digitale. I parametri comprendono almeno uno tra una pluralità di fattori crittografici quali ad esempio: un algoritmo di crittografia da utilizzare, il formato di file di firma digitale da generare, l'ente certificatore di riferimento, la tipologia di certificato da utilizzare, specifica delle azioni da eseguire dopo la firma del documento.

Ulteriori vantaggi e caratteristiche del metodo, del file formattato e dell'applicazione di firma secondo la presente invenzione risulteranno evidenti dalla descrizione che segue, data a solo scopo esemplificativo e non limitativo, con riferimento alle figure allegate.

Breve descrizione delle figure

La figura 1 è un diagramma di flusso del metodo per effettuare una firma digitale secondo la presente invenzione.

La figura 2 è un esempio di una porzione di un file formattato comprendente parametri per un'esecuzione della firma digitale, secondo

il metodo di figura 1.

Descrizione dettagliata

Con riferimento alla figura 1, sono schematicamente rappresentate le fasi di un metodo per effettuare una firma digitale secondo la presente invenzione, ed in particolare per firmare digitalmente un documento tramite un'applicazione di firma 4 ricevente in input il documento da firmare ed una chiave di crittografia di un firmatario 5.

La firma digitale è ad esempio richiesta per l'espletamento di un servizio fornito da un server 9, il servizio essendo accessibile ad un indirizzo Internet 2 presso il quale è anche possibile scaricare il documento da firmare. Il servizio e il documento da firmare sono memorizzati sul server 9 e quest'ultimo è collegato ad una rete, come la rete Internet, ed è accessibile da un dispositivo elettronico 1 del firmatario 5, come un palmare, un personal computer e simili, anch'essi collegati alla rete. In particolare, il dispositivo elettronico 1 è dotato di un navigatore 6 o browser, per accedere all'indirizzo Internet 2.

In altre parole, la firma digitale è ad esempio richiesta per la fruizione di un servizio erogato da un server web 9 accessibile ad un indirizzo Internet 2. Accedendo a tale indirizzo mediante il proprio dispositivo elettronico 1, l'utente può scaricare la struttura dati per l'apposizione della firma rappresentante l'invenzione e indicata nel seguito della descrizione anche come "richiesta di firma".

Dopo aver acceduto al servizio tramite l'indirizzo Internet 2, il dispositivo elettronico 1 del firmatario riceve una richiesta 3 di firma

digitale, necessaria per l'espletamento del servizio. La richiesta di firma è ad esempio inviata dal server 9 sul navigatore 6 del dispositivo elettronico 1. Tuttavia, nulla toglie che tale richiesta 3 possa essere inviata tramite altri mezzi, ad esempio tramite e-mail, oppure tramite un altro server 8 connesso alla rete e dedicato alla gestione del processo di firma necessario per l'espletamento del servizio.

Secondo la presente invenzione, la richiesta 3 di firma digitale comprende una trasmissione di un file formattato al dispositivo elettronico 1, che include uno o più parametri per una corretta esecuzione della firma digitale, nel seguito anche indicati come informazioni per la corretta esecuzione della firma. In particolare, il file formattato è associato all'applicazione di firma 4 nel dispositivo elettronico 1, e l'applicazione di firma 4 è atta a rilevare i parametri dal file formattato e a concludere la firma digitale ricevendo in input dal firmatario solo una sua chiave di crittografia.

In altre parole, sempre secondo la presente invenzione, la richiesta 3 di firma digitale è una struttura dati comprensiva del documento da firmare ed uno o più parametri per una corretta esecuzione della firma digitale. In particolare, il file contenente la struttura dati e formattato secondo una precisa codifica è associato all'applicazione di firma 4 nel dispositivo elettronico 1, e l'applicazione di firma 4 è atta a recuperare da esso il documento da firmare ed i parametri necessari ad apporre la firma ricevendo in input dal firmatario solo una sua chiave di crittografia.

