Adobe® PDF Security

Comprendere e utilizzare le funzionalità di protezione di Adobe Reader e Adobe Acrobat

SOMMARIO

Perché è importante proteggere i documenti elettronici?

La maggior parte delle persone considerano la carta uno strumento affidabile per natura. Gli estratti conto bancari, i contratti e la corrispondenza ufficiale vengono spediti su carta aziendale prestampata in buste intestate. I documenti di prestito riportano firme originali.

Ogni giorno, tuttavia, un numero crescente di aziende distribuisce versioni elettroniche di questi documenti e chiede ai clienti di accettarli e di utilizzarli con lo stesso grado di fiducia che ripongono nei corrispettivi cartacei.

L'adozione di documenti elettronici invece che cartacei può contribuire ad accelerare i processi, migliorare la distribuzione delle informazioni e ridurre i costi sia per le aziende sia per i clienti. Purtroppo, anche i cosiddetti cyber criminal, sempre più esperti di informatica, utilizzano i documenti elettronici come strumenti di frode. Tentano infatti di contraffare i comunicati stampa, alterare i rapporti azionari e utilizzano messaggi scam di "phishing" per indurre le persone a rivelare informazioni personali in modo da rubare le loro identità. Questi tipi di crimine spingono le persone a diffidare dai documenti elettronici.

Ottimizzazione della protezione delle informazioni con i documenti Adobe PDF

Quando si scaricano o si ricevono documenti elettronici, è necessario avere la garanzia che siano autentici e inalterati. Le organizzazioni che creano documenti elettronici devono disporre di soluzioni per proteggere la riservatezza delle informazioni e preservare i documenti da modifiche o utilizzi non autorizzati.

Questi obiettivi sono più facili da raggiungere se i documenti sono in formato Adobe® PDF (Portable Document Format). Il formato Adobe PDF consente infatti una distribuzione e uno scambio di documenti elettronici più affidabile e sicuro. Salvando i documenti in PDF, le organizzazioni possono mantenere integro l'aspetto e il layout dei documenti originali consentendo allo stesso tempo ai destinatari di utilizzare Adobe Acrobat® o il software gratuito Adobe Reader® per visualizzare e interagire con i file ricevuti.

Sia Adobe Reader sia Acrobat includono numerose funzionalità che consentono ai destinatari di determinare se uno specifico documento PDF è autentico e quali operazioni, ad esempio la copia o la stampa, sono state limitate dall'autore del documento. Queste applicazioni consentono inoltre di firmare digitalmente i documenti PDF, ad esempio i moduli inviati da un ente commerciale o pubblico.

Gli autori di documenti PDF possono utilizzare le funzionalità aggiuntive di Acrobat per proteggere i documenti da accessi, modifiche e utilizzi non autorizzati. Con Acrobat è possibile apporre firme digitali per garantire agli utenti finali l'autenticità e l'integrità del documento PDF ricevuto. Gli autori possono inoltre gestire e controllare gli utilizzi dei documenti PDF creati.

Nelle due sezioni successive della presente guida verranno illustrate nel dettaglio le funzionalità di protezione offerte da Adobe Reader 7.0 e Acrobat 7.0 e in particolare le funzionalità per gli utenti destinatari di documenti in formato PDF. Nell'ultima sezione verranno descritte le funzionalità di protezione che gli autori possono utilizzare per proteggere i documenti e offrire ai destinatari una maggiore garanzia dell'autenticità di un documento.

I termini scritti in corsivo alla loro prima occorrenza vengono definiti nel glossario disponibile alla fine della guida.

Difendersi dai cyber criminal

I cyber criminal inviano messaggi di posta elettronica, noti come messaggi "scam" di phishing, che sembrano provenire da fonti attendibili, ad esempio istituti finanziari ed enti pubblici, per spingere gli utenti a divulgare informazioni personali riservate, che poi utilizzano per accedere a conti bancari, ottenere prestiti e perpetrare altre forme di furto d'identità.

Per aiutare le persone a proteggere la propria identità e difendersi da questo genere di violazioni, l'Anti-Phishing Working Group pubblica sul sito www.antiphishing.org informazioni sul phishing e sugli attuali messaggi "scam" in circolazione.

Adobe

In base a quali criteri è possibile stabilire se un documento Adobe PDF è affidabile?

Si immagini di aver appena ricevuto tramite e-mail un modulo Adobe PDF, apparentemente inviato dalla propria banca o società di credito, in cui viene richiesto di aggiornare le informazioni di contatto relative al proprio conto. Per considerare sufficientemente attendibile il documento, inserire le informazioni necessarie e restituire il modulo, ci si pone le domande seguenti:

> *Questo documento proviene veramente dalla mia banca o istituto di credito? Oppure è stato falsificato da un criminale che sta tentando di sottrarre le mie informazioni personali per appropriarsi della mia identità?*

Uno dei modi migliori per assicurarsi che un documento PDF sia autentico è di verificare se le eventuali firme digitali in esso contenute siano autentiche. Per semplicità, una firma digitale può essere paragonata a una scheda di identificazione elettronica che contiene determinate informazioni sulla persona o sull'entità che ha firmato digitalmente il documento PDF. Un documento PDF può contenere due tipi di firme digitali:

- **Una firma di certificazione**, che può essere applicata dall'autore del documento. In Adobe Reader e Acrobat viene automaticamente controllata l'autenticità di questo tipo di firma all'apertura del documento e viene quindi visualizzata una finestra in cui viene indicato se la firma è valida, ovvero autentica e attuale. In questa guida, la firma di certificazione viene denominata anche "firma digitale dell'autore".
- **Una firma standard**, che può essere applicata da tutti gli utenti in possesso di un'autorizzazione appropriata per la firma digitale del documento. In Adobe Reader e Acrobat viene automaticamente controllata l'autenticità delle firme standard all'apertura del documento. In alternativa, è possibile controllarle manualmente all'interno dell'applicazione.

