

Dispositivo di firma *idyweb* versione 4 - Guida alla sicurezza del dispositivo -

Questa Guida, assieme alla Guida rapida, alla Guida utente, alla Guida e-commerce e alla Guida avanzata, rappresentano la documentazione utente del dispositivo di firma *idyweb* versione 4.

La Guida alla sicurezza del dispositivo fornisce informazioni e consigli per un utilizzo sicuro del dispositivo di firma.

Sommario

- Il dispositivo di firma e la sicurezza
- Introduzione alla firma digitale
- Regole per la sicurezza del dispositivo
- Protezione del certificato tramite il PIN
 - o *Profili di protezione del certificato*
 - o *Come modificare il PIN, il profilo di protezione e l'indirizzo email*
 - o *Come modificare la protezione senza cambiare profilo*
- Cosa fare in caso di smarrimento del PIN o del dispositivo
- Come controllare l'autenticità del server di *idyweb*

Il dispositivo di firma e la sicurezza

Il dispositivo di firma *idyweb* nasce come supporto alla sicurezza per l'utilizzo di applicativi web.

La comodità e il basso costo di tali applicativi ne stanno favorendo una sempre più ampia diffusione. Attualmente la quasi totalità di questi programmi, compresi quelli il cui grado di criticità è particolarmente elevato, come gli applicativi di home banking e quelli che gestiscono archivi contenenti dati personali sensibili, affidano completamente la loro sicurezza all'accesso controllato tramite un nome utente e una o più password o PIN.

Via via che la consapevolezza degli utenti verso l'importanza degli aspetti legati alla sicurezza aumenta, cresce anche la richiesta di strumenti che siano in grado di garantire la disponibilità, la confidenzialità e l'integrità (che sono i tre attributi principali in cui si sostanzia il concetto di sicurezza) del patrimonio informativo che i gestori degli applicativi web custodiscono per conto degli utenti.

Da questa esigenza è nato il progetto *idyweb*: un dispositivo per la firma digitale che assicuri il necessario livello di sicurezza alle operazioni effettuate tramite internet, mantenendo nel contempo la semplicità di utilizzo. Per fare login tramite dispositivo di firma è sufficiente avviare il proprio dispositivo (vedi la Guida rapida per l'avvio del dispositivo) e "presentare" il proprio certificato digitale alla pagina web di ingresso degli applicativi che si avvalgono di *idyweb* come sistema di autenticazione.

Introduzione alla firma digitale

La firma digitale è il risultato di un procedimento informatico che garantisce a chi invia informazioni in formato elettronico che tali informazioni giungeranno a destinazione nella loro integrità, e che solo i destinatari autorizzati potranno accedervi. Allo stesso modo, garantisce ai destinatari la certezza della provenienza (identità del mittente) e l'integrità del contenuto.

La firma digitale si basa sulla crittografia a chiavi asimmetriche: ogni titolare dispone di una coppia di chiavi, una privata, segreta e protetta da un codice di accesso (PIN), l'altra pubblica, gestita dall'organizzazione che l'ha rilasciata, che viene usata per la verifica della firma. Ciò che viene codificato con la chiave privata può essere decodificato solo con la chiave pubblica e viceversa.

Il sistema a chiavi asimmetriche è realizzato attraverso certificati digitali. Il certificato digitale dichiara la corrispondenza tra una persona e la sua chiave pubblica. Si tratta, quindi, di una sorta di documento d'identità nel mondo digitale.

Il sistema di autenticazione, commercio elettronico e firma digitale *idyweb* si basa su questi meccanismi, che oggi rappresentano standard internazionali. Tutti gli accessi, le transazioni e le interazioni tra utenti e *idyweb* e tra applicazioni e *idyweb* sono crittografati e garantiscono, pertanto, un elevato livello di sicurezza e riservatezza.

Regole per la sicurezza del dispositivo

Agli utenti *idyweb* viene assegnato un certificato digitale personale registrato su un supporto rimovibile (chiave USB o cd-card): l'insieme viene chiamato "dispositivo di firma". Il dispositivo ha numerose funzionalità, tutte garantite dall'elevato livello di sicurezza legato ai meccanismi crittografici. E' importante, tuttavia, attenersi scrupolosamente alle prassi di seguito indicate, che assicurano che la sicurezza di tipo informatico assicurata dal dispositivo non sia vanificata dal comportamento incauto del suo possessore.