Vantaggiosamente, secondo il metodo della presente

invenzione, la possibilità di errore durante un processo di firma è sostanzialmente annullata perché il firmatario riceve sul dispositivo il file formattato che comprende tutti i parametri da impostare per la firma ed anche il corretto file da firmare per l'espletamento del servizio, e l'applicazione di firma estrae automaticamente il file da firmare e tutti i parametri necessari per effettuare correttamente la firma digitale, completando la firma solo quando il firmatario inserisce la sua chiave di crittografia. In altre parole, l'unica incombenza a carico del firmatario è l'inserimento della chiave di crittografia in input all'applicazione di firma. Qualora il firmatario inserisca erroneamente una chiave sbagliata, ad esempio una chiave di sottoscrizione anziché una chiave di autenticazione, l'applicazione di firma sospende il processo, segnalando un errore. Quindi anche questa possibilità di errore è annullata. Invece, secondo l'arte nota, qualora il firmatario utilizzi un certificato errato, ad esempio un certificato di sottoscrizione anziché un certificato di autenticazione, l'applicazione di firma sospende il processo, talvolta segnalando un errore non sempre semplice da comprendere. L'invenzione elimina anche anche questa possibilità di errore.

Secondo un aspetto della presente invenzione, è previsto che i parametri comprendano almeno una tra le seguenti informazioni:

- un algoritmo di crittografia da utilizzare nell'applicazione di firma 4, ad esempio DES, AES, etc;

- il nome di un file da firmare ed una sua estensione;

- il file da firmare, una o più informazioni alfanumeriche per la corretta esecuzione della firma digitale.

Le informazioni alfanumeriche comprendendo preferibilmente un dato temporale, come la data dell'operazione di firma, o un'azione 7 da eseguire dopo la firma digitale, per la trasmissione di un esito della firma digitale, ad esempio una trasmissione al server 9 che fornisce il servizio.

Secondo un aspetto della presente invenzione, è previsto che i parametri comprendano almeno una tra le seguenti informazioni:

- il file al quale apporre la firma;
- la modalità firma (e.g. collezione di informazioni che caratterizzano la firma come ente certificatore, tipologia, etc..);
- l'azione, specifica delle operazioni da eseguire sul file specificato (e.g. firma semplice, firma e spedisci a mezzo mail, firma e spedisci con post action).

In un contesto reale a seguito delle operazioni di firma l'applicazione di firma 4 restituirà al server 9 il documento firmato correlato di ulteriori informazioni quali l'esito del processo ed una marcatura temporale.

In una forma di realizzazione dell'invenzione, l'azione 7 da eseguire dopo la firma digitale comprende un invio di un e-mail ad un indirizzo predefinito o un'azione HTTP_POST. In una variante di realizzazione, le informazioni per l'apposizione della firma comprendono anche un'azione 7 da eseguire prima del procedimento di firma digitale.

Secondo un altro aspetto della presente invenzione, il file formattato rappresentativo della richiesta di firma ha un'estensione predefinita e l'applicazione di firma 4 è automaticamente eseguita

quando il file formattato è ricevuto nel dispositivo elettronico 1. Associando l'estensione del file formattato all'applicazione di firma si riduce ulteriormente la possibilità di errore perché non è lasciata al firmatario nemmeno la scelta di quale applicazione utilizzare per la firma. Vantaggiosamente, il firmatario 5 fornisce in input all'applicazione di firma 4 solo la chiave di crittografia per il completamento della firma digitale e tutte le altre informazioni sono automaticamente estratte dal file formattato, tramite l'applicazione di firma.

Naturalmente è possibile che l'applicazione di firma non sia installata sul dispositivo elettronico nel momento in cui il firmatario accede all'indirizzo Internet che fornisce il servizio, ad esempio al primo accesso. In tal caso, secondo un aspetto della presente invenzione, l'applicazione di firma è trasmessa dal server 9, dopo che il firmatario ha acceduto all'indirizzo Internet 2. In tal caso l'applicazione di firma è trasmessa dal server 9 al navigatore 6 del dispositivo elettronico 1.

