PkSuite®

Digital Signature Leader

PkBox®

Massive Signature with HSM setting

INTESI GROUP
www.intesigroup.com

Introduction

PkBox is the security server which allows adding quite easily functionalities of digital signature, cryptography and authentication to servers handling data and processes for enterprise applications.

PkBox is composed by:

- an application server to support signature operation;
- one or more cryptographic devices (token software, security cards, set of smart cards);
- digital certificates, issued by a Certification Authority (qualified or test), or user generated.

PkBox can be used via several interfaces/protocols (e.g. Soap/Xml, http, Java, .Net/Com); it is also platform-independent and can be configured according to diversified hardware/software cryptographic devices.

PkBox has effective interface to:

- several security devices (via standard interface Rsa Pkcs#11),
- certificates issued by all the most relevant Certification Authorities,
- software certificates without hardware support, also auto-signed.

Regarding to the user's configuration, one PkBox can support at the same time connections to more application servers; however more PkBoxes can be installed to improving fault tolerance and load balancing.

More PkBoxes can be configured in multi-level mode to distribute the basic operations according to the data allocation.

PkBox ®

Massive Signature with HSM setting

Available Versions

PkBox is currently available in several versions both for Windows and for the most popular Linux implementations:

PkSdk - *Free Libraries for PkBox programming*

PkBox Basic - *Massive signature with HSM setting*

PkBox Advanced - *Massive signature by law*

PkBox Enterprise - *Maximal scalability and functionality*

Funzionalità	BASIC	ADVANCED	ENTERPRISE
Digital Signature (Compliance to Italian and EU laws)	YES	YES	YES
Multiple Signature (parallel & counterYESgned)	-	YES	YES
Pkcs#7 / CAdES Signature	YES	YES	YES
PDF/PAdES Signature	-	YES	YES
XMLDYESG/XAdES Signature	-	-	YES
MasYESve Signature	YES	YES	YES
Digest Signature	-	YES	YES
Detached Signature	-	YES	YES
Computed digest generic documents	YES	YES	YES
Computed digest PDF documents (PDF Signature)	-	YES	YES
Handling streaming documents	-	YES	YES
Multi Verification detached Signatures	-	OPT.	YES
Multi Verification digest Signature	-	OPT.	YES
Verification digest Signature	-	YES	YES
Certificate status verification (Separate API from the Signature Verification one)	-	YES	YES
CRL cache handling	-	YES	-
Advanced CRL cache handling	-	-	YES
Time Stamp (RFC3161)	YES	YES	YES
Time Stamp (M7M input format)	-	YES	YES
Detached Timestamp	-	YES	YES

PkBox®

Massive Signature with HSM setting

Funzionalità	BASIC	ADVANCED	ENTERPRISE
CA Interoperability	YES	YES	YES
RSA Encryption/decrypt ion (CMS format)	-	YES	YES
RSA Encryption/decrypt ion (PGP format)	-	YES	YES
Symmetric keys Encryption/decryption	-	-	Opt.*
Digital Signature authentication	-	YES	YES
OTP authentication	-	-	Opt.
JCE interface	-	-	YES
Pkcs#11 interface	-	-	YES
ASSP protocol	-	-	Presto disponibile
Three Tier architectures	-	-	YES
Use of self-signed certificate	YES	YES	YES
Certificate request generation	YES	YES	YES
Security device certificate loading	YES	YES	YES
Load balancing	-	YES	YES
Backup/Restore keys*	YES	YES	YES
Programming interface	.NET COM Java WS	.NET COM Java WS	.NET COM Java WS
Windows operating system*	YES	YES	YES
Linux operating system (Centos ver.4.4 - Red Hat Enterprise ver.4.4)	-	YES	YES
User documentation	YES	YES	YES
Development documentation	YES	YES	YES
Technical support	YES	YES	YES
"Full Service" support	-	Opt.	Opt.
Customization	-	Opt.	Opt.
Credential On Database	-	Opt.	Opt.
Secure PIN (Manage ciphered PIN)	-	-	YES
Encrypted Password (Manage configuration ciphered parameters)	-	-	YES
Remote Sign	-	-	YES
Key usage counting (Counting keys deciphered private keys)	-	-	YES

* Non disponibile su configurazione COD (Credential On Database)