Nota: *per il controllo delle firme digitali in Adobe Reader o Acrobat è necessario disporre di accesso a Internet.*

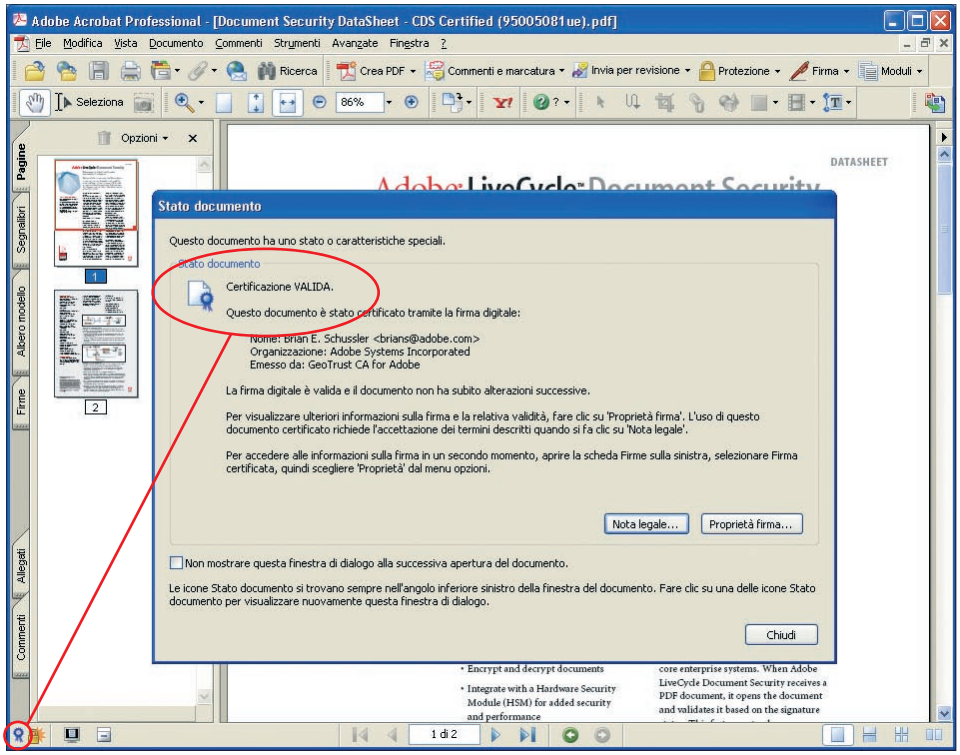
Verifica della firma di certificazione

Immediatamente dopo l'apertura di un documento Adobe PDF certificato, in Adobe Reader o Acrobat vengono automaticamente verificate la presenza di modifiche non autorizzate nel documento e l'autenticità della firma di certificazione. Viene quindi aperta la finestra Stato documento in cui viene visualizzato uno dei tre risultati possibili, che verranno descritti dettagliatamente in seguito:

- **Certificazione VALIDA**, con un nastro di colore blu
- **Validità dell'autore NON confermata**, con un punto interrogativo di colore blu accanto all'immagine di una persona
- **Certificazione NON VALIDA**, con una X di colore rosso

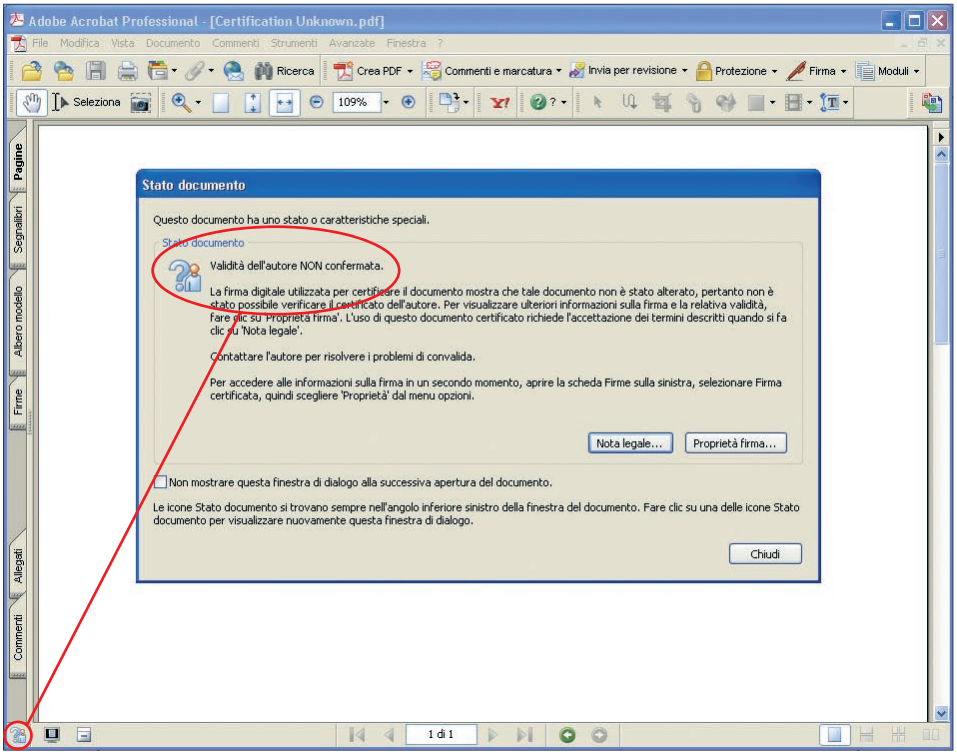
Certificazione VALIDA. Questo risultato e un nastro blu visualizzato nell'angolo inferiore sinistro della finestra principale indicano che l'applicazione ha eseguito le due attività principali. Innanzitutto, è stata effettuata la connessione a un server per verificare l'ID digitale del firmatario, che è risultato essere valido e attuale. Successivamente, è stato eseguito un confronto bit per bit del documento così com'era al momento della firma rispetto al documento al momento del controllo di convalida ed è stato rilevato che le due versioni sono identiche. Questo tipo di risultato offre un'elevata garanzia che il documento non è stato modificato e che è autentico.

Nota: *ogni entità che rilascia un ID digitale possiede requisiti e processi diversi per la conferma dell'autenticità e della precisione delle informazioni contenute nell'ID digitale. Il livello di affidabilità associato a ogni ID digitale corrisponde spesso al livello associato a questi requisiti e processi. In linea di massima, più i requisiti sono rigidi e più i processi sono complessi, maggiore sarà il livello di affidabilità associato all'ID digitale. Per ulteriori informazioni sugli ID digitali e sulla loro affidabilità, vedere "Determinare l'affidabilità delle firme digitali sconosciute" più avanti in questa guida.*