Secondo un altro aspetto della presente invenzione, l'azione 7 per la trasmissione dell'esito della firma digitale è trasmessa dall'applicazione di firma 4 ad un server 8 di gestione della firma digitale differente dal server 9 che fornisce il servizio. Preferibilmente, in tal caso, l'applicazione di firma 4 trasmette una conferma di firma 10 ed il file firmato anche al server 9 che fornisce il servizio, secondo i parametri specificati nel file formattato.

Secondo una forma di realizzazione, il file formattato è implementato come un file di archivio, ad esempio un file .zip o un file

.JAR. Il file di archivio comprende il file da firmare in un campo DATA e i parametri per la corretta esecuzione della firma digitale in un campo MANIFEST. I parametri sono ad esempio inseriti in un file XML del tipo riportato in figura 2 dalla quale si evince che un tag <sign_request> è utilizzato per contrassegnare il tipo del file XML, cioè un file di richiesta di firma digitale, un tag <sign_params> per indicare la posizione del file XML dove reperire i parametri. Nell'esempio di figura 2, I parametri includono un numero identificativo della richiesta di firma (tag <RID>), un formato da utilizzare nel procedimento di firma (tag <Type>), un tipo di chiave da utilizzare per la firma, ad esempio una chiave di sottoscrizione (tag <Cert_Type>), ed un'azione da effettuare, ad esempio dopo la firma (tag <sign_post_Action>). Quanto sopra indicato come file XML è incluso in un file formattato per l'automazione di una firma digitale, secondo la presente invenzione che comprendente uno o più parametri per una corretta esecuzione della firma digitale e che è automaticamente rilevato da un'applicazione di firma digitale per concludere la firma digitale, ricevendo in input dal firmatario solo la sua chiave di crittografia.

Qui di seguito vengono schematicamente riassunti gli aspetti funzionali principali della presente invenzione.

La definizione di uno schema di firma digitale che utilizzi un modello di "richiesta di firma" per apporre una firma digitale. Lo schema prevede che un qualunque dispositivo elettronico di un firmatario riceva una richiesta di firma digitale memorizzata in un file con uno specifico formato e la cui estensione è associata ad un'applicazione di firma

residente. Il file rappresentativo della "richiesta di firma" comprende il documento da firmare, i parametri per una corretta esecuzione della firma digitale ed eventuali istruzioni relative alle operazioni da eseguire una volta apposta la firma al documento.

I parametri comprendono almeno uno tra una pluralità di fattori crittografici quali: un formato di firma da utilizzare nell'applicazione di firma, il documento da firmare, una collezione di informazioni per la corretta esecuzione della firma digitale come ad esempio la specifica di un'azione da eseguire dopo l'apposizione della firma digitale. L'azione successiva all'apposizione della firma comprende la restituzione del file firmato attraverso un invio di un e-mail ad un indirizzo di posta predefinito o un'azione HTTP/POST.

Il file è costruito con un'estensione predefinita e/o una specifico mime type tale che l'applicazione di firma è automaticamente eseguita quando il file formattato è ricevuto nel dispositivo elettronico e il firmatario deve soltanto concedere l'uso della propria chiave crittografica privata all'applicazione di firma per il completamento della firma digitale. Secondo un aspetto dell'invenzione, l'azione per la trasmissione dell'esito della firma digitale è trasmessa dall'applicazione di firma ad un server di gestione della firma digitale. L'applicazione di firma trasmette ulteriormente al server che fornisce il servizio una conferma di firma e il file firmato.

Il file formattato rappresentativo della "richiesta di firma" è un file archivio compresso contenente il documento firmato e le informazioni necessarie all'esecuzione della firma.

Il file di archivio comprende, in un campo DATA, un file da firmare, e, in un campo MANIFEST, un file XML che include detti parametri per una corretta esecuzione della firma digitale.

