edu.Library

Feature Comparison for GUI KeyStore Managers

January 27, 2014

Document version 1.0.1

EduLib S.R.L.

Legal Notice

Copyright

EduLib S.R.L.

Calea Bucuresti, Bl. 27B, Sc. 1, Ap. 2
Craiova, DOLJ, 200675, Romania
Phone: +40 351 420970
Fax: +40 351 420971
E-mail: office@edulib.ro

1. Feature Comparison for GUI KeyStore Managers

We have made a comparison of the features between CERTivity® KeyStores Manager and the most relevant similar products. Although this comparison was made by EduLib, the creator of CERTivity, we tried to be as objective and fair as possible.

If you have any comments or suggestions, do not hesitate to contact us at http://www.edulib.com/company/contact/.

Feature Name	**CERTivity 2.0**	**Keystore Explorer 5.0.1**	**Portecle 1.7**	**KeyTool IUI 2.4.1**
Released Date	2014-01-23	2013-11-24	2011-01-23	2008-10-18
Maintained	+	+	-	-
Platforms	On any Platform That Can Run Java	On any Platform That Can Run Java	On any Platform That Can Run Java	On any Platform That Can Run Java
Has bundled JRE	+	-	-	-
Has installer	+	+	-	-
KeyStore Management				
Supported Java KeyStore Types	JKS, JCEKS, PKCS12, BKS, BKS-V1, UBER	JKS, JCEKS, PKCS12, BKS, UBER	JKS, PKCS#12, JCEKS, JKS (case sensitive), BKS, UBER, GKR (but option is inactive)	JKS, JCEKS, PKCS#12, BKS, UBER
Create a New KeyStore	+	+	+	+
Open an Existent KeyStore	+	+	+	+
Open Windows Root CA KeyStore	+	-	-	-
Open Windows User KeyStore	+	-	-	-
Discover JREs CA TrustStores	+	-	-	-
Open JREs CA TrustStores	+	Only main JRE	Only main JRE	Only main JRE
Save a KeyStore	+	+	+	It's done automatically after some operations
Defining a Default KeyStore	(planned for future releases)	+	-	-
Convert KeyStore Type	+	+	+	-
Change KeyStore Password	+	+	+	+
Delete Entry	+	+	+	+
Change Entry Password	+	+	+	+
Change Entry Alias	+	+	+	+

Cut/Copy - Paste Single KeyStore Entry	+	+	Allows only cloning a certificate into the same KeyStore.	Allows only copying a certificate into the same KeyStore
Cut/Copy - Paste Multiple Entries	+	-	-	-
TrustStore Management				
Set/Remove CA Certs TrustStore at runtime without restarting the application	+	+	+	-
Set Multiple TrustStores for Trust Path Validation	+	-	-	-
Availability to use JRE CA Certs TrustStores (from discovered JREs) for Trust Path Validation	+	-	-	-
Availability to use Windows KeyStores (for Microsoft Windows Systems) for Trust Path Validation	+	(only Windows Root CA)	-	-
Availability to use Custom KeyStores for Trust Path Validation	+	(only if the CA Certs is changed to a custom one)	(only if the CA Certs is changed to a custom one)	-
Availability to use current opened (and selected) KeyStore for Trust Path Validation	+	-	-	-
Display Trust Status for Certificate Entries in KeyStores	+	-	-	-
Display Trust Status for Opened Certificates	+	-	-	-
Customizable Trust Path Validation Options Without Restarting the Application	+	-	-	-
Available Trust Path Validation Options	Inhibit any policy, Explicit policy required, Inhibit policy mapping, Use revocation checking, Use policy qualifier processing,	-	-	-

