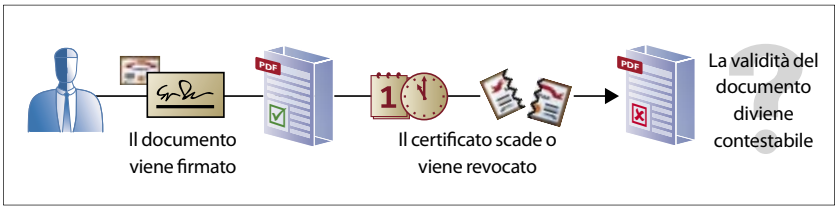
Adobe® PDF
Validità a lungo termine delle Firme Digitali

Strategie per garantire la validità a lungo temine dei documenti PDF con le firme digitali

Introduzione

L'utilizzo delle firme digitali nei documenti archiviati presenta alcuni problemi. In funzione di specifici requisiti di archiviazione, può essere necessario conservare i documenti per periodi di venti anni o più. La validità dei documenti che sono stati firmati digitalmente si basa sulla verifica affidabile delle loro firme, quindi cosa accade alla validità di una firma digitale nel lungo termine? Cosa accade a un documento firmato quando l'identità del firmatario scade, oppure quando la Certification Authority che ha emesso il certificato in origine cessa di esistere? Nel lunghissimo termine, cosa accade all'autenticità del documento quando la tecnologia utilizzata per crearlo e convalidarlo diviene obsoleta? Eventi come quelli sopra descritti costituiscono una vera sfida se si tratta di garantire nel tempo l'autenticità di un documento. In che modo le firme digitali PDF possono offrire soluzione al problema dell'integrità e dell'autenticità a lungo termine dei documenti?



Firme digitali basate sull'infrastruttura a chiave pubblica (PKI)

La funzionalità incorporata nei PDF per la firma digitale è basata sull'infrastruttura tecnologica a chiave pubblica (Public Key Infrastructure, PKI). Le firme digitali PKI utilizzano tecnologie crittografiche unicamente per identificare individui (con identità digitale e certificati) e per creare un'impronta digitale di un dato documento (un hash o una classificazione del documento). L'identità di un utente viene definitivamente legata all'impronta di un documento allo scopo di creare una "firma" unica , autenticando così il firmatario e garantendo che il documento non possa essere alterato senza invalidare la firma.

Le firme digitali coinvolgono anche "l'affidabilità". L'individuo o il gruppo che riceve un documento e che ha necessità di convalidarne la firma digitale deve potersi fidare dell'identità digitale utilizzata per creare la firma, esattamente come il commerciante ha fiducia nella società o nella banca che emette una carta di credito. Affinché una firma sia ritenuta affidabile, anche l'identità (ID) digitale di colui che la emette deve essere tale. Organizzazioni come enti pubblici, banche e grandi aziende emettono ID digitali, così come accade per i governi nei confronti dei loro cittadini. Ciò consente di stabilire una "entità fiduciaria", che sia il firmatario sia chi deve convalidare, devono poter ritenere affidabile. Questa entità fiduciaria può essere l'emittente di identità digitali all'interno di un ente pubblico o di un'azienda oppure una "autorità di certificazione" indipendente come una banca o una Certification Authority (CA) specializzata.

I certificati degli utenti finali possono essere inoltrati all'entità fiduciaria al momento della firma o della convalida. Questa operazione, combinata con il "controllo di revoca" (operazione tendente a verificare che i certificati nella catena

FIRME DIGITALI: PROBLEMI PER IL LUNGO TERMINE

- Scadenza del certificato
- Revoca delle credenziali
- Dipendenza dalle infrastrutture e dalla disponibilità
- Modifica delle relazioni di fiducia
- Obsolescenza della tecnologia e migrazione
- Durata del contratto con la Certification Authority

non siano scaduti o revocati, analogamente a quanto accade durante la convalida di una carta di credito durante un acquisto onde verificare che la stessa non sia scaduta o sia stata cancellata) mantiene l'affidabilità. Tutto ciò fornisce al destinatario la certezza dell'autenticità (mediante l'identità del firmatario) e dell'integrità (mancata alterazione del contenuto) di un documento.

