



soluzioni di **Firma Remota**
con PkBox



Il prodotto ideale per creare soluzioni di firma centralizzata

PkBox è il prodotto ideale per creare soluzioni di firma centralizzata. Pensato per aziende di qualsiasi dimensione soddisfa tutte le esigenze di funzionalità, prestazioni, capacità, affidabilità, scalabilità e prezzo.

PkBox è conforme a tutti i requisiti normativi Italiani ed Europei, ed è stato pensato per offrire interfacce di programmazione assolutamente semplici e facilmente integrabili nelle applicazioni esistenti, per poter essere configurato e dimensionato in base a qualsiasi esigenza senza per questo richiedere interventi sui codici sorgente.

Firma Remota

Firma Remota

La normativa Italiana sulla firma digitale permette l'uso di soluzioni di firma qualificata a valenza legale che prevedano l'uso di chiavi crittografiche generate e a bordo di un dispositivo HSM (certificato Common Criteria EAL4+). L'HSM può essere installato remotamente e sostituisce a pieno titolo, nei casi permessi, il dispositivo personale direttamente gestito dall'utente (smartcard o token).

Ai fini della valenza legale delle operazioni di firma remota, il possesso esclusivo della credenziale e la volontà esplicita della firma devono essere garantite tramite strumenti di Strong Authentication che permettano di verificare in modo certo l'identità della persona e lo sblocco controllato dell'operazione.

Strong Authentication

La normativa Italiana non indica con precisione quali siano le tecnologie di autenticazione valide per la realizzazione di soluzioni di firma remota. Va quindi adottata una soluzione che risulti adeguatamente sicura e affidabile, eventualmente considerando il parere autorevole degli enti qualificati a validare e "autocertificare" l'aderenza delle infrastrutture di firma ai requisiti normativi, le Certification Authority.

Se si tiene conto degli aspetti essenziali di sicurezza e di protezione dalla copia degli algoritmi crittografici e della protezione delle chiavi, si possono certamente considerare validi gli approcci basati sulla generazione dinamica di codici validi per una sola autenticazione (codici OTP, One Time Password).

Meccanismi di autenticazione

- OTP per firma remota (va indicato il provider da usare)
- OTP per sblocco firma automatica (va indicato il provider da usare)
- Doppio Pin
- Singolo Pin
- Nessuna autenticazione

La richiesta di autenticazione forte, durante l'operazione di firma, distingue la firma qualificata remota dalla firma automatica (anche massiva). Nel secondo caso, l'autenticazione dell'utente deve avvenire solo nei momenti in cui si attiva o si sospende il servizio. Una volta attivato, il servizio di firma potrà procedere in autonomia senza il coinvolgimento dell'utente proprietario della credenziale.

PkBox prevede la possibilità di gestire le credenziali indicando singolarmente, per ognuna di esse, la modalità di autenticazione richiesta e se necessario l'*Authentication Provider* da utilizzare.

Configurando quindi opportunamente le credenziali è possibile effettuare, sullo stesso server, sia operazioni di firma remota sia di firma automatica.

In alternativa è possibile adottare tecnologie biometriche ma queste non sono ancora dichiaratamente gradite dagli enti di controllo Italiani e vanno quindi considerate con cautela.

Le soluzioni possibili si distinguono poi in base allo specifico dispositivo e/o canale usato per la generazione dei codici e la successiva comunicazione all'utente.

PkBox offre la massima flessibilità di configurazione permettendo, come già detto, di impostare liberamente, per ognuna delle credenziali, il meccanismo di autenticazione da utilizzare e il provider associato.

Authentication Provider. Vers. Base

- Intesi PassID SMS
- Intesi PassID Mobile
- RSA Authentication Manager
- RSA SecurID Authentication Engine (SAE)
- Vasco Identikey Authentication Server
- Vasco Vacman Controller



Leader per **Innovazione**

PkBox - Server di Sicurezza per la Firma Digitale Massiva

PkBox è il server di sicurezza che permette di aggiungere senza sforzo funzionalità di firma digitale, di crittografia e di autenticazione ai server che gestiscono i dati e i processi delle applicazioni aziendali. Grazie alle sue caratteristiche di semplicità, flessibilità e configurabilità, PkBox rappresenta la soluzione migliore oggi disponibile per gestire in modo rapido e completo tutte le problematiche di firma digitale e di protezione dei dati su sistemi applicativi non presidiati dal lato server.