Vantaggiosamente, secondo la presente invenzione, la possibilità di errore durante il procedimento di firma è sostanzialmente annullata, richiedendo al firmatario solo di inserire la propria chiave di crittografia nell'applicazione di firma e incorporando tutte le altre informazioni e parametri necessari per l'esecuzione del procedimento nel file formattato. Il vantaggio è ancor più evidente quando un servizio è espletato solo a valle di una specifica firma digitale, cioè di una firma che richiede parametri specifici nel procedimento di firma, poiché tali parametri possono essere incorporati nel file formattato insieme al documento da firmare, ed il file formattato inviato al dispositivo dell'utente.

Ing. Mario BOTTI
N. Iscr. ALBO 493 BM

RIVENDICAZIONI

1. Metodo per effettuare una firma digitale comprendente la fase di ricevere su un dispositivo elettronico (1) di un firmatario una richiesta (3) di firma digitale, caratterizzato dal fatto che la richiesta (3) di firma digitale comprende una trasmissione di un file formattato al dispositivo elettronico (1), comprendete parametri per una corretta esecuzione della firma digitale, detto file essendo associato ad un'applicazione di firma (4) nel dispositivo elettronico (1) atta a rilevare i parametri dal file formattato e a concludere la firma digitale ricevendo in input una chiave di crittografia del firmatario.

2. Metodo secondo la rivendicazione 1, caratterizzato dal fatto che detti parametri comprendono almeno uno tra un algoritmo di crittografia da utilizzare nell'applicazione di firma (4), un nome di un file da firmare ed una sua estensione, un file da firmare, una o più informazioni alfanumeriche per la corretta esecuzione della firma digitale, dette informazioni comprendendo preferibilmente un dato temporale o un'azione (7) da eseguire dopo la firma digitale per la trasmissione di un esito della firma digitale.

3. Metodo secondo la rivendicazione 1, caratterizzato dal fatto che detta azione comprende un invio di un e-mail ad un indirizzo predefinito o un'azione HTTP_POST.

4. Metodo secondo la rivendicazione 1, caratterizzato dal fatto che il file formattato ha un'estensione predefinita, l'applicazione di firma (4) è automaticamente eseguita quando il file formattato è ricevuto nel dispositivo elettronico (1) e il firmatario (5) fornisce in input

all'applicazione di firma (4) solo la chiave di crittografia per il completamento della firma digitale.

5. Metodo secondo la rivendicazione 4, caratterizzato dal fatto che detto indirizzo Internet (2) è acceduto tramite un navigatore (6) del dispositivo elettronico (1) e la richiesta (3) di firma digitale necessaria per l'espletamento di un servizio richiesto dal firmatario è ricevuta sul navigatore.

6. Metodo secondo le rivendicazioni 2 e 5, caratterizzato dal fatto che l'azione (7) per la trasmissione dell'esito della firma digitale è trasmessa dall'applicazione di firma (4) ad un server (8) di gestione della firma digitale differente da un server (9) che fornisce il servizio tramite all'indirizzo Internet (2).

7. Metodo secondo la rivendicazione 6, caratterizzato dal fatto che detta applicazione di firma (4) trasmette ulteriormente al server (9) che fornisce il servizio una conferma di firma (10) e un file firmato.

8. Metodo secondo una qualsiasi delle precedenti rivendicazioni, caratterizzato dal fatto che detto file formattato comprende un file di archivio, preferibilmente un file .zip o un file .JAR.

9. Metodo secondo la rivendicazione 8, caratterizzato dal fatto che detto file di archivio comprende, in un campo DATA, un file da firmare, e, in un campo MANIFEST, un file XML che include detti parametri per una corretta esecuzione della firma digitale.

10. File formattato per l'automazione di una firma digitale, comprendente uno o più parametri per una corretta esecuzione della firma digitale, detti parametri comprendono almeno uno tra un

algoritmo di crittografia da utilizzare nell'applicazione di firma, un nome di un file da crittografare ed una sua estensione, un file da crittografare, una o più informazioni alfanumeriche per la corretta esecuzione della firma digitale, un'azione (7) da eseguire dopo la firma digitale per la trasmissione di un esito della firma digitale, detta azione comprendendo preferibilmente un invio di e-mail ad un indirizzo predefinito o un'azione HTTP_POST.