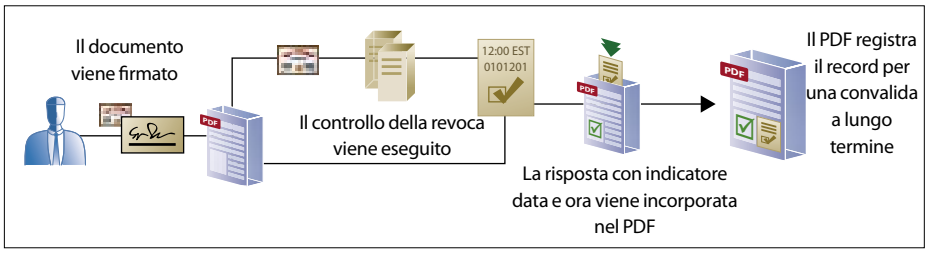
Sfide a lungo termine

Le ambiguità di verifica compaiono nei sistemi di firma basati su PKI quando le credenziali iniziano a scadere. A chiunque tenti di verificare la credenziale in questione potrebbe essere scaduta in modo convenzionale, o potrebbe essere stata deliberatamente revocata a causa di un problema di sicurezza. Situazioni simili si possono verificare nel caso in cui la Certification Authority cessi di esistere. La percezione dell'affidabilità da parte dell'utente finale è generalmente binaria: sì o no, per cui qualunque ambiguità finisce potenzialmente per introdurre disguidi e abusi. Quindi, come preservare l'autenticità di un documento oltre il tipico ciclo di vita della scadenza di un certificato, oppure anche oltre la durata della vita delle attuali tecnologie PKI? Per tentare di rispondere a questo interrogativo, di seguito verranno illustrati tre metodi per garantire la validità a lungo termine delle firme digitali.

Soluzione 1: incorporazione delle risposte del controllo di revoca (OCSP)

Il protocollo di stato dei certificati online (Online Certificate Status Protocol, OCSP) è attualmente il metodo preferito per il controllo di revoca del certificato e può essere effettuato in tempo reale, riducendo la possibilità di ricevere risposte non aggiornate. Tipicamente, questo controllo dovrebbe essere eseguito da chi deve verificare l'autenticità di un documento firmato. Ciò offre a chi verifica la possibilità di controllare lo stato corrente di un certificato di firma, ma non fornisce alcuna informazione riguardo lo stato del certificato al momento effettivo della firma del documento. In ogni caso, lo stato di un certificato al momento della firma può essere fornito incorporando la risposta di revoca all'interno del documento.

Le risposte di revoca da un server OCSP vengono di norma applicate con un indicatore di data e ora dal server che le crea. Incorporando nel documento questa risposta di revoca con indicatore di data e ora si crea una semplice firma "a lungo termine" registrando in modo sicuro la data e l'ora in cui il documento è stato firmato; questa informazione può servire come verifica in combinazione con le date valide della credenziale di firma. Se una firma è stata applicata durante il periodo di validità, anche se il certificato è al momento scaduto, il documento può essere considerato autentico.



Esempio 1

Un consorzio di produttori farmaceutici intraprende la fornitura di standard per le firme digitali tra i suoi membri e i loro trading partner. Il consorzio utilizza il PDF e Acrobat per le firme. Per rafforzare la validità legale del sistema, il consorzio vorrebbe conferire longevità alle firme oltre le date di scadenza dei loro certificati di firma. Essi hanno necessità di fornire un semplice meccanismo ad hoc di indicatori di data e ora.

Il controllo revoca certificati OCSP dei certificati di firma è un requisito dei loro standard interni, che richiedono, anche, l'incorporazione delle risposte di revoca all'interno dei loro documenti. Per utilizzare questo sistema come soluzione "leggera" e a lungo termine, essi devono semplicemente garantire che i loro server OCSP forniscano risposte di revoca mediante indicatori di data e ora e che i loro client Adobe Acrobat e Reader siano configurati correttamente per incorporare queste risposte all'interno del documento firmato. Ciò conferisce al documento con firma digitale un livello significativo di autenticità a lungo termine senza la necessità di ulteriori requisiti infrastrutturali e con un carico di lavoro relativamente ridotto per utenti finale e sistemi.

Soluzione 2: controllo affidabile di data e ora

L'applicazione di indicatori data e ora RFC 3161 è un metodo per verificare lo stato di un documento in un preciso momento. Nel processo di inserimento di indicatori data e ora, viene generata "l'impronta" di un documento (come per le firme con infrastruttura PKI). Questa impronta viene quindi trasmessa a un server di generazione di indicatori data e

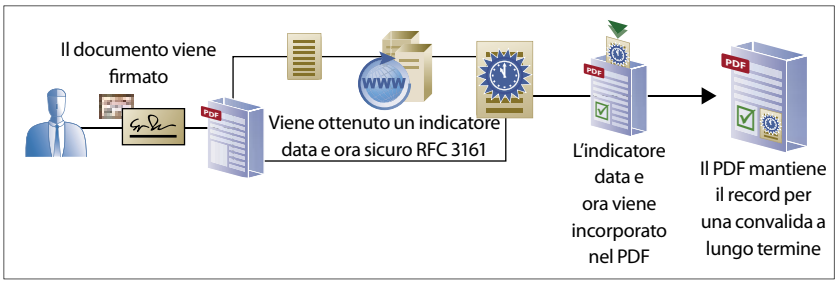
FIRME DIGITALI CONTRO FIRME DIGITALIZZATE

La famiglia di prodotti Acrobat include il supporto incorporato per firme digitali basate su PKI. Firme di tipo biometrico, "digitalizzate" e "firme dinamiche" sono supportate nei PDF mediante plug-in di terze parti.