	Use path length constraint (with customizable path length size), Use custom validation date, Provider selection (default provider or Bouncy Castle provider)			
Interface Usability				
MDI Interface for KeyStores	+	+	-	-
MDI Interface for Certificates/CRL/ CSR	+	-	-	-
KeyStore Representation	Tree List (Entries are displayed as a list of expandable nodes) Available SubItems for KeyPairs : Private/Public Keys, Certificate Chains, Certificates, Extensions Available Subitems for Certificates: Public Key, Extensions	Simple List (entries are not expandable)	Simple List (entries are not expandable)	Simple List (entries are not expandable)
Available Entries Direct Information	Algorithm and Size, Expiry Date, Last Modified, Validity Status, Trust Status	Algorithm and Size, Expiry Date, Last Modified, Validity Status	Alias Name, Last Modified	For Key Pairs and Certificates: Alias, Entry Type, Valid Date, Self-Signed, Trusted C. A., Key Size, Cert. Type, Cert. Sig. Algorithm, Modified Date For Secret Keys: Alias, Entry, Modified Date
Mark Locked Keys	+	+	-	-
Mark Expired Key Pairs/Certificates	+	+	-	+
Mark Certificate Trust Status	+	-	-	+
Mark Key Pairs with Key sizes smaller than a configurable value	+	-	-	-
Undo/Redo for KeyStore Operations and Imports	+	+	-	-
Prompting to re-enter password in case of wrong password for	+	-	-	-

unlocking Private/ Secret Keys				
Prompting to re-enter password in case of wrong password when converting a KeyStore to a different type (operation does not fail)	+	-	-	-
Informing when a Key Store which contains Secret Keys can not be converted to a Key Store type that does not support Secret Keys before entering all the passwords	+	-	Converts with removing secret keys (it gives a slight warning first)	-
Prompting for passwords when converting from a KeyStore type which does not support passwords to a KeyStore type which supports entry passwords	+	-	-	-
Displaying Entry Information Mode	Bottom Panel (And few details in the KeyStore View)	New Dialog (And few details in the KeyStore View)	New Dialog (and few details in the KeyStore View)	New Dialog (text based content)
Allows rearranging Key Store/Certificate tabs	+	-	-	-
Configurable Arrangement and Positioning of Tabs	+	-	-	-
Configurable Tabs Position by Dragging	+	-	-	-
Window Configuration Options	Maximize, Float, Float Group, Minimize, Minimize Group, Dock, Dock Group, New Document Tab Group, Collapse Document Tab Group	-	-	-
Multiple KeyStore Entries Selection	+	-	-	-
Multiple KeyStore Entries Copy - Paste between KeyStores	+	-	-	-

Copy a Certificate From a Certificate Chain and Paste It Into Another KeyStore	+	-	-	-
Configurable Key Shortcuts (Keymap)	+	-	-	-
Displaying Providers List	(planned for future releases)	+	+	-
"Close All Documents" Option	+	+	-	-
Opened Tabs Manager	+	-	-	-
Opened Tabs Manager Options	Switch to Document, Close Document(s)	-	-	-
Easy Tab Selector Drop list	+	-	-	-
Available Actions/ Options Tree Like Structure	(planned for future releases)	-	-	+
Quick Search (with text box)	+	-	-	-
Change Look And Feel	(planned for future releases)	+	+	-
Password Strength Indicator	(planned for future releases)	+	-	-
Show tips at startup	(planned for future releases)	+	-	-
Key Pair Operations				
Generate Key Pair (RSA/DSA)	+	+	+	+
Regenerate Key Pair	+	-	-	-
Sign With Selected KeyPair at Generation Time	+	-	-	-
Key Pair Generation - Signature Algorithms (for DSA Keys)	SHA1 With DSA, SHA224 With DSA, SHA 256 With DSA, SHA 384 With DSA, SHA 512 With DSA	SHA.1 with DSA, SHA-224 with DSA, SHA-256 With DSA, SHA-384 with DSA, SHA-512 with DSA	SHA1withDSA, SHA224withDSA, SHA256withDSA	SHA1withDSA
Key Pair Generation - Signature Algorithms (for RSA Keys)	MD2 with RSA, MD5 with RSA, SHA1 with RSA, SHA1 With RSA and MGF1, SHA224 With RSA, SHA224 With RSA and MGF1, SHA256 With RSA, SHA256 With	MD2 with RSA, MD5 with RSA, RIPEMD-128 with RSA, RIPEMD-160 with RSA, RIPEMD-256 with RSA, SHA.1 with RSA, SHA-224 with RSA, SHA-256	MD2withRSA, MD5withRSA, SHA1withRSA, SHA224withRSA, SHA256withRSA, SHA384withRSA, SHA512withRSA, RIPEMD128withRSA,	MD5withRSA, SHA256withRSA, SHA384withRSA, SHA512withRSA, RIPEMD128withRSA, RIPEMD160withRSA, RIPEMD256withRSA

