PkSuite®

Digital Signature Leader

PkNet®

Qualified Signature with Smartcard

INTESI GROUP
www.intesigroup.com

PkNet®

Qualified Signature with Smartcard

Introduction

PkNet is an effective toolkit offering the capability to integrate functionalities of digital signature, cryptography and authentication within the user applications.

PkNet provides for a simple and intuitive interface. Each functionality is invoked by the application via a single call to the PkNet functions. Therefore the use of the product is easy and immediate also for the less expert developers in digital security.

A typical PkNet based solution is composed of:

- PkNet software components in charge for the signature operation,
- A security device, for protecting the private keys, such as a smartcard or a token USB (Table 1- list all the devices supported in Italy),
- Digital certificates, issued by Certification Authorities (qualified or test), or user-generated.

PkNet is able to recognize and use in a transparent and automatic way:

- the several security devices supported (smartcard and token USB),
- the certificates issued by the most relevant Certification Authorities (e.g. Actalis, Infocamere and Postecom in Italy, the equivalent ones in Belgium but also in other countries via specific localization),
- software certificates without hardware support, also auto-signed with own private key.

Available Versions

PkNet is currently available in 2 versions:

PkNet Express: *Free on-line version*

PkNet: *The rich set of useful functionalities*

In Table 2 the functional details of each version are shown.

PkNet®

Qualified Signature with Smartcard

Functionalities

- Digital signature (single, multiple or counter-signed) with/without time stamping. Signature generation and verification in format pkcs#7 or PDF
- Compliance to the Italian law related to digital signature and to electronic document (DPR 445/00, DPCM 8/2/99, AIPA 42/2001), (DPCM 13.1.2004, CNIPA 4/2005) and to the EU Directive 1999/93/CE (Art. 5.1 advanced signature based on qualified certificate issued by a certified body). Compliance can be provided to other countries' legislations via specific development
- Interoperability with different Certification Authorities
- Automatic "runtime" recognition of the signature device used
- Verification of signatures, certificates and time stamps
- Cryptography and de-cryptography
- Management of certified archives (user or Certification Authority owned)
- Generation of certification requests (Pkcs#10)
- Importing certificates into the signature device
- Generation of auto-signed certificates
- Integration within applications through programming interfaces (Microsoft Com, Java API, Applet)

Main hardware devices supported

For further information please refer to techinical specification

SMARTCARD	Siemens
	Oberthur
	Gemplus
	Bio AuthentIC
	Athena
	CRS/CNS (Services Regional/National Card)
Token USB	Eutron CryptoIdentity
	eToken Aladdin/SafeNet
	Aruba KEY
	InfoCert Business Key
	Actalis ONE
	Vasco DIGIPASS
	KOBIL mIDentity

PkNet®

Qualified Signature with Smartcard

Functionalities	EXPRESS COM	PKNET COM/JAVA
Remote device management (Remote Sign with PkBox)	-	YES/YES
Hardware device management (Smartcard / Token)	YES	YES/YES
Software device management	-	YES/YES
Multiple Signature (parallel and counter-signature)	-	YES/YES
Pkcs#7 / CAdES Signature	YES	YES/YES
PDF / PAdES Signature	-	YES/YES
XML-DSIG/XAdES Signature	-	-/YES
Signature of documents' basket	-	YES/YES
Digest Signature	-	-/YES
Detached Signature	-	YES/YES
Handling Streaming documents	-	-/YES
Certificate Status Verification	-	-/YES
Time Stamp (RFC3161)	YES	YES/YES
Time Stamp (M7M input format)	-	YES/YES
Time Stamp (Poste.comt)	-	-/-
Detached Time Stamp	-	YES/YES
Security device automatic recognition	YES	YES/YES
Handling of credentials filters	-	-/YES
CAs Interoperability	YES	YES/YES
RSA Encryption / Decryption	-	YES/YES
Digital signature athentication	-	YES/YES
Use of self-signed certificate	-	YES/-
Generation certificate requests	-	YES/-
Load balancing	-	YES/-
Backup / Restore keys	-	YES/-
OpenVPN integration	-	YES/-
Terminal server mode	-	YES/-
Windows operating system	YES	YES/YES
Linux operating system	-	-/YES
Macintosh operating system	-	-/ Opt.
Logo personalization	-	Opt./ Opt.
User & Developer documentation	YES	YES/YES
Technical support	-	Opt./ Opt.
"Full Service" support	-	Opt./ Opt.