La possibilità di utilizzare il dispositivo di firma è legata a due fattori: il possesso fisico del dispositivo e la conoscenza del PIN di protezione del certificato. I sistemi che utilizzano *idyweb* come metodo di autenticazione assumono che chi sia in possesso di un certificato digitale e ne conosca il PIN, ne sia anche il legittimo titolare, esattamente come un terminale POS fa con chi inserisca un bancomat e digiti il PIN corretto. Ne consegue che:

1. il dispositivo deve essere considerato come strettamente personale: non deve essere prestato, ceduto, lasciato in posti in cui possa essere sottratto.
2. il PIN di protezione del certificato deve essere memorizzato con attenzione. Non dovrebbe essere scritto su un foglietto. Nel caso, evitare di conservarlo assieme al dispositivo. Si sconsiglia di utilizzare la funzionalità di registrazione del PIN sul dispositivo stesso.
3. qualora più persone all'interno di una stessa organizzazione abbiano la necessità di accedere alle stesse funzionalità e agli stessi dati (ad esempio più impiegati che tengono la contabilità di una azienda), ciascuna di esse dovrà essere dotata di un proprio dispositivo personale.
4. evitare di utilizzare il dispositivo su PC "non sicuri", cioè su PC che potrebbero essere infettati da virus, spyware e simili; assicurare nel tempo la sicurezza dei PC tramite gli appositi software di sicurezza: antivirus (indispensabile), firewall (utilizzare almeno quello di Windows XP), antispyware.
5. modificare periodicamente il PIN
6. in caso di smarrimento del dispositivo, informare immediatamente l'ufficio commerciale di Indaco, che provvederà ad invalidare il certificato smarrito e ad emetterne uno nuovo a sostituzione.

A garanzia della totale sicurezza e riservatezza del titolare, l'unica copia esistente della sua chiave privata è quella memorizzata sul suo dispositivo, che è dotato di una protezione anticopia.

Questi consigli, validi in generale, diventano tanto più importanti quanto più il dispositivo è utilizzato per accedere ad applicativi che contengono informazioni di valore o sensibili, come dati personali, o per effettuare transazioni di tipo economico oppure ancora per la firma di documenti o l'autorizzazione di azioni e provvedimenti.

In questi casi, oltre all'utilizzo dei profili di protezione del certificato più elevati, si consiglia l'utilizzo di dispositivi dotati di eeprom per la custodia sicura del certificato oppure di dispositivi biometrici.

Protezione del certificato tramite il PIN

Profili di protezione del certificato

E' possibile modulare il livello di protezione del certificato tramite l'inserimento del PIN in modo da adattarlo al proprio contesto di utilizzo. Sono disponibili 5 profili di protezione, con livello crescente di sicurezza, che possono rispondere adeguatamente alle realtà del proprio ambiente di lavoro e alla criticità dei dati e degli applicativi utilizzati tramite il dispositivo:

- **1 (Al portatore)**: con questo profilo è possibile registrare il PIN sul dispositivo, in modo da non doverlo inserire ad ogni avvio. Questa opzione ne fa un dispositivo "al portatore", ossia: non è necessario nemmeno conoscere il PIN per poter utilizzare il dispositivo. Ne sconsigliamo l'utilizzo al di fuori di ambienti assolutamente sicuri, in cui non vi sia alcun rischio che qualcuno si appropri del dispositivo, né rischio di smarrimento.
- **2 (Dispositivo + PC)**: con questo profilo è possibile registrare il PIN sul PC a cui il dispositivo è collegato. In questo modo non sarà necessario inserire il PIN per avviare il dispositivo su tale PC, mentre sarà necessario inserirlo qualora si utilizzi il dispositivo su altri PC.
- **3 (Verifica PIN all'accesso)**: con questo profilo il PIN viene sempre richiesto all'avvio del dispositivo.
- **4 (Verifica PIN all'accesso e rinnovo)**: come per il livello 3, ma viene richiesto il rinnovo (variazione) del PIN ogni tre mesi.

- **5 (Verifica continua del PIN):** come per il livello 4. Inoltre il dispositivo rileva il tempo di inattività del PC e richiede il PIN di attivazione all'arrivo di una nuova richiesta di firma, qualora siano trascorsi più di 5 minuti dall'ultima attività rilevata (mouse o tastiera).