AFFIDABILITÀ

Il concetto di affidabilità nell'infrastruttura PKI è analogo a quello tra commerciante e cliente in una transazione con carta di credito. Una banca emette carte di credito ai suoi clienti, che le possono utilizzare per effettuare acquisti presso qualsiasi punto vendita. Il punto vendita non ritiene affidabile in modo diretto il cliente, ma la banca che ha emesso la sua carta di credito. Nel caso di PKI, la "banca" è l'entità che emette il certificato: la fonte affidabile. L'autore della firma digitale è il "cliente" e il "punto vendita" è la parte accettante.

ora, che combina le risultanze di una fonte oraria affidabile con l'impronta stessa del documento allo scopo di generare una seconda firma univoca che consente di convalidare sia il contenuto sia il momento in cui al documento è stata apposta la firma digitale stessa. L'indicatore data e ora risultante può essere memorizzato all'interno del documento. Poiché l'indicatore data e ora fornisce unicamente informazioni su QUANDO è stato formato e COSA conteneva un documento, esso viene tipicamente combinato con una firma PKI per fornire informazioni su CHI l'ha firmato. Questa combinazione è in grado di offrire un'autenticazione a lungo termine per un documento, memorizzando ora e data di firma; il documento può quindi essere concettualmente convalidato nel lungo termine proprio come nell'Esempio 1 precedentemente riportato.



Esempio 2

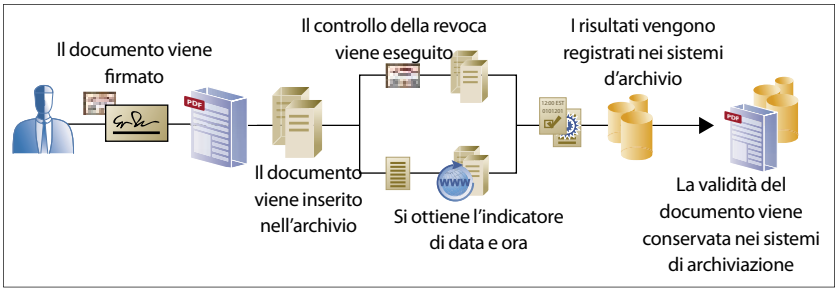
Un consorzio di consulenti finanziari decide di fornire ai suoi membri un sistema di autenticazione digitale a livello notarile. Per aggiungere valore al loro sistema, essi decidono che il loro sistema dovrebbe fornire un livello di autenticazione più elevato di una tipica firma digitale PKI. Essi hanno anche necessità di un mezzo per conciliare e convalidare l'ora e la data delle loro firme rispetto ai loro record. Poiché hanno una forma di authority centralizzata all'interno del consorzio e possono implementare un set singolo di standard per tutti i loro membri, decidono di utilizzare un server sicuro per la fornitura di indicatori di data e ora. Quando ciascun notaio inserisce una firma elettronica, essi applicano una firma digitale al documento. Al momento della firma, Acrobat può collegarsi al server centrale dell'organizzazione per ottenere l'indicatore di data e ora per il documento, il quale può essere incorporato nella firma del documento. Per rafforzare la validità, la risposta con l'indicatore data e ora potrebbe anche essere registrata dai server stessi dell'organizzazione per una futura verifica indipendente. Ciò offre una prova significativa che il certificato del firmatario era valido al momento della firma e che può anche essere utilizzato come meccanismo di verifica indipendente.

Soluzione 3: convalida di archivio

MINIMIZZAZIONE DELL'INFRASTRUTTURA

Adobe PDF e Acrobat includono efficaci funzionalità per la convalida di documenti a lungo termine. Combinando l'applicazione di indicatori di data e ora sicuri con l'incorporazione delle risposte del controllo di revoca, i documenti possono essere efficacemente resi "auto-convalidanti", riducendo così i requisiti dell'infrastruttura di convalida e massimizzando la portabilità degli stessi. Quando un documento contiene sia l'indicatore di data e ora sicuro sia il risultato degli indicatori di data e ora di un controllo di revoca, diviene "autonomamente convalidante". L'indicatore di data e ora offre un riferimento per il controllo di revoca e la firma digitale previene l'alterazione. Documenti come questi non hanno necessità di utilizzare un'infrastruttura esterna per continuare a garantire la loro validità nel tempo e possono così ridurre le spese di archiviazione a lungo termine.

