



Leader nella **Firma Digitale**



PkBox®

Server di sicurezza per
la Firma Digitale massiva

Introduzione

PkBox è il server di sicurezza che permette di aggiungere con impegno minimale le funzionalità di firma digitale, di crittografia e di autenticazione a tutte le applicazioni aziendali che richiedono la sicurezza logica dei dati. Tali funzionalità, allo stato dell'arte della tecnologia, si completano con PkBox EMV e PkNet nella linea di prodotti Intesi PkSuite.

PkBox è composto da:

- un server applicativo per eseguire le operazioni di firma;
- uno o più dispositivi crittografici (token software, scheda di sicurezza, pool di smart card);
- le componenti client per gestire, tra le altre cose, la comunicazione con le applicazioni, la fault tolerance e il bilanciamento del carico.

PkBox può essere utilizzato attraverso molteplici interfacce/protocolli quali Soap/XML, http, Java, .Net/Com; inoltre le sue funzionalità sono indipendenti dalle piattaforme hardware e software che ospitano le diverse componenti della soluzione.

PkBox è in grado di interfacciarsi con:

- diversi dispositivi di sicurezza (tramite l'interfaccia standard Rsa Pkcs#11),
- i certificati emessi dalle più importanti Certification Authority nazionali ed estere,
- i certificati software senza supporto hardware, anche auto-firmati.

Per quanto riguarda la configurazione d'uso:

- uno stesso PkBox può supportare contemporaneamente connessioni con diversi server applicativi;
- più PkBox possono essere installati per ottenere capacità di tolleranza ai guasti e di bilanciamento del carico;
- più PkBox possono essere configurati in modalità multi-livello per distribuire le operazioni di base in funzione della dislocazione dei dati.

Versioni disponibili

La rinnovata linea di prodotto PkBox è disponibile sia in versioni per i sistemi operativi Windows che per diverse distribuzioni Linux:

- **PkBox Basic** - Server di sicurezza per la firma massiva
- **PkBox Advanced** - Elevate funzionalità di firma con supporto HSM
- **PkBox Enterprise** - Massima scalabilità ed affidabilità

Funzionalità offerte

Funzionalità	Basic	Advanced	Enterprise
Firma Digitale (Conforme alla normativa Italiana ed Europea)	SI	SI	SI
Firme Multiple (parallele e controfirme)	-	SI	SI
Firma Pkcs#7 / CADES	SI	SI	SI
Firma PDF/PAdES	-	SI	SI
Firma XML-D SIG/XAdES	-	-	SI
Firma Massive	SI	SI	SI
Gestione e Firma impronta	-	SI	SI
Gestione e Firma detached	-	SI	SI
Calcolo impronte documenti generici	SI	SI	SI
Calcolo impronte documenti PDF	-	SI	SI
Gestione documenti in streaming	-	SI	SI
Verifica multipla firme detached	-	Opz.	SI
Verifica multipla firme impronte	-	Opz.	SI
Verifica firme impronte	-	SI	SI
Verifica dello stato del Certificato (con API separata da quella di Verifica Firma)	-	SI	SI
Gestione CRL cache	-	SI	-
Gestione avanzata CRL cache	-	-	SI
Time Stamp (RFC3161)	SI	SI	SI
Time Stamp (formato input M7M)	-	SI	SI
Detached Time stamp	-	SI	SI
Interoperabilità CA	SI	SI	SI
Cifratura/Decifratura RSA (formato CMS)	-	SI	SI
Cifratura/Decifratura RSA (formato PGP)	-	-	SI

Server di sicurezza per la Firma Digitale massiva

Funzionalità	Basic	Advanced	Enterprise
Cifratura/Decifratura chiavi simmetriche	-	-	Opz.*
Autenticazione con Firma Digitale	-	SI	SI
Autenticazione OTP	-	-	Opz.
Supporto interfaccia JCE	-	-	SI
Supporto interfaccia Pkcs#11	-	-	SI
Supporto protocollo ASSP	-	-	Presto disponibile
Possibilità architetture Three Tier	-	-	SI
Uso di certificati autofirmati	SI	SI	SI
Generazione richieste certificato	SI	SI	SI
Caricamento certificati su dispositivo di firma	SI	SI	SI
Load balancing	-	SI	SI
Backup/Restore chiavi private *	SI	SI	SI
Interfaccia di programmazione	.NET COM Java WS	.NET COM Java WS	.NET COM Java WS
Sistema operativo Windows *	SI	SI	SI
Sistema operativo Linux (Centos ver.4.4 - Red Hat Enterprise ver.4.4)	-	SI	SI
Documentazione utente	SI	SI	SI
Documentazione API per lo sviluppo	SI	SI	SI
Supporto Tecnico	SI	SI	SI
Supporto "Full Service"	-	Opz.	Opz.
Personalizzazioni	-	Opz.	Opz.
Credential On Database	-	Opz.	Opz.
Secure PIN (Gestione PIN cifrato)	-	-	SI
Encrypted Password (Gestione parametri di configurazione cifrati)	-	-	SI
Firma Remota	-	-	SI
Counting chiavi (Conteggio firme decifratura chiavi private)	-	-	SI

* Non disponibile su configurazione COD (Credential On Database)