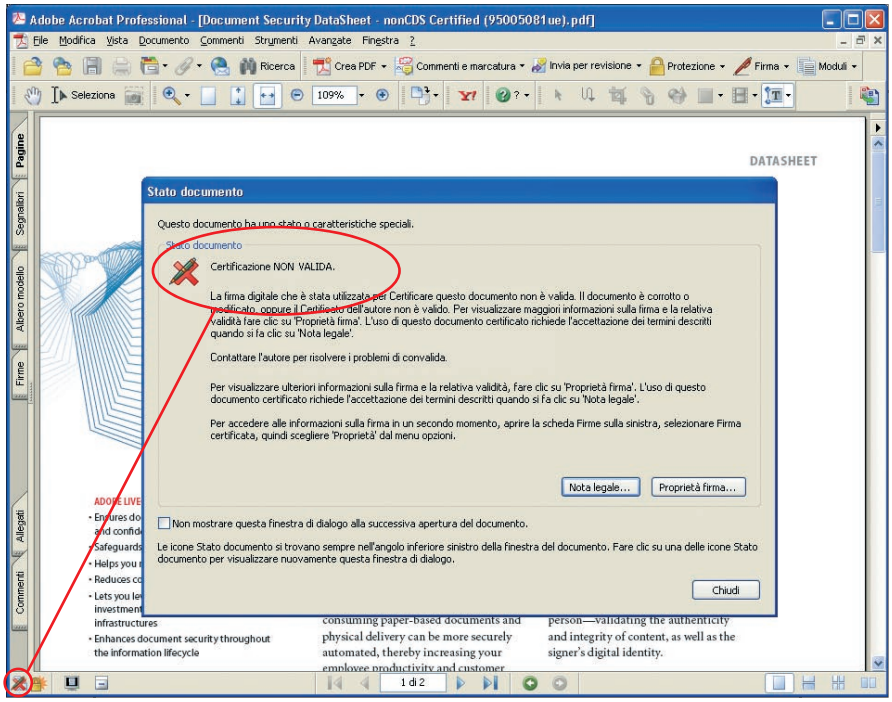
Lo stato Certificazione VALIDA nella finestra Stato documento di Adobe Reader o Acrobat consente di garantire che il documento PDF certificato è autentico e non è stato modificato. Verificare sempre che nell'angolo inferiore sinistro della finestra principale venga visualizzato anche un nastro di colore blu.

Validità dell'autore NON confermata. Questo risultato e un punto interrogativo visualizzato accanto all'immagine di una persona in basso a sinistra nella finestra principale indicano che non è stato possibile verificare l'autenticità della firma digitale dell'autore. Prima di considerare attendibile questa firma, è opportuno determinare l'affidabilità dell'ID digitale della firma, come descritto in "*Determinare l'affidabilità delle firme digitali sconosciute*" più avanti in questa guida.



Lo stato Validità dell'autore NON confermata nella finestra Stato documento di Adobe Reader o Acrobat indica che l'ID digitale del firmatario del documento PDF certificato non è stato accertato. in basso a sinistra nella finestra principale appare un punto interrogativo di colore blu accanto all'immagine di una persona.

Certificazione NON VALIDA. Questo risultato e una X di colore rosso nell'angolo inferiore sinistro della finestra principale indicano che il documento è stato alterato in qualche modo oppure che l'ID digitale utilizzato dall'autore per certificare il documento è scaduto o è stato annullato (revocato). Non è possibile considerare attendibile un documento PDF con uno stato di certificazione non valida ed è consigliabile non utilizzarlo.



Lo stato Certificazione NON VALIDA nella finestra Stato documento di Adobe Reader o Acrobat indica che il documento PDF certificato è stato modificato o che la firma di certificazione non è più valida. Nell'angolo inferiore sinistro della finestra principale viene visualizzata una X di colore rosso.

Verifica delle altre firme

Oltre alla firma di certificazione, un documento Adobe PDF può contenere una o più firme standard aggiunte da terzi prima che il destinatario riceva il documento. Quest'ultimo può, ad esempio, ricevere una versione PDF di un documento ipotecario contenente la firma digitale del consulente finanziario. Quando si aggiunge una firma digitale personale a un documento, si aggiunge anche una firma standard.

Come per le firme di certificazione, anche per le firme standard è opportuno determinare se siano attendibili controllandone l'autenticità. A tale scopo è innanzitutto necessario verificare di essere collegati a Internet per eseguire il controllo automatico delle firme digitali con Adobe Reader o Acrobat. Visualizzare quindi la scheda Firme nel riquadro di navigazione. Verranno mostrate tutte le firme di un documento. Nella scheda Firme scegliere Opzioni > Convalida firme per eseguire il controllo automatico delle firme.

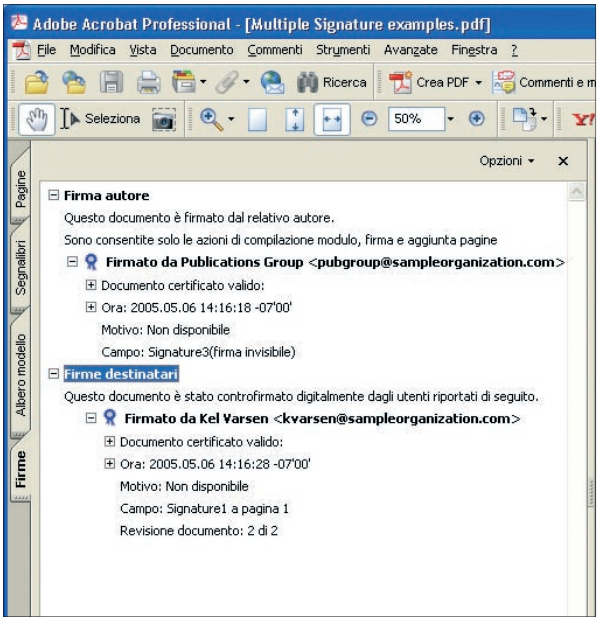
Per ogni voce contenuta nella scheda Firme verrà visualizzato uno dei vari risultati possibili. Tra questi vi sono i seguenti:

Alcune delle possibili icone di stato visualizzate in Adobe Reader o Acrobat al termine della convalida delle firme.

- **Un segno di spunta verde (Firma valida)** indica che è stata effettuata la connessione a un server per verificare l'ID digitale del firmatario, che è risultato essere valido e attuale.
- **Un punto interrogativo blu accanto a una persona (Validità della firma sconosciuta)** indica che non è possibile convalidare l'ID digitale utilizzato per firmare il documento. Prima di considerare attendibile questa firma, è opportuno determinare l'affidabilità dell'ID digitale della firma, come descritto in "Determinare l'affidabilità delle firme digitali non confermate" più avanti in questa guida.
- **Una X rossa (Firma non valida)** indica che l'ID digitale utilizzato per applicare la firma digitale non è valido poiché è scaduto oppure è stato annullato (revocato).

Nota: *le icone visualizzate sopra possono contenere anche un triangolo di avviso di colore giallo. Il triangolo indica che il documento è stato modificato dopo l'inserimento della firma. In Adobe Reader e Acrobat sono disponibili varie funzionalità per visualizzare e confrontare le versioni firmate, nonché per rilevare eventuali modifiche. Per ulteriori dettagli, vedere la sezione "Convalida delle firme".*

Per ogni firma viene indicato quando è stato firmato il documento e se è stato modificato dopo che è stata apposta l'ultima firma di uno dei firmatari autorizzati. Queste informazioni aggiuntive consentono di valutare l'affidabilità del documento.