In alcuni casi può essere richiesta ad un utente una impostazione minima del suo profilo di protezione:

- un delegato può specificare il profilo di protezione minimo da lui ritenuto necessario e per accettare richieste di autorizzazione da un delegante (vedi sezione *Deleghe* nella Guida Utente). Qualora il delegante non abbia applicato un profilo di livello uguale o superiore a quello richiesto, ogni sua richiesta di autorizzazione (vedi sezione *Richieste di autorizzazione* nella Guida Utente) andrà fallita senza essere presentata al firmatario.
- un applicativo può richiedere un profilo di protezione minimo come condizione essenziale per le operazioni di accesso all'applicativo, emissione di richieste di autorizzazione, o loro firma. Qualora il dispositivo non abbia applicato un profilo di livello uguale o superiore a quello richiesto dall'applicativo, le operazioni relative non avranno successo.

Come modificare il PIN, il profilo di protezione e l'indirizzo email

Per modificare questi dati, e anche per controllare quale è il profilo attualmente impostato, accedere alla maschera di inserimento nuovo PIN, scegliendo dal menù principale l'opzione *Utilità->Cambia PIN*:



Per motivi di sicurezza, per accedere a questa maschera viene richiesto il PIN attuale (v. la sezione *Inserimento del PIN* nella Guida rapida per le modalità di inserimento del PIN). Dopo averlo inserito si apre una prima maschera che permette di modificare il proprio indirizzo email (che viene da idyweb per le comunicazioni agli utenti) e il proprio profilo di protezione.



Nella parte sinistra della maschera è possibile modificare il proprio indirizzo email, mentre nella parte destra della maschera è presente un cursore da posizionare sul livello di protezione da impostare. Premere OK per confermare. Si apre una seconda maschera che consente l'impostazione di un nuovo PIN.



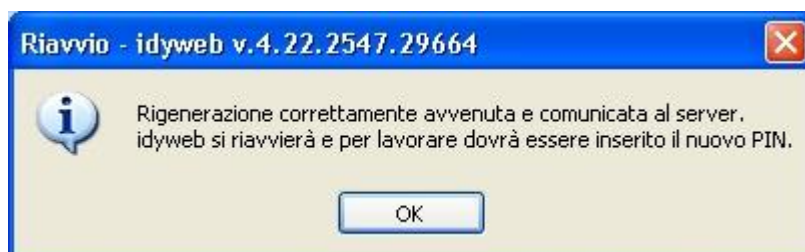
Inserire due volte il nuovo PIN e premere OK. Tenere presente le regole per la formazione di un PIN sicuro:

- deve essere lungo tra 6 e 12 caratteri;
- deve contenere almeno una lettera minuscola, una maiuscola e un numero;

Una volta confermato il nuovo PIN apparirà un messaggio che invierà ad uscire dai programmi che usano idyweb (nel caso se ne abbia uno aperto).



Il nuovo PIN viene rigenerato e appare un messaggio che conferma l'avvenuta operazione e informa che il dispositivo verrà riavviato.



Nel caso le proprie impostazioni di sicurezza lo prevedano, al riavvio verrà richiesto l'inserimento del nuovo PIN.

Come modificare la protezione senza cambiare profilo

E' possibile modificare il livello di protezione legato alla richiesta del PIN anche senza modificare il proprio profilo. Scegliendo dal menù principale l'opzione *Richiesta del PIN*, si possono selezionare alcune opzioni che modificano le modalità con cui idyweb effettua la richiesta del PIN.

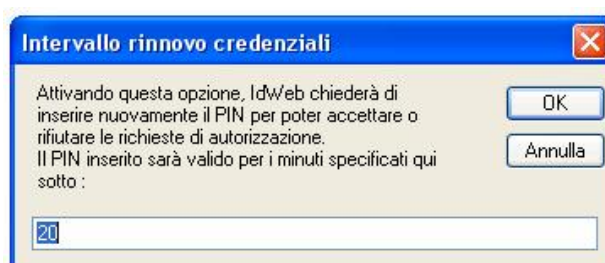
Sono disponibili fino a quattro opzioni, ma vengono mostrate solo quelle compatibili con il profilo di protezione impostato:

- **Registra il PIN del certificato su questo dispositivo:** questa opzione registra il PIN del certificato sul dispositivo, sul un file crittografato. In questo modo non è necessario inserirlo ad ogni avvio. Questa opzione ne fa un dispositivo "al portatore": in pratica non è necessario conoscere il PIN per poter utilizzare il dispositivo. Ne sconsigliamo fortemente l'utilizzo al di fuori di ambienti assolutamente sicuri, in cui non vi sia alcun rischio che qualcuno si appropri del dispositivo, né rischio di smarrimento.

