



LP7Creator 2.0
Technical data sheet

Technical characteristics	
Certificate format	X509V3
Personal signature storage	PKCS#11 (IAIK provider), PKCS#12
File format	XAdES (ETSI TS 101 903) ou CAdES (ETSI TS 101 733)
Time stamping	RFC 3161, HTTP, HTTPS, socket
Development language	JDK 1.4
Cryptographic library	Open source : Bouncy Castle
Personal signature creation	RSA et DSA (512, 1024, 2048)
Java Virtual Machine	JVM 1.4, 1.5, 1.6 - 50MB minimum memory
Operating system	Windows 98, 2000, XP, 2003, Vista, Linux, Mac OS X

Functionality	
Appellation signature	Creation of a digital original (consent on the creation of the digital evidence).
Signature and cosignature(s)	Consent on the document's content.
Countersignature(s)	Consent on one of the document's signature(s).
Time stamp token	Time stamp token integrated to a document's signature: guarantees the anteriority of the signature with respect to the token's date and time.
Transactional token	Transactional token integrated to a document's signature: validates the signature by a third party present or a remote transaction server.
Personal signature creation	Key-pair creation with self-signed X509V3 certificate.
Import of personal signature	Import of .p12 file containing a key pair and its X509V3 certificate.
Personal signature declaration	Declaration of a personal signature on a PKCS#11 token or on a PKCS#12 file.
Import of certificates	Import of certificates in p7b, cer, der or pem format.
Certificate registration	Registration of a signature or countersignature affixed on an LP7 document.
Creation, deletion, modification of drawers	Management of certificates and personal signatures.
Association of a decorator to a certificate	Association of an image (jpeg, gif or png) and a border color with a certificate.
Export of signatures	For documents with XAdES signatures: possibility to export an individual signature as a XAdES enveloped signature.
Display of signatures	Detailed or summary display of signatures affixed on an LP7 document.
Extraction of content	Extraction of a document's original content into a file.
Content viewing	Viewing of the original content by the application referenced by the original content file's extension.
Signed attributes/properties	Signature production place; signature policy; commitment indication (approval, origin, delivery, receipt, sent); signing time; MIME type; encoding; signed content's filename.
Certificate revocation list	Automatic verification of certificate revocation status via download of certificate revocation lists when available (support HTTP ou LDAP).
Verification and controls	Automatic verification: document integrity, signatures, countersignatures, certificate chains, timestamp and transactional tokens, date coherency (signing time, timestamp, certificate validity and certificate revocation date)
Microsoft Windows integration	Default messaging client support for sending the digital evidence to its recipient(s) (via MAPI interface).