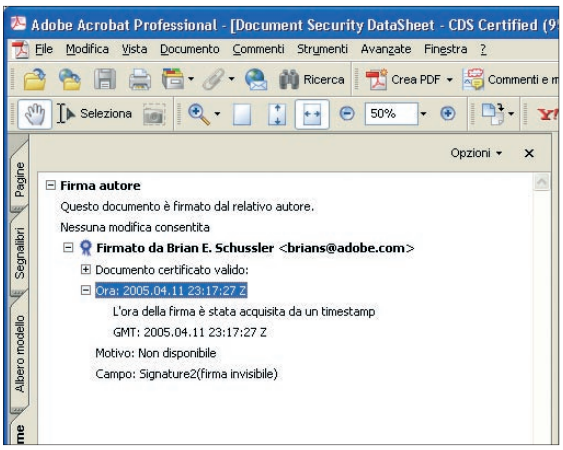


Nella scheda Firme del riquadro di navigazione è possibile visualizzare tutte le firme digitali di un documento PDF. Nel menu Opzioni della scheda è possibile convalidare le firme e visualizzare l'origine degli ID digitali corrispondenti.

Verifica del momento in cui è stato firmato un documento

Le informazioni relative all'ora e alla data di una firma digitale, denominate controllo data/ora, possono essere importanti se si utilizzano documenti vincolati dal tempo, ad esempio contratti, offerte immobiliari, richieste di finanziamento e pagamenti. Il controllo data/ora può, ad esempio, indicare quando è stata redatta un'offerta o una controfferta oppure se un documento è stato firmato prima di una determinata scadenza.

In Adobe Reader o Acrobat è possibile visualizzare i controlli data/ora delle firme aprendo la scheda Firme del riquadro di navigazione e quindi facendo clic sui segni più per espandere le informazioni relative a una specifica firma.



Per visualizzare maggiori informazioni sulla firma, ad esempio, per conoscere quando è stata applicata una particolare firma digitale, aprire la scheda Firme del riquadro di navigazione.

Gestione di documenti non certificati né firmati

Non tutti i documenti Adobe PDF che si ricevono sono certificati o firmati. Tra questi vi sono ad esempio moduli, domande, brochure, offerte speciali, annunci di modifiche a servizi e così via. Com'è possibile stabilire se questi documenti sono affidabili, in quanto integri e autentici?

In questi casi è necessario considerare in che modo si sono ricevuti i documenti e se l'origine è affidabile. Ad esempio:

- Se il documento è stato scaricato personalmente dal sito web dell'organizzazione, è più probabile che sia autentico e che non sia stato modificato.
- Se il documento è stato inviato per posta elettronica, in genere non è possibile accertare l'autenticità del documento senza contattare il mittente e chiedergliene conferma.

- Se il documento o il relativo collegamento è pervenuto in modo non richiesto oppure da un'origine sconosciuta, è opportuno prestare cautela, in quanto il documento potrebbe condurre a numeri di telefono o siti web fasulli. In caso di dubbio, utilizzare un numero di telefono o un sito web conosciuti per contattare la società che ha apparentemente inviato il documento e chiedere al reparto di assistenza clienti se il documento è sicuro.

Determinazione dell'affidabilità delle firme digitali sconosciute

Ogni volta che in Adobe Reader o Acrobat una firma digitale riporta lo stato Validità della firma SCONOSCIUTA, è necessario decidere se determinare l'affidabilità della firma in questione. Questa operazione prevede tre passaggi fondamentali:

1. Ottenere un *certificato* per la firma digitale da un individuo o da un sito web conosciuto e attendibile. Negli ambiti di lavoro richiedere il certificato al reparto IT della propria società. I certificati sono archivi elettronici che contengono informazioni relative a un singolo o un'organizzazione utilizzate per stabilirne l'identità digitale e che svolgono la stessa funzione di patenti di guida, passaporti, tessere di iscrizione e simili.

2. Aggiungere il certificato in Adobe Reader o Acrobat e quindi impostare il livello di affidabilità del certificato.

3. Convalidare nuovamente la firma.

Di solito, queste informazioni di configurazione vengono fornite dall'amministratore del computer. Per istruzioni generali sulla creazione di un elenco di identità affidabili, vedere l'argomento "ID digitali e metodi di certificazione" nella Guida di Adobe Reader o Acrobat. Per ulteriore assistenza, rivolgersi a tecnici esperti in materia di sicurezza e di funzionalità di protezione di Adobe Reader o Acrobat.

È opportuno tener presente che la valutazione dell'affidabilità di un certificato comporta pur sempre un determinato rischio. In generale, è consigliabile configurare Adobe Reader o Acrobat in modo da convalidare solo i certificati scaricati personalmente da un sito web conosciuto e attendibile o i certificati ricevuti direttamente da un individuo affidabile, dopo aver verificato di persona o per telefono che sia stato proprio quel mittente a inviare il certificato in questione.

Se si prevede di ricevere molti documenti firmati dallo stesso autore o dalla stessa società, è consigliabile approntare metodi adeguati per valutare l'affidabilità di un certificato. In questo modo ogni volta che si sceglierà l'opzione Convalida firme in Adobe Reader o Acrobat, verrà eseguito un controllo automatico a fronte dell'elenco di firme affidabili impostato dall'utente.

In che modo è consentito utilizzare un documento Adobe PDF?

"Perché non è possibile aprire alcuni documenti PDF?"

"Perché è possibile stampare alcuni documenti e altri no?"

"Perché talvolta le opzioni Copia e Incolla sono disattivate?"

"Perché a volte con Adobe Reader è possibile salvare informazioni contenute all'interno di moduli e altre volte no?"

"Com'è possibile firmare elettronicamente un modulo di richiesta dopo averlo compilato?"

In base alle modalità di protezione del contenuto scelte dall'autore di un documento Adobe PDF, è possibile riscontrare determinati limiti nell'utilizzo dei documenti PDF. Ad esempio, l'autore può impostare autorizzazioni specifiche per impedire l'apertura o l'utilizzo del documento da parte di persone non autorizzate. Le organizzazioni possono configurare un documento PDF in modo che all'apertura in Adobe Reader vengono attivate, temporaneamente ed esclusivamente per la compilazione di quel documento, funzionalità in genere non disponibili, quali il salvataggio delle informazioni immesse in un modulo. In alternativa, se il documento è un modulo, l'autore può predisporlo in modo da accettare la firma digitale del destinatario.