11. Applicazione di firma digitale atta a rilevare i parametri dal file formattato secondo la rivendicazione 10 e a concludere la firma digitale ricevendo in input una chiave di crittografia del firmatario (4).

Ing. Mario BOTTI
N. Iscr. ALBO 493 BM

CLAIMS

1. A method for making a digital signature comprising the step of receiving on a signer's electronic device (1) a digital signal request (3), characterized in that the digital signature request (3) comprises a transmission of a formatted file to the electronic device (1), comprising parameters for a correct execution of the digital signature, said file being associated to a signature application (4) in the electronic device (1) suitable to detect the parameters from the formatted file and to accomplish the digital signature receiving as an input a signer's cryptographic key.

2. A method according to claim 1, characterized in that said parameters comprise at least one among a cryptographic algorithm to be used in the signature application (4), a name of a file to be signed and an extension thereof, a file to be signed, one or more alphanumeric information for the correct execution of the digital signature, said information preferably comprising time data or an action (7) to be executed after the digital signature for the transmission of an outcome of the digital signature.

3. A method according to claim 1, characterized in that said action comprises the fact of sending an e-mail to a predetermined address or a HTTP_POST action.

4. A method according to claim 1, characterized in that the formatted file has a predetermined extension, the signature application (4) is automatically executed when the formatted file is received in the electronic device (1) and the signer (5) provides as an input to the

signature application (4) only the cryptographic key for accomplishing the digital signature.

5. A method according to claim 4, characterized in that said Internet address (2) is accessed by a navigator (6) of the electronic device (1) and the digital signature request (3) needed to perform a service required by the signer is received on the navigator.

6. A method according to claims 2 and 5, characterized in that the action (7) for the transmission of the outcome of the digital signature is transmitted by the signature application (4) to a digital signature management server (8) which is different from a server (9) which provides the service by means of the Internet address (2).

7. A method according to claim 6, characterized in that said signature application (4) further transmits to the server (9) which provides the service a signature confirmation (10) and a signed file.

8. A method according to any of the previous claims, characterized in that said formatted file comprises an archive file, preferably a .zip file or a .JAR file.

9. A method according to claim 8, characterized in that said archive file comprises, in a DATA field, a file to be signed, and, in a MANIFEST field, a XML file which includes said parameters for a correct execution of the digital signature.

10. A formatted file for the automation of a digital signature, comprising one or more parameters for a correct execution of the digital signature, said parameters comprise at least one among a cryptographic algorithm to be used in the signature application, a name of a file to be

cryptographed and an extension thereof, a file to be cryptographed, one or more alphanumeric information for the correct execution of the digital signature, an action (7) to be executed after the digital signature for the transmission of an outcome of the digital signature, said action preferably comprising the fact of sending an e-mail to a predetermined address or a HTTP_POST action.

11. A digital signature application suitable to detect the parameters from the formatted file according to claim 10 and to accomplish the digital signature receiving as an input a signer's cryptographic key (4).