	RSA and MGF1, SHA384 With RSA, SHA384 With RSA and MGF1, SHA512 With RSA, SHA512 With RSA and MGF1, RIPEMD128 With RSA, RIPEMD160 With RSA, RIPEMD256 With RSA	With RSA, SHA-384 with RSA, SHA-512 with RSA	RIPEMD160withRSA, RIPEMD256withRSA	
Generate Key Pair (EC)	+	-	-	+
Key Pair Generation - EC Algorithms	EC(ECDSA), ECGOST3410	-	-	EC(ECDSA)
Key Pair Generation - EC Parameters Specification (for ECDSA Algorithm)	c2pnb272w1, c2tnb191v3, c2pnb208w1, c2tnb191v2, c2tnb191v1, c2tnb359v1, prime192v1, prime192v2, prime192v3, c2tnb239v3, c2pnb163v3, c2tnb239v2, c2pnb163v2, c2tnb239v1,, c2pnb163v1, c2pnb176w1, prime256v1, c2pnb304w1, c2pnb368w1, c2tnb431r1, prime239v3, prime239v2, prime239v1, sect233r1, secp112r2, secp112r1, secp256k1, sect113r2, secp521r1, sect113r1, sect409r1, secp192r1, sect193r2, sect131r2, sect193r1, sect131r1, secp160k1, sect571r1, sect283k1, secp384r1, sect163k1,	-	-	prime192v1, prime239v1, prime256v1

	secp256r1, secp128r2, secp128r1, secp224k1, sect233k1, secp160r2, secp160r1, sect409k1, sect283r1, sect163r2, sect163r1, secp192k1, secp224r1, sect239k1, sect571k1, B-163, P-521, P-256, B-233, P-224, B-409, P-384, B-283, B-571, P-192, brainpoolp512r1, brainpoolp384t1, brainpoolp256r1, brainpoolp192r1, brainpoolp512t1, brainpoolp256t1, brainpoolp224r1, brainpoolp320r1, brainpoolp192t1, brainpoolp160r1, brainpoolp224t1, brainpoolp384r1, brainpoolp320t1, brainpoolp160t1			
Key Pair Generation - EC Parameters Specification (for ECGOST3410 Algorithm)	GostR3410-2001-CryptoPro-A, GostR3410-2001-CryptoPro-XchB, GostR3410-2001-CryptoPro-XchA, GostR3410-2001-CryptoPro-C, GostR3410-2001-CryptoPro-B	-	-	-
Key Pair Generation - Signature Algorithms (for ECDSA EC Keys)	SHA1withECDSA, SHA224withECDSA, SHA256withECDSA, SHA384withECDSA, SHA512withECDSA	-	-	SHA1withECDSA,, SHA224withECDSA, SHA256withECDSA, SHA384withECDSA, SHA512withECDSA
Key Pair Generation - Signature Algorithms (for ECGOST3410 EC Keys)	GOST3411 with ECGOST3410	-	-	-
Key Pair Generation CERT X.500 DN Fields	Common Name (CN), Organization Unit (OU), Organization (O),	Common Name (CN), Organization Unit (OU), Organization (O),	Common Name (CN), Organization Unit (OU), Organization (O),	Common Name (CN), Organization Unit (OU), Organization (O),