Di seguito vengono descritte le procedure comunemente adottate dagli autori per restringere l'accesso ai documenti e viene illustrato come determinare il tipo di autorizzazioni concesse a un utente per uno specifico documento PDF. Viene inoltre descritta la procedura di applicazione della firma a un documento per cui si dispone dell'autorizzazione appropriata.

Determinazione delle restrizioni di apertura di un documento

Talvolta può capitare di ricevere un documento Adobe PDF che non è possibile aprire. Se si riceve un messaggio in cui è indicato che per aprire il documento è necessario disporre di una versione più recente di Adobe Reader o Acrobat, è sufficiente visitare il sito www.adobe.it/products/acrobat/readstep2.html e scaricare la versione aggiornata del software gratuito Adobe Reader.

Utilizzo delle funzionalità nascoste di Adobe Reader

Alcuni documenti Adobe PDF consentono di eseguire in Adobe Reader operazioni che di solito non sono possibili. Ciò è dovuto alla possibilità di utilizzare Adobe LiveCycle Reader Extensions per creare documenti PDF che a seconda della specifica situazione sono in grado di attivare funzionalità generalmente non disponibili in Adobe Reader, tra cui le seguenti:

- Salvare localmente un modulo dopo averlo completato.
- Inviare un modulo completato tramite Internet.
- Firmare digitalmente un documento.
- Inserire commenti e rivedere un documento.

Per disporre di queste funzionalità per tutti i documenti PDF e per creare documenti PDF, è necessario passare ad Acrobat Standard o Acrobat Professional.

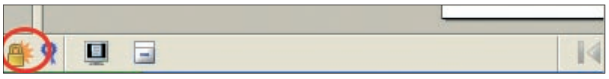
Se si riceve un messaggio in cui viene richiesto l'inserimento di una password e/o di un ID utente, significa che l'autore ha limitato l'accesso per garantire la riservatezza delle informazioni contenute nel documento. Ad esempio, l'autore può richiedere le operazioni seguenti:

- **Digitare una password** per aprire o utilizzare il documento. Se il documento è protetto tramite password, contattare l'autore per ricevere le informazioni necessarie.
- **Inserire una password e ID utente** che possono essere autenticati con Adobe LiveCycle™ Policy Server prima di poter aprire o utilizzare il documento. Se non si dispone già delle informazioni necessarie per l'accesso, contattare l'autore per ricevere un nome utente e una password adeguati.

Informazioni su Adobe LiveCycle Policy Server. Gli autori che proteggono i documenti con Adobe LiveCycle Policy Server possono tenere traccia di tutte le operazioni, ad esempio di apertura, stampa e modifica, eseguite su ogni copia di un documento. Possono inoltre modificare o revocare in qualsiasi momento i diritti di accesso. Se viene revocato l'accesso a un documento protetto con Adobe LiveCycle Policy Server, alla successiva apertura del documento in Adobe Reader o Acrobat l'utente viene informato che i diritti di accesso assegnatigli sono stati rimossi.

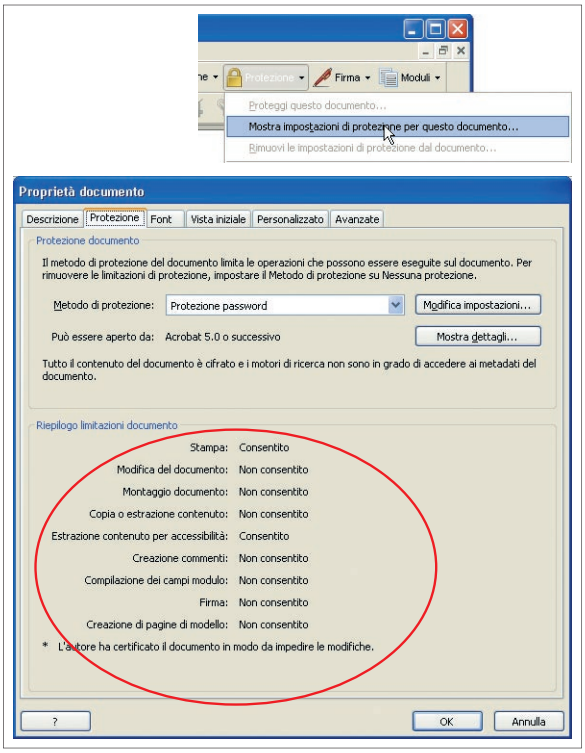
Determinazione delle altre restrizioni in un documento Adobe PDF

Un modo rapido per controllare le restrizioni applicate a uno specifico documento Adobe PDF è verificare la presenza di un'icona a forma di lucchetto nell'angolo inferiore sinistro della finestra principale di Adobe Reader o Acrobat. Spostando il mouse sul lucchetto è possibile visualizzare un riepilogo delle operazioni che l'autore ha concesso o bloccato.



Un'icona a forma di lucchetto nell'angolo inferiore sinistro di un documento PDF indica che sono state applicate restrizioni di utilizzo.

Per visualizzare le specifiche autorizzazioni e restrizioni di un documento, utilizzare il menu Protezione nella barra degli strumenti e scegliere Mostra impostazioni di protezione per questo documento oppure aprire la finestra di dialogo Proprietà documento dal menu File e selezionare la scheda Protezione. In Windows® è possibile fare clic con il pulsante destro del mouse sul lucchetto nell'angolo inferiore sinistro della finestra del documento e quindi selezionare Protezione documento.



In Adobe Reader o Acrobat utilizzare il menu Protezione nella barra degli strumenti (in alto) per verificare le impostazioni di protezione che verranno visualizzate nella finestra di dialogo Proprietà documento (in basso). In questa finestra è possibile visualizzare informazioni dettagliate su autorizzazioni e restrizioni del documento. In alternativa, è possibile aprire questa finestra di dialogo facendo clic su File > Proprietà documento e quindi selezionando la scheda Protezione.

Se si utilizza Adobe Reader in un browser web, è possibile visualizzare le impostazioni di protezione facendo clic sul triangolo visualizzato sopra la barra di scorrimento verticale. Nel menu a comparsa scegliere Proprietà documento e quindi visualizzare la scheda Protezione.

Tutte le opzioni o i comandi correlati alle restrizioni di utilizzo sono inattivi nell'intera interfaccia utente di Adobe Reader o Acrobat.

Firma di un documento Adobe PDF

Per aggiungere una firma digitale a un documento Adobe PDF, è innanzitutto necessario ottenere un ID digitale personale.