PkBox può supportare contemporaneamente connessioni con diversi server applicativi; può essere installato sia su una macchina indipendente, sia sullo stesso server applicativo in modo da ridurre ulteriormente il costo della soluzione complessiva.

Più PkBox possono essere utilizzati per ottenere capacità di tolleranza ai guasti e di bilanciamento del carico. PkBox può essere interfacciato utilizzando molteplici interfacce/protocolli quali Soap/XML, Http, Java, .Net/Com; è indipendente dalla piattaforma e può essere configurato per utilizzare diversi dispositivi crittografici hardware e software.

PkBox può essere equipaggiato con differenti token crittografici, per offrire un'ampia scelta di configurabilità dell'installazione finale, sia dal punto di vista delle prestazioni, sia dal punto di vista del costo totale del server di sicurezza.

PkBox è disponibile nelle diverse versioni:

PkSdk

Librerie gratuite per la programmazione con PkBox

E' la proposta gratuita di Intesi per facilitare l'approfondimento delle modalità di programmazione con PkNet e PkBox senza richiedere alcun investimento iniziale in termini di prodotto. Con PkSdk infatti vengono fornite tutte le informazioni e tutte le librerie PkBox Client necessarie per la realizzazione di applicazioni in grado di eseguire operazioni di sicurezza. Il prodotto PkSdk è scaricabile direttamente dal sito www.pksuite.it.

PkBox Basic

Server di sicurezza per la firma massiva

E' il prodotto server che Intesi propone per la realizzazione di soluzioni di Firma Massiva e di automazione di funzionalità di sicurezza logica dei dati secondo quanto indicato dalla normativa di legge Italiana ed Europea.

PkBox Advanced

Elevate funzionalità di firma con supporto HSM

E' la proposta di Intesi per la Firma Massiva a norma di legge per applicazioni critiche in configurazioni complesse e ad alta affidabilità. Il PkBox Advanced consente la facile integrazione con applicazioni che prevedono elevati volumi di firma, garantendo alte prestazioni grazie al meccanismo del bilanciamento del carico.

PkBox Enterprise

Massima scalabilità ed affidabilità

E' il prodotto top della gamma che Intesi propone in tutte le situazioni in cui sia richiesta un'elevata scalabilità sia funzionale che architetture, per affrontare le problematiche di Firma Digitale Massiva a norma di legge, in ambienti complessi e distribuiti geograficamente.



Leader nella **Firma Digitale**

www.pksuite.it

Leader nella **Tecnologia**

PkNet – Firma Qualificata con Smartcard

PkNet è una libreria software in grado di gestire operazioni di firma digitale, crittografia e autenticazione nelle applicazioni che interagiscono direttamente con l'utente (interfacce Web e moduli Client).

PkNet permette di utilizzare in modo trasparente diversi supporti fisici quali Smartcard e token USB, i certificati emessi dalle più importanti CA italiane e i certificati software senza supporto hardware anche self-signed.

Il software PkNet è in grado di identificare automaticamente la Smartcard dell'utente e di riconfigurarsi per operare con le Smartcard di tutte le principali CA (Actalis, Infocamere e PosteCom) e con le carte servizi distribuite ai cittadini italiani (Carta Nazionale dei Servizi, Carte Regionali dei Servizi, Carte di Identità Elettronica); PkNet non richiede quindi allo sviluppatore di definire quali Smartcard saranno effettivamente usate dall'utente.

PkNet è disponibile per ambienti di sviluppo Microsoft Com/.Net e per ambienti Java. Con PkNet viene fornita una applicazione completa di sicurezza e di gestione dei certificati che permette di eseguire immediatamente le operazioni di firma e di crittografia su file.

PkNet è disponibile nelle diverse versioni:

PkNet Express

Versione Gratuita disponibile on-line

E' la versione gratuita con cui risolvere tutte le problematiche di sicurezza logica dell'utente aziendale (firma di contratti, autenticazione, protezione di file).

Il prodotto PkNet Express è scaricabile direttamente dal sito www.pksuite.it.

PkNet

La versione più potente

E' la versione più potente che include anche funzionalità, altrimenti opzionali, quali l'output M7M per l'interoperabilità completa con Infocamere per le Marche Temporali e la gestione della Firma XML.



Leader nella **Firma Digitale**

www.pksuite.it