Un metodo efficace per mantenere l'autenticità di un documento per periodi molto lunghi è costituito dalla completa internalizzazione del processo di autenticazione. L'archiviazione in sé coinvolge l'autenticazione e la verifica e le organizzazioni possono registrare le informazioni di convalida di un documento durante questo processo. Quando i documenti con firma digitale vengono inseriti in un archivio, sulle loro firme possono essere effettuati controlli di validità, revoca e sugli indicatori di data e ora. Il risultato di questi controlli può essere registrato insieme al documento archiviato. Nel tempo, questi metadati contenenti le informazioni di verifica potranno fornire informazioni certe sull'autenticità del documento. Fino a quando l'archivio risulterà integro, il documento e i relativi dati di convalida verranno conservati.



Esempio 3

Un tribunale accetta documenti legali, moduli e prove in formato PDF. Ogni anno riceve milioni di pagine di documenti, con involucri di archiviazione e ha necessità di garantire che tutti i documenti registrati siano conservati per più di 50 anni. Riceve file da numerose fonti con firme digitali di molteplici fornitori. Il tribunale non può contare sul fatto che i certificati siano validi di per sé o sul fatto che una

qualunque delle Certification Authority continui ad esistere oltre il loro tempo minimo di conservazione dei documenti. Quando riceve un documento, può utilizzare Adobe LiveCycle Document Security per convalidarne le firme digitali. Il sistema ottiene, quindi, un indicatore di data e ora conforme allo standard RFC 3161 per il documento valido utilizzando il proprio time server sicuro. Il risultato dei controlli viene documentato e memorizzato nei database e può essere referenziato nel sistema di gestione dei contenuti che ospita i documenti. In questo modo, non ci sono dipendenze esterne di alcun tipo, e non sussiste alcun problema al momento in cui le firme originali nel documento perderanno la validità, poiché l'informazione sulla loro validità è stata trasferita e gestita dai sistemi informatici del tribunale stesso. Il documento può quindi essere considerato valido per un periodo indefinito, coincidente con l'esistenza dei sistemi di archiviazione.

Conclusione

Questi esempi illustrano opzioni che garantiscono la validità delle firme digitali a lungo termine. Funzionalità e benefici possono cambiare, ma non esiste una risposta univoca alla pluralità di problemi. Ogni esempio precedentemente descritto ha applicazioni ideali, tuttavia è importante ricordare che nell'implementazione di un sistema di archiviazione o di firma digitale, la tecnologia e buona quanto la policy sottostante. La tecnologia da sola non è in grado di produrre archivi o firme digitali legalmente difendibili. Il miglior modo per garantire la validità legale di un qualsiasi processo documentale consiste nell'avere la certezza che la tecnologia supporti policy e procedure predisposte dall'organizzazione, e che queste ultime siano assimilate dagli utenti e rispettate con coerenza.

Nota su PDF/A

PDF/A, o PDF per l'Archiviazione, è uno standard aperto ISO per la conservazione a lungo termine dei documenti.

Adobe consente agli utenti di tutto il mondo di creare, gestire e distribuire contenuti digitali di elevata qualità.
Better by Adobe.™

Adobe Systems Italia S.r.l.
Centro Direzionale Colleoni, Viale Colleoni 5, Palazzo Taurus A3, 20041 Agrate Brianza (MI), Italia
www.adobe.it, www.adobe.com

Adobe, il logo Adobe, Acrobat, Clearly Adobe Imaging, il logo Clearly Adobe Imaging, Illustrator, ImageReady, Photoshop e PostScript sono sia marchi commerciali registrati sia marchi commerciali di Adobe Systems Incorporated negli Stati Uniti e/o in altri paesi. Mac e Macintosh sono marchi commerciali di Apple Computer, Inc., registrati Negli stati uniti e in altri paesi. PowerPC è un marchio commerciale di IBM Corporation registrato negli Stati Uniti. Intel e Pentium sono marchi commerciali o marchi commerciali registrati di Intel Corporation o delle sue filiali negli Stati Uniti e in altri paesi. Microsoft, Windows e Windows NT sono sia marchi commerciali registrati sia marchi commerciali di Microsoft Corporation negli Stati Uniti e/o in altri paesi. Tutti gli altri marchi appartengono ai rispettivi proprietari.
© 2006 Adobe Systems Incorporated. Tutti i diritti riservati.
Printed in Italy.
Q305

Adobe