Nota: *sia Adobe Reader sia Acrobat supportano la firma digitale dei documenti. Tuttavia, è possibile utilizzare Adobe Reader per la firma dei documenti solo se l'autore ha utilizzato Adobe LiveCycle Reader Extensions per attivare la relativa funzionalità in Adobe Reader.*

Richiesta di un ID digitale. Esistono vari modi per ottenere un ID digitale:

- **Rivolgersi a un fornitore CDS (Certified Document Services), ad esempio GeoTrust.** I fornitori *CDS (Certified Document Services)* chiederanno al richiedente di attestare la propria identità prima di accordargli un *ID digitale CDS*. Questo tipo di ID digitale offre un'elevata garanzia dell'identità di una persona. In Adobe Reader o Acrobat viene automaticamente eseguito un controllo della validità di tutte le firme create con un ID digitale CDS. Per questa operazione non è richiesta alcuna modifica al computer del destinatario.
- **Rivolgersi a un fornitore CA (Certificate Authority), ad esempio GeoTrust, VeriSign o Entrust.** I fornitori *CA (Certificate Authority)* si differenziano tra loro per la quantità di informazioni che richiedono per attestare l'identità di una persona.
- **Ottenere un ID digitale dal gruppo IT della propria azienda.** Alcuni gruppi IT definiscono gli ID digitali "certificati di firma", "certificati e-mail" o "certificati di identità".
- **Creare un ID digitale autofirmato.** È possibile creare un ID digitale autofirmato utilizzando Adobe Reader o Acrobat.

Firma del documento. Il destinatario di un documento PDF può firmarlo digitalmente solo se l'autore gli ha concesso l'autorizzazione appropriata. È possibile applicare una firma digitale in vari modi, tra cui:

- Fare clic su un campo firma vuoto aggiunto dall'autore in una determinata pagina.
- Scegliere Firma questo documento dal menu Firma nella barra degli strumenti.

Se non è possibile firmare un documento in Adobe Reader o Acrobat (ad esempio, il menu Firma non è disponibile nella barra degli strumenti oppure il comando Firma questo documento non è attivo), l'utente non dispone delle autorizzazioni necessarie per apporre una firma digitale al documento in questione.

Nota: *per istruzioni su come ottenere un ID digitale, creare firme digitali e firmare i documenti, vedere l'argomento "Firma digitale di documenti Adobe PDF" nella Guida di Adobe Reader o Acrobat.*

Aspetto della firma

In Adobe Reader o Acrobat è possibile modificare l'aspetto di una firma da inserire in un documento PDF. Ad esempio, è possibile aggiungere un elemento grafico, come la scansione di una firma manoscritta oppure l'immagine del logo aziendale. Per istruzioni vedere l'argomento "Modifica dell'aspetto della firma" nella Guida di Adobe Reader o Acrobat.

Come può un autore di documenti Adobe PDF garantirne e gestirne l'affidabilità?

Gli autori di documenti Adobe PDF interessati a garantirne l'autenticità e l'integrità e a proteggerne il contenuto hanno in genere varie esigenze, tra cui le seguenti:

- Autorizzare accessi e utilizzi specifici per garantire la riservatezza delle informazioni sensibili e impedirne l'alterazione.
- Proteggere l'accesso tramite password e ID utente per controllare e monitorare l'utilizzo dei documenti.
- Garantire ai destinatari, ad esempio ai clienti, che i documenti PDF distribuiti sono autentici e integri.
- Preparare un documento PDF da far firmare ai destinatari.

In questa sezione vengono descritte le funzionalità di protezione disponibili in Acrobat per eseguire queste operazioni.

Autorizzazione degli accessi e utilizzi

È possibile limitare l'accesso e l'utilizzo di un documento Adobe PDF assegnando determinate autorizzazioni. In base alla situazione e al documento, è possibile definire quali utenti sono autorizzati ad accedere al documento e che tipo di utilizzo possono farne. In Acrobat è possibile impostare autorizzazioni per le operazioni seguenti:

- Estrapolare materiale dal documento, ad esempio copiare testo, elementi grafica o pagine da ridistribuire.

- Modificare il documento, ad esempio aggiungere o eliminare pagine, riordinare le pagine o aggiungere campi modulo e firma digitale.
- Completare moduli interattivi e firmare digitalmente il documento.
- Aggiungere commenti al documento.
- Stampare il documento con una risoluzione bassa o alta.

È possibile salvare più impostazioni di autorizzazione con un unico criterio di protezione per utilizzarle ripetutamente. Se si utilizza Acrobat con Adobe LiveCycle Policy Server, è inoltre possibile assegnare autorizzazioni diverse a ogni utente o gruppo che accede al documento PDF.

Protezione degli accessi e controllo degli utilizzi

All'interno del processo di assegnazione delle autorizzazioni, Acrobat supporta vari meccanismi di protezione dell'accesso al documento Adobe PDF e delle relative impostazioni di protezione. In questa guida verranno illustrati due metodi, ovvero la protezione tramite password e Adobe LiveCycle Policy Server. Adobe LiveCycle Policy Server è la soluzione ideale per le organizzazioni, in quanto consente di controllare più facilmente l'accesso di grandi gruppi di utenti, di modificare dinamicamente le autorizzazioni e di controllare l'utilizzo di documenti specifici.

Protezione tramite password. In Acrobat è possibile impostare tre tipi di password valide per tutti gli utenti del documento PDF.

- La password di **apertura documento** impedisce la visualizzazione non autorizzata del documento.
- La password per le **autorizzazioni** impedisce la modifica non autorizzata dei diritti di accesso.
- La password di **apertura allegato** impedisce l'apertura non autorizzata di file allegati al documento PDF.

Quando si creano password è consigliabile utilizzare una combinazione di lettere e numeri. Non è opportuno utilizzare parole o frasi facilmente decifrabili per chi conosce l'utente, ad esempio il nome del proprio animale domestico o la data di un anniversario.

Nonostante la protezione tramite password sia la soluzione più rapida per proteggere l'accesso a un documento, con Adobe LiveCycle Policy Server è possibile usufruire di una maggiore protezione.