- **Registra il PIN del certificato su questo dispositivo:** questa opzione registra il PIN del certificato in forma crittografata sul PC a cui il dispositivo è collegato. In questo modo non sarà necessario inserire il PIN per avviare il dispositivo su tale PC, mentre sarà necessario inserirlo qualora si utilizzi il dispositivo su altri PC. Può essere utilizzato sui PC di cui si abbia l'uso esclusivo, e il cui accesso sia protetto da login e password.



- **Attiva richiesta del PIN dopo 20 minuti dall'ultima richiesta:** con questa opzione, *idyweb* richiederà di specificare un intervallo di tempo da attendere dopo l'ultima richiesta di autorizzazione. Al termine di questo intervallo, al sopraggiungere di una nuova richiesta di autorizzazione, il sistema solleciterà l'inserimento del PIN per verificare l'identità dell'utente prima di mostrare la richiesta e consentire all'utente di accettarla o rifiutarla.



- **Attiva richiesta del PIN dopo 5 minuti di inattività:** con questa opzione, *idyweb* verifica se il computer è stato utilizzato negli ultimi 5 minuti, e se risulta inattivo richiede il PIN per verificare l'identità dell'utente prima di mostrare la richiesta e consentire all'utente di accettarla o rifiutarla. Questo comportamento è standard per i certificati di profilo 5 ("con verifica continua PIN"), per i quali non può essere disattivato.

Cosa fare in caso di smarrimento del PIN o del certificato

Chi avesse dimenticato il PIN deve chiamare il nostro ufficio commerciale e chiedere una nuova emissione del certificato del dispositivo. Verrà emesso un nuovo certificato e l'utente riceverà tramite posta elettronica le istruzioni per installarlo e sostituirlo a quello vecchio sul dispositivo rimovibile. I nostri uffici comunicheranno anche il nuovo PIN. Si raccomanda di modificare immediatamente questo PIN in modo da preservare l'assoluta confidenzialità del proprio dispositivo.

In caso di smarrimento del dispositivo, è necessario chiamare subito il nostro ufficio commerciale per far invalidare il certificato, in modo che non possa essere utilizzato abusivamente. Anche in questo caso il nostro ufficio provvederà ad una nuova emissione con le stesse modalità descritte sopra.

Si precisa che i nostri sistemi informativi e le nostre procedure operative non prevedono in nessun modo la conservazione di copia dei certificati emessi e dei relativi PIN. Non è pertanto possibile richiedere al nostro personale duplicati del proprio certificato o del PIN. Si raccomanda, pertanto, di memorizzare il PIN e di conservare il proprio dispositivo con cura.

Come controllare l'autenticità del server *idyweb*

Collegarsi alla pagina <https://idweb.indacoweb.com/AIW/>. Facendo doppio click sul lucchetto giallo in basso, nella barra di stato, si visualizza finestra dei certificati.



In Internet Explorer 7 il lucchetto si trova a destra della barra degli indirizzi:



Selezionare il Tab "Dettagli" ed esaminare le 3 voci indicate verificando che i loro valori coincidano con quelli riportati di seguito.



Identificatore della chiave dell'oggetto: 55 2d ce cc 3f a5 a0 36 b4 db 20 9c 92 05 ef 66 3c ed 31 f6

Identificativo chiave dell'autorità:

ID chiave=cd 3a ab 97 93 04 80 71 b9 6f d0 75 69 ca 8a b2 c4 a6 71 56

Autorità di certificazione:

Indirizzo directory:

CN=Idyweb CA

OU=idyweb Certification Authority

O=idyweb

L=Falciano

S=San Marino

C=SM

Numero di serie certificato=00 ed 38 6f ed 5d 33 1b 01

Identificazione personale: b2 62 22 14 49 66 0b 35 31 f8 59 5f b0 ff 43 90 65 69 0c 11