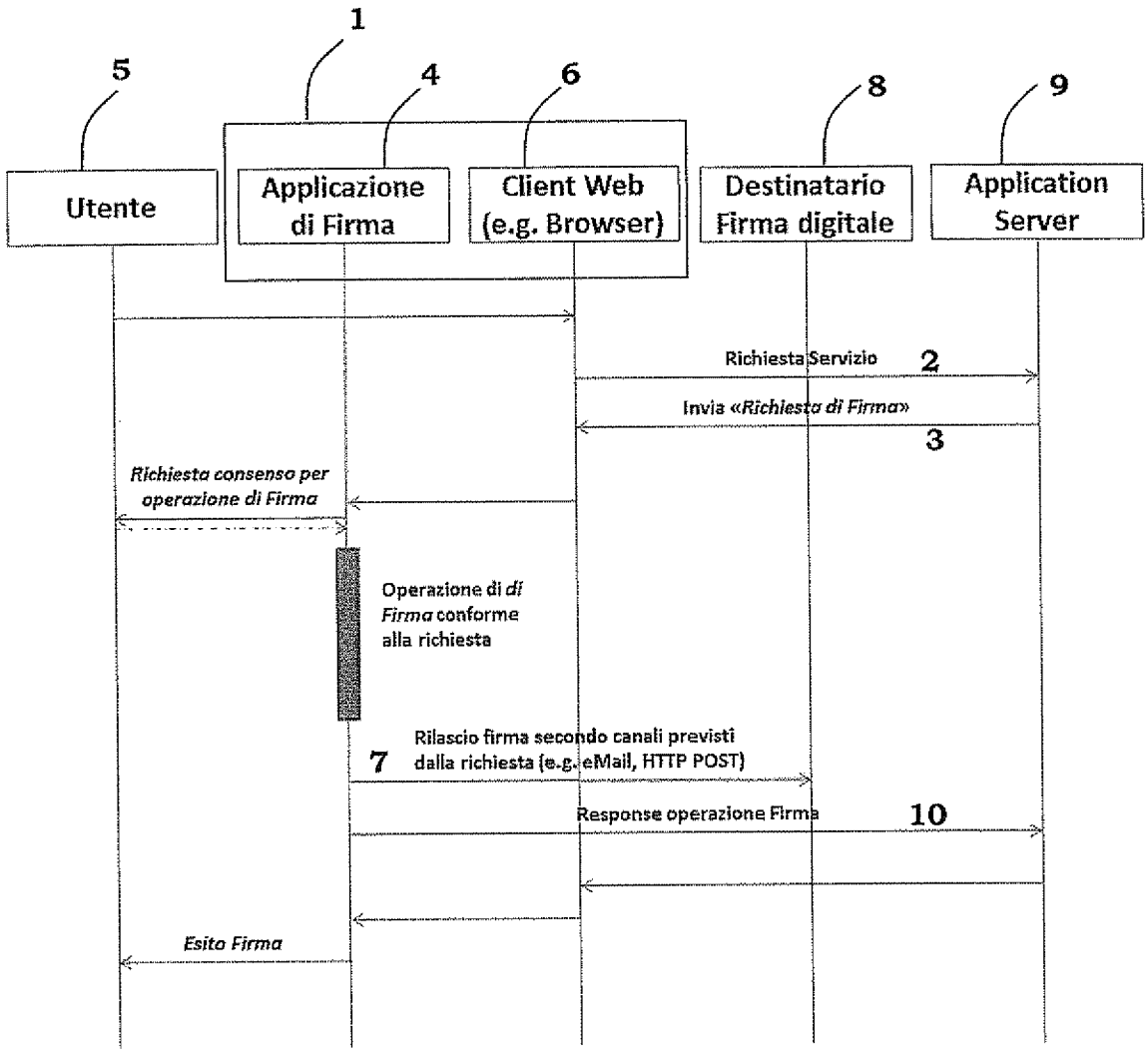

Fig. 1

Ing. Mario BOTTI
N. Iscr. ALBO 493 BM

```
<?xml version="1.0" encoding="UTF-8"?>
<sign_request>
    <sign_params>
        <RID>2939837</RID>
        <Type>pades,cades</Type>
        <Cert_Type>Sottoscrizione</Cert_Type>
        <Sign_algorithms>DSA</Sign_algorithms>
    </sign_params>
    <sign_post_Action>
        <Type>Email,HTTP_POST</Type>
        <Action>filefirmato</ Action>
        <URL>Sottoscrizione</URL>
    </sign_post_Action>
</sign_request>
```

Fig. 2

Ing. Mario BOTTI
N. Iscr. ALBO 493 BM