Utilizzo di Adobe LiveCycle Policy Server per il controllo e il monitoraggio degli accessi.
Adobe LiveCycle Policy Server offre un livello di protezione superiore a quello ottenuto tramite password, poiché per ogni utente vengono richiesti un ID utente e una password specifici, e consente inoltre di gestire l'utilizzo di un documento Adobe PDF durante il suo intero ciclo di vita. Adobe LiveCycle Policy Server è progettato per le imprese e offre agli autori di documenti funzionalità di protezione aggiuntive a quelle di Acrobat. Con Adobe LiveCycle Policy Server le organizzazioni possono:

- Gestire facilmente l'accesso di grandi gruppi di utenti, ad esempio dipendenti, clienti o cittadini.
- Applicare controlli di accesso a tempo, impostando ad esempio le date di inizio e di fine di accesso a un documento.
- Revocare l'accesso a documenti già distribuiti, ad esempio per mantenere il controllo delle versioni annullando i diritti di determinati utenti ad aprire versioni precedenti di un documento di cui sono già in possesso.
- Definire e applicare facilmente criteri di protezione personalizzati per scopi diversi, utenti individuali o interi gruppi.
- Elaborare per batch i diritti di accesso di più documenti PDF alla volta.
- Controllare l'utilizzo dei documenti, tenendo traccia ad esempio del momento in cui i destinatari autorizzati hanno ricevuto, aperto, firmato o modificato un documento PDF.

Per aprire e utilizzare i documenti PDF gestiti da Adobe LiveCycle Policy Server, i destinatari devono disporre di un account registrato nel server dell'autore. Gli utenti interni di un'organizzazione possono accedere al server fornendo il nome utente e la password aziendali. Gli utenti esterni, ad esempio i clienti, possono utilizzare il proprio indirizzo e-mail e la propria password.

Garanzia dell'autenticità e dell'integrità di un documento (certificazione del documento)

L'impostazione di autorizzazioni e di opzioni di protezione dell'accesso è fondamentale per garantire la protezione della riservatezza e dell'integrità del contenuto di un documento. Tuttavia, queste precauzioni da sole non impediscono ai malintenzionati di falsificare una copia del documento, riproducendone esattamente l'aspetto ma utilizzando informazioni diverse, e quindi di inviare il documento contraffatto sotto l'identità del mittente originale.

Per garantire ai destinatari l'autenticità e l'integrità delle informazioni ricevute, è necessario certificare il documento Adobe PDF in Acrobat. La certificazione favorisce l'affidabilità in due modi:

- Innanzitutto, l'atto della certificazione prevede l'applicazione di una firma digitale di cui viene automaticamente verificata l'autenticità in Adobe Reader o Acrobat. Questo processo consente ai destinatari di accertare all'apertura del file che il documento provenga realmente dal mittente presunto.
- In secondo luogo, durante la certificazione è possibile impedire che vengano apportate determinate modifiche che altrimenti intaccherebbero la validità della certificazione stessa. Se qualcuno inserisce queste modifiche nel documento, all'apertura del documento in Adobe Reader e Acrobat il destinatario viene avvisato che il documento è stato modificato e pertanto la certificazione viene considerata non valida.

Dato che le modifiche apportate a un documento PDF possono invalidare la certificazione, è consigliabile attendere che il documento sia completo prima di certificarlo. Per certificare un documento, utilizzare File > Salva come documento certificato.

Nota: *non firmare il documento PDF prima di certificarlo. Dopo la firma del documento il comando Salva come documento certificato non è più disponibile e non è possibile certificare il documento.*

Utilizzo di Adobe Certified Document Services. Per promuovere un maggior livello di affidabilità dei documenti Adobe PDF, è possibile applicare firme digitali create da Adobe Certified Document Services (CDS). CDS nasce da una collaborazione tra Adobe e specifiche autorità di certificazione che utilizzano un processo di attenta selezione per convalidare le identità dei singoli e delle organizzazioni che richiedono ID digitali. Gli ID digitali creati da CDS vengono memorizzati in soluzioni hardware di sicurezza, ad esempio un dispositivo USB, per proteggerli da utilizzi non autorizzati o eventuali furti.

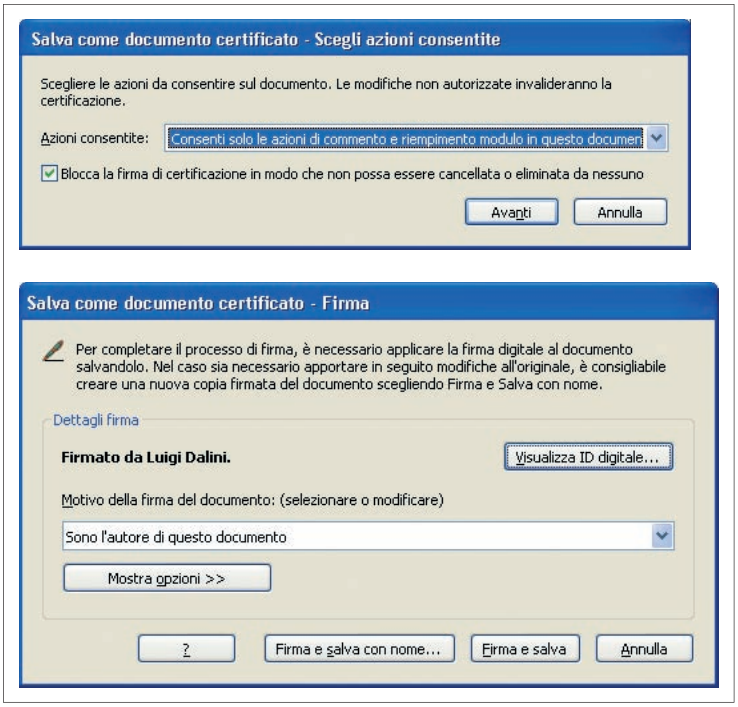
Confronto delle funzionalità di protezione di Adobe Reader e Acrobat

OPERAZIONE	ADOBE READER	ACROBAT
Funzionalità che consentono di garantire agli utenti l'autenticità e l'integrità del documento		
Certificazione dei documenti PDF		x
Controllo automatico delle firme di certificazione	x	x
Applicazione di firme digitali standard	x*	x
Controllo manuale delle firme digitali	x	x
Funzionalità che consentono di garantire la riservatezza e di proteggere i diritti di accesso		
Impostazione di autorizzazioni con la protezione tramite password		x
Impostazione di autorizzazioni con la protezione tramite certificati (PKI)		x
Impostazioni di autorizzazioni con Adobe LiveCycle Policy Server		Versione 7.0 o successiva
Funzionalità che consentono di monitorare gli utilizzi e di gestire (assegnare e revocare) i diritti di accesso dopo la distribuzione		
Applicazione di criteri di protezione con Adobe LiveCycle Policy Server		Versione 7.0 o successiva
Accesso a documenti PDF protetti con Adobe LiveCycle Policy Server	Versione 7.0 o successiva	Versione 7.0 o successiva

* Gli autori possono attivare questa funzionalità di Adobe Reader per determinati documenti PDF utilizzando Adobe LiveCycle Reader Extensions.