	Locality (L), State (ST), Country (C), Email (E)	Locality (L), State (ST), Country (C), Email (E)	Locality (L), State (ST), Country (C), Email (E)	Locality (L), State (ST), Country (C), Email (E)
Standardized DN Country Codes (2 letter code) support	+	-	-	+
Key Pair Generation CERT X.500 DN Fields (extended)	(planned for future releases)	-	-	Title, Device serial number name, Business category, DN qualifier, Pseudonym, 1-letter gender, Name at birth, Date of birth, Place of birth, Street, Postal code, Postal address, 2-letter country of residence, 2-letter country of citizenship
Key Pair Generation CERT X.520 Name	(planned for future releases)	-	-	Surname, Given name, Initials, Generation, Unique Identifier
Import Key Pair into KeyStore (from PKCS#12 Files)	+	+	+	-
Import Key Pair into KeyStore (from PKCS#8 private key and Certificate)	+	+	-	-
Import Key Pair into KeyStore from OpenSSL private key and certificate)	+	+	-	-
Import Key Pair into KeyStore (from PVK private key and Certificate)	(planned for future releases)	+	-	-
Import Key Pair into KeyStore (from PEM private key and Certificate Chain)	+	+	-	+
Import Key Pair into KeyStore (from other KeyStore)	(planned for future releases)	-	-	+
Import Key Pair into KeyStore from a Private Key and More Certificate Files (which can create a chain)	+	-	-	-
Export Key Pair (PKCS#12)	+	+	+	-

Export Key Pair (PEM Encoded)	(planned for future releases)	-	+	-
Extend Validity of Self-Signed KeyPairs	+	-	-	-
Enter New Serial Number When Extending Validity of Self-Signed Certificates	+	-	-	-
Certificates Operations				
Open a standalone certificate/Examine standalone certificate	+	+	+	-
Open a Certificate Chain/Examine Certificate Chain	+	+	+	-
View Certificate Details	+	+	+	+
View Certificate Details From Signature	+	-	-	(only Certificate Type and Subject DN, for each signed entry, for JAR files)
Available Certificate Details	Format, Version, Serial Number, Valid From/To, Public Key, Extensions, Signature Algorithm, Multiple Fingerprints, Subject/Issuer Information (CN, OU, O, L, ST, C, E), PEM, ASN.1	Version, Serial Number, Valid From/Until, Public Key, Signature Algorithm, Multiple Fingerprints, Subject/Issuer Information (CN, OU, O, L, ST, C, E), Extensions, PEM, ASN.1	Chain position and total number of certificates in the chain, Version, Serial Number, Valid From/ Until, Public Key, Signature Algorithm, Fingerprints, Subject/Issuer DN String, Extensions, PEM Encoding	Owner (Subject DN String), Issuer (Issuer DN String), Version, Serial Number, Valid From/Until, Signature Algorithm, Fingerprints, Extensions
Available Fingerprints	MD2, MD4, MD5, SHA1, RIPEMD-128, RIPEMD-160, RIPEMD-256, SHA-224, SHA-256, SHA-384, SHA-512	MD2, MD4, MD5, RIPEMD-128, RIPEMD-160, RIPEMD-256, SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	SHA1, MD5	MD5, SHA.1
View PEM Representation for a Certificate	+	+	+	-
View ASN.1 for a Certificate	+	+	-	-
Import Certificate from files into KeyStore	+	+	+	+
Import Root CA Certificate (directly	(planned for future releases)	-	-	+

