



Digital Signature Leader



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 Version*
- **PkNet:** *The rich set of useful functionalities*

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

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).

hardware devices supported

Device	Manufacturer	Model
Smartcard	Siemens	CardOS M4.01
	Siemens	CardOS M4.01°
	Oberthur	AuthentiC v 203
	Oberthur	Bio AuthentiIC
	Oberthur	Id One
	Gemplus	CardOS M4
	Gemplus	GemGATE - 32k
	Gemplus	GPK16000
	Gemplus	GPK8000
	Incard	CNS
Incard	Sysgillo	
Token USB	Eutron	1024
	Eutron	2048
	Eutron	ITSEC
	Eutron	ITSEC-P
	Alladin	eToken Pro 16 e 32k

Functionalities offered	Express Com	PkNet Com/Java
Hardware device management (Smartcard / Token)	Yes	Yes / Yes
Software device management	-	Yes / Yes
Remote device management (Remote Sign with PkBox)	-	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
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 authentication	-	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.