A differenza degli altri ID digitali, per stabilire l'affidabilità degli ID digitali CDS i destinatari dei documenti PDF non devono configurare manualmente i propri computer. Adobe Reader e Acrobat sono infatti progettati per riconoscere gli ID digitali CDS e segnalare automaticamente se la firma è valida o meno. Nel caso di ID digitali che provengono da fonti non CDS, è necessario interpretarne e valutarne autonomamente l'affidabilità e quindi configurare manualmente il computer e le applicazioni Adobe Reader o Acrobat affinché considerino attendibili gli ID digitali.

Se si desidera che i propri documenti vengano ritenuti affidabili su larga scala senza che i destinatari siano costretti a riconfigurare i computer, è consigliabile richiedere un ID digitale da un partner CDS e utilizzarlo per certificare e firmare i documenti PDF. Per un elenco di partner Adobe CDS, visitare www.adobe.com/security/partners_cds.html.



Durante la certificazione di un documento PDF è possibile scegliere le azioni consentite che ne alterino l'autenticità e l'integrità nonché includere il motivo della firma del documento (in basso).

Preparazione di un documento Adobe PDF per la firma

Per consentire a clienti e dipendenti di applicare firme digitali a un documento Adobe PDF, è necessario creare un campo modulo per ogni firmatario prima di certificare e distribuire il documento. In sostanza, il documento PDF viene trasformato in un modulo elettronico compilabile in formato PDF.

Se si desidera che il documento venga firmato da utenti del software gratuito Adobe Reader, come avviene di solito con i clienti, è necessario utilizzare Adobe LiveCycle Reader Extensions per preparare il documento PDF per la firma.

Utilizzo di Adobe LiveCycle Reader Extensions. Adobe LiveCycle Reader Extensions consente di assegnare a un documento Adobe PDF diritti estesi, che a ogni apertura del documento attiveranno temporaneamente funzionalità nascoste di Adobe Reader. Ad esempio, è possibile consentire a tutti gli utenti del software gratuito Adobe Reader di eseguire le operazioni seguenti:

- Salvare localmente le informazioni contenute nei moduli.
- Firmare digitalmente moduli e documenti.
- Aggiungere commenti.
- Inviare o indirizzare il documento PDF tramite Internet.

Dopo che l'utente ha completato tutte le operazioni necessarie in uno specifico documento PDF, le funzionalità di Adobe Reader vengono nuovamente disattivate fino a che l'utente non riceve un altro documento PDF con diritti estesi. Utilizzando Adobe LiveCycle Reader Extensions per preparare i documenti PDF è possibile migliorare la collaborazione con dipendenti e clienti.

Glossario

Adobe LiveCycle Policy Server: soluzione server Adobe che consente alle aziende di gestire l'accesso alle informazioni in modo più sicuro attraverso un controllo dinamico e costante dei documenti.

Autenticità: garanzia che un documento sia vero e che provenga dall'autore presunto.

ID digitale CDS: vedere CDS (Certified Document Services).

Certificato: nel contesto di un documento PDF, la parte pubblica di un ID digitale. Noto anche come certificato di chiave pubblica. Vedere anche ID digitale.

CA (Certificate Authority): autorità di certificazione che rilascia ID digitali. Una CA può essere un'organizzazione che vende ID digitali, come GeoTrust, VeriSign o Entrust, il reparto IT di un'azienda di grandi dimensioni, ad esempio una banca o una compagnia di assicurazioni, oppure un ente pubblico che rilascia ID digitali.

Documento Adobe PDF certificato: un documento che contiene una firma di certificazione dell'autore.

CDS (Certified Document Service): una soluzione offerta da Adobe in collaborazione con partner del settore della sicurezza che consente ai destinatari di verificare l'affidabilità di un documento PDF. CDS consente di garantire l'identità dell'autore, convalidando l'autenticità del documento, e allo stesso tempo di dimostrare che il documento PDF non è stato modificato, convalidando quindi l'integrità del documento. CDS è l'unica soluzione di sicurezza che offre la convalida automatica di questi attributi in Adobe Reader o Acrobat, senza richiedere applicazioni software aggiuntive o modifiche alla configurazione dei computer dei destinatari.

Certificare: applicare una firma digitale a un documento PDF per garantire ai destinatari che il documento proviene da una fonte affidabile (autenticità del documento) e che non sono state apportate al contenuto modifiche non autorizzate (integrità del documento).

ID digitale: identità elettronica che consente di creare una firma digitale. Un ID digitale può essere memorizzato in un file protetto da password nel computer oppure, per maggiore sicurezza, in un token USB, una smart card o un altro dispositivo hardware di sicurezza. Viene denominato anche chiave privata, credenziale, profilo, certificato di firma, certificato di identità o certificato e-mail.

Firma digitale: rappresentazione elettronica della firma di una persona creata con un ID digitale.

Integrità: garanzia che un documento non è stato contraffatto o modificato in modo non autorizzato.

Criterio di protezione: set predefinito di diritti di accesso che è possibile salvare per riutilizzarlo in un secondo momento.

Controllo data/ora: la parte di una firma digitale che indica la data e l'ora della creazione della firma. Il controllo data/ora viene generato dall'orologio di sistema del computer del firmatario oppure da un server di controllo data/ora esterno.

Selezione: un processo utilizzato da un'autorità di certificazione (CA) per verificare l'identità di un'organizzazione o di un individuo prima di rilasciare un ID digitale. Il grado di rigorosità della selezione può variare notevolmente. Alcune CA chiedono di immettere informazioni relative alla carta di credito in una pagina web, altre di presentarsi di persona muniti di uno o più moduli di identificazione rilasciati da un ente pubblico. Alcune CA prevedono inoltre il controllo delle informazioni commerciali e personali del richiedente. Più il processo di selezione adottato è severo, maggiore è la garanzia di affidabilità dell'ID digitale rilasciato da una CA.

Un ID digitale appartiene esclusivamente al proprietario, al pari di una carta di credito, e viene utilizzato per firmare digitalmente un documento PDF. L'ID digitale è costituito da una parte pubblica, denominata certificato, che viene aggiunta a ogni firma digitale creata. Il certificato serve ad attestare che la firma digitale è stata creata con il suo ID digitale.

PER ULTERIORI INFORMAZIONI

- Firma digitale con Adobe PDF, vedere www.adobe.it/firmadigitale
- Soluzioni Adobe per il controllo e la protezione dei documenti, vedere www.adobe.it/security
- Adobe LiveCycle Policy Server, vedere www.adobe.com/products/server/policy
- Adobe LiveCycle Document Security, vedere www.adobe.it/products/server/securityserver
- Adobe LiveCycle Reader Extensions, vedere www.adobe.it/products/server/readerextensions
- Adobe Certified Document Services, vedere www.adobe.com/misc/pki/cds_cp.html

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