into the Root CA certs KeyStore)				
Import Certificate into a KeyStore directly from Certificate Details Dialog	(planned for future releases)	+	-	-
Import Certificate into KeyStore with trust path validation	+	+	+	(manual validation)
Import Certificate from Server into KeyStore	+	+	-	-
Import Certificate from Signature into KeyStore	+	-	-	-
Export Certificate	+	+	+	+
Export Certificate From Signature to file (JAR, APK, PDF, XML)	+	-	-	-
Export Certificate Supported Formats	X.509, X.509 PEM Encoded, PKCS#7, PKCS#7 PEM Encoded, PKI Path	X.509, X.509 PEM Encoded, PKCS#7, PKCS#7 PEM Encoded, PKI Path, SPC	DER Encoded, PEM Encoded, PKCS#7, PkiPath	DER, PKCS#7, PEM
Export Certificate Chain	+	+	+	(only when exporting with private key also)
Export Certificate Chain Supported Formats	PKCS#7, PKCS#7 PEM Encoded, PKI Path	PKCS#7, PKCS#7 PEM Encoded, PKI Path	PKCS#7, PkiPath	DER, PEM
Obtain the Revocation Status	+	-	-	-
Retrieve Certificate From SSL Server	TLSv1, TLS v1.1, TLS v1.2 and default algorithm	TLSv1, TLS v1.1, TLS v1.2	TLSv1 (SSLv 3.1)	-
Retrieve Certificate From SSL Server (additional connection info)	(planned for future releases)	-	Connection Protocol, Connection Cipher Suite	-
Retrieve Certificate From SSL Server using HTTPS URL (not host and port specifically)	+	-	-	-
Test Certificates on Given Protocol	+	-	-	-
View Associated CRL	+	-	+	-
Append signer certificate to key pair certificate chains	+	+	-	-

Remove signer certificate from key pair certificate chains	+	+	-	-
Rename Certificate	+	+	+	+
Delete Certificate	+	+	+	+
Renewal of Certificate	Only when the certificate is within a Key Pair	-	-	-
Certificate Extensions				
View Certificate Extensions	+	+	+	+
View ASN.1 for a Certificate Extension	+	+	-	-
Add Certificate Extensions when generating a new KeyPair	+	+	-	-
Add Certificate Extensions to CA Replies	+	+	-	-
Save Certificate Extensions Template	+	+	-	-
Save Certificate Extensions Template as XML	+	-	-	-
Available Certificate Extensions	Authority Information Access, Authority Key Identifier, Basic Constraints, Certificate Policies, CRL Distribution Points, Extended Key Usage, Freshest CRL, Inhibit Any Policy, Issuer Alternative Name, Key Usage, Name Constraints, Netscape Cert Type, Private Key Usage Period, Policy Constraints, Policy Mappings, Subject Alternative Name, Subject Information Access, Subject Directory Attributes, Subject Key Identifier.	Authority Information Access, Authority Key Identifier, Basic Constraints, Certificate Policies, Extended Key Usage, Inhibit Any Policy, Issuer Alternate Name, Key Usage, Name Constraints, Netscape Base URL, Netscape CA Policy URL, Netscape CA Revocation CRL, Netscape Certificate Renewal URL, Netscape Certificate Type, Netscape Comment, Netscape Revocation URL, Netscape SSL Server Name, Policy Constraints, Policy Mappings, Private Key Usage Period, Subject Alternative	(many only for display, but not specified anywhere)	(many for display) For Key Pair Creation: Key Usage, Extended Key Usage

		Name, Subject Information Access, Subject Key Identifier		
Extensions display at creation time (GUI Point of view)	Tree - like Structure where all extensions, properties and sub-items are visible in a single dialog	List of extensions, each one opening in a different dialog for setting properties, and each sub-item opens also in a different dialog	-	-
Certificate Authority Functions				
Check PKI file type	+	+	-	-
Certificate Signing made easier using “Select as CA Issuer” and “Sign Certificate by <aliasForIssuer>” actions	+	-	-	-
Certificate chain management: append and remove signer certificate (with Copy/Paste/ Delete/Undo/ Redo functionality included)	+	(supported only from menu without Copy/Paste)	-	-
Generate Certificate Signing Request (CSR) files	+	+	-	-
Sign Certificate Signing Request (CSR) files	+	+	-	-
Import CA Reply	+	+	-	-
Trust verification when Importing CA Reply	+	+	+	-
Trust verification when Importing CA Reply (with user confirmation when trust is not established)	+	+	+	-
Act as a testing purposes CA (by generating CSR files, signing CSRs and importing CA Replies	+	+	-	-
CSR				
View CSR Details/ Examine CSR	+	+	+	(only PEM display)

Available CSR Details	Format, Version, Public Key (with details available), Signature Algorithm, Subject (CN, OU, O, L, ST, C, E), Challenge, CSR Dump (PEM)	Format, Public Key (with details available), Signature Algorithm, Subject (CN, OU, O, L, ST, C, E), Challenge, CSR Dump (PEM, ASN.1)	Version, Subject DN String, Public Key (Algorithm and size), Signature Algorithm, PEM	PEM
Generate CSR Files	+	+	+	+
Generate CSR Files Supported Formats	PKCS#10, SPKAC	PKCS#10, SPKAC	PKCS#10 (probably)	PKCS#10
CRL				
View CRL Details/ Examine CRL	+	+	+	-
View Remote CRLs	+	-	-	-
Protocols Supported for Opening Remote CRLs	HTTP, HTTPS, FTP, LDAP	-	-	-
Available CRL Details	Type, Version, This Update, Next Update, Signature Algorithm, Issuer (CN, OU, O, L, ST, C, E), Extensions, ASN.1, Revoked Certificates (+Extensions)	Version, Issuer (CN, OU, O, L, ST, C, E), Effective Date, Next Update, Signature Algorithm, Extensions, ASN.1, Revoked Certificates (+Extensions)	Version, Issuer DN String, Effective Date, Next Update, Signature Algorithm, Extensions, Revoked Certificates (+Extensions)	-
View CRL Extensions	+	+	+	-
Next Update Exeeded Verification	+	+	+	-
CA Reply				
Import CA Reply With Trust Path Validation	+	+	+	-
View CA Reply Details	(Only if opened as a certificate and browse through the chain)	(Only if opened as a certificate, and browse through the chain)	(Only if opened as a certificate, and you can browse through the chain)	-
Create CA Reply	+	+	-	-
Secret Key Operations				
Available Secret Keys Information	Algorithm, Last Modified	Algorithm, Key Size, Last Modified	Last Modified	Modified date
View Secret Key Details	(planned for future releases)	+	-	Algorithm, Format, Size, Value in hexa
Generate Secret Key	+	+	-	+
Secret Key Supported Algorithms	AES, AESWrap, ARCFOUR, BlowFish, Camellia,	AES, ARC4, Blowfish, Camellia, CAST-128,	-	AES, ARCFOUR, Blowfish, DES, DESede, HmacMD5,

	Cast5, Cast6, DES, DESede, DESedeWrap, GOST28147, Grainv1, Grain128, HC128, HC256, Noekeon, RC2, RC4, RC5, RC5-64, RC6, Rijndael, Salsa20, Seed, Serpent, Skipjack, TEA, Twofish, VMPC, VMPC-KSA3, XTEA, HmacMD2, HmacMD4, HmacMD5, HmacRIPEMD128, HmacRIPEMD160, HmacSHA1, HmacSHA224, HmacSHA256, HmacSHA384, HmacSHA512, HmacTIGER	CAST-256, DES, DESEDE, GOST 28147-89, Grain v1, Grain-128, HC-128, HC-256, HMac-MD2, HMac-MD4, HMac-MD5, HMac-RipeMD128, HMac-RipeMD160, HMac-SHA1, HMac-SHA224, HMac-SHA256, HMac-SHA384, HMac-SHA512, HMac-Tiger, NOKEON, RC2, RC5, RC6, Rijndael, Salsa20, Serpent, SEED, Skipjack, TEA, Twofish, XTEA		HmacSHA1, HmacSHA256, HmacSHA384, HmacSHA512, RC2
Provider Selection for Generation Available	+	-	-	-
Offers Supported Key Sizes for Each Algorithm	+	+	-	-
Import Secret Key From File	(planned for future releases)	-	-	+
Export Secret Key To File	(planned for future releases)	-	-	+
Export Secret Key To File Format	(planned for future releases)	-	-	DER, PEM
Private Key Operations				
View Private Key Details	+	+	-	+
Available Private Key Details (for DSA)	Algorithm, Key Size, Fields (Basic Generator G, Prime Modulus P, SubPrime Q, Private Key Value;), ASN.1	Algorithm, Key Size, Fields (Prime Modulus P, Prime Q, Generator G, Secret Exponent X), ASN.1	-	Key Size
Available Private Key Details (for RSA)	Algorithm, Key Size, Fields (Modulus, Private Exponent, Public Exponent, CRT Coefficient, Prime Exponent P, Prime Exponent Q,	Algorithm, Key Size, Format, Encoded, Fields (Public Exponent, Modulus, Prime P, Prime Q, Prime Exponent P, Prime Exponent Q, CRT	-	Key Size

	Prime Modulus P, Prime Q), ASN.1	Coefficient, Private Exponent), ASN.1		
Available Private Key Details (for ECDSA / ECGOST3410)	Algorithm, Key Size, Parameters Specification, Fields (Private Value S, Cofactor, First Coefficient A, Second Coefficient B, Field Size, Seed, Generator Affine X-Coordinate, Generator Affine Y-Coordinate, Generator Order), ASN.1	Algorithm, Key Size (for ECDSA only), Format, Encoded, ASN.1	-	Key Size (for ECDSA only)
Export Private Key	+	+	-	(but only together with certificate file)
Export Private Key Supported Formats	PKCS#8, PKCS#8 PEM Encoded, Open SSL PEM Encoded	PKCS#8, PKCS#8 PEM Encoded, PVK, OpenSSL PEM Encoded	-	DER, PEM
Export Private Key Encryption Algorithms (PKCS#8)	PBE_SHA1_2DES, PBE_SHA1_3DES, PBE_SHA1_RC2_40, PBE_SHA1_RC2_128, PBE_SHA1_RC4_40, PBE_SHA1_RC4_128	PBE with SHA.1 and 2 key DESede, PBE with SHA.1 and 3 key DESede, PBE with SHA.1 and 40 bit RC2, PBE with SHA.1 and 128 bit RC2, PBE with SHA.1 and 40 bit RC4, PBE with SHA.1 and 128 bit RC4	-	-
Export Private Key Encryption Algorithms (OpenSSL)	AES-128-CBC, AES-128-CFB, AES-128-ECB, AES-128-OFB, BF-CBC, BF-CFB, BF-ECB, BF-OFB, DES-CBC, DES-CFB, DES-ECB, DES-EDE-CBC, DES-EDE-CFB, DES-EDE-ECB, DES-EDE-OFB, DES-EDE, DES-EDE3-CBC, DES-EDE3-CFB, DES-EDE3-ECB, DES-EDE3-OFB, DES-EDE3, DES-OFB, RC2-40-CBC, RC2-64-CBC, RC2-	PBE with DES CBC, PBE with DESede CBC, PBE with 128 but AES CBC, PBE with 192 bit AES CBC, PBE with 256 bit AES CBC	-	-

	CBC, RC2-CFB, RC2-ECB, RC2-OFB			
Public Key Operations				
View Public Key Details	+	+	-	-
Available Public Key Details (for DSA Keys)	Algorithm, Key Size, Fields (Basic Generator G, Prime Modulus P, SubPrime Q, Public Key), ASN.1	Algorithm, Key Size, Format, Encoded, Fields (Prime Modulus P, Prime Q, Generator G, Public Key Y), ASN.1	-	-
Available Public Key Details (for RSA Keys)	Algorithm, Key Size, Fields (Modulus, Public Exponent), ASN.1	Algorithm, Key Size, Format, Encoded, Fields (Public Exponent, Modulus), ASN.1	-	-
Available Public Key Details (for ECDSA / ECGOST3410 Keys)	Algorithm, Key Size, Fields (Basic Generator G, Prime Modulus P, SubPrime Q, Public Key), ASN.1	Algorithm, Key Size, Format, Encoded, ASN.1	-	-
Export Public Key	+	+	-	-
Export Public Key Supported Formats	Open SSL, Open SSL PEM Encoded	Open SSL, Open SSL PEM Encoded	-	-
Sign and Verify				
Verify Signatures for JAR Files	+	-	-	+
Verify Signatures for APK Files	+	-	-	+
Verify Signatures for PDF Files	+	-	-	-
Verify Signatures for XML Files	+	-	-	+
Verify XML Signature - allow using external cert. validation	+	-	-	-
Verify XML Signature - set use external cert. validation and embedded cert. validation order	+	-	-	-
Verify XML Signature - allow selecting the external cert. from file or from a given KeyStore entry (from KeyStore file)	+	-	-	-
Sign JAR Files	+	+	-	+

JAR Signing - Signature Algorithms	SHA.1 with DSA, MD2 with RSA, MD5 with RSA, SHA.1 with RSA, SHA.1 with ECDSA	SHA.1 with DSA, MD2 with RSA, MD5 with RSA, SHA.1 with RSA	-	SHA.1 With DSA, SHA.1 With RSA
JAR Signing - Digest Algorithms	MD2, MD5, SHA.1, SHA224, SHA256, SHA384, SHA512	MD2, MD5, SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	-	SHA.1
JAR Signing - Add Full Manifest Digest Attribute Configurable	+	-	-	-
Sign APK Files	+	+	-	+
APK Signing - Signature Algorithms	SHA.1 with DSA, MD2 with RSA, MD5 with RSA, SHA.1 with RSA	SHA.1 with DSA, MD2 with RSA, MD5 with RSA, SHA.1 with RSA	-	-
APK Signing - Digest Algorithms	MD2, MD5, SHA.1, SHA224, SHA256, SHA384, SHA512	MD2, MD5, SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	-	-
APK Signing - Add Full Manifest Digest Attribute Configurable	+	-	-	-
Sign XML Files	+	-	-	+
XML Signing - Signature Types	Enveloped, Enveloping, Detached	-	-	Enveloped
XML Signing - Digest Algorithms	SHA1, SHA256, SHA512	-	-	-
XML Signing - Canonicalization Algorithms	Inclusive, Inclusive With Comments, Exclusive, Exclusive With Comments	-	-	-
XML Signing - Allow Attaching Key To Signature	+	-	-	-
XML Signing - Allow Attaching Certificate To Signature	+	-	-	-
Sign PDF Files	+	-	-	-
PDF Signing - Signature Subfilters	adbe.pkcs7.sha1, adbe.x509.rsa_sha1, adbe.pkcs7.detached	-	-	-
Sign CSR Files/ Create Certificate from CSR	+	+	-	-
Prevention for Signing CSR Files by the Same Key Pair That Created Them	+	-	-	-

CSR Signing - Signature Algorithms	SHA.1 with DSA, SHA224 with DSA, SHA256 with DSA, SHA384 with DSA, SHA512 with DSA, MD2 with RSA, MD5 with RSA, SHA.1 with RSA, SHA.1 with RSA and MGF1, SHA224 with RSA, SHA224 with RSA and MGF1, SHA256 with RSA, SHA 256 with RSA and MGF1, SHA384 with RSA, SHA 384 with RSA and MGF1, SHA512 with RSA, SHA512 with RSA and MGF1, RIPEMD128 with RSA, RIPEMD160 with RSA, RIPEMD256 with RSA	SHA.1 with DSA, SHA-224 with DSA, SHA-256 With DSA, SHA-384 with DSA, SHA-512 with DSA, MD2 with RSA, MD5 with RSA, RIPEMD-128 with RSA, RIPEMD-160 with RSA, RIPEMD-256 with RSA, SHA.1 with RSA, SHA-224 with RSA, SHA-256 With RSA, SHA-384 with RSA, SHA-512 with RSA	-	-
Sign J2ME MIDlet Applications Files	-	+	-	-
Verify Detached Signature - CMS	(planned for future releases)	-	-	+
Sign With Detached Signature - CMS	(planned for future releases)	-	-	+
Detached Signature - CMS Formats - CMS Signature File	(planned for future releases)	-	-	P7M, P7S
Detached Signature - CMS Formats - CMS Certs-only file	(planned for future releases)	-	-	P7C
Detached Signature - CMS Formats - digest algorithms	(planned for future releases)	-	-	SHA1, SHA224, SHA256, SHA384, SHA512, MD5, RIPEMD128, RIPEMD160, RIPEMD256
Verify Detached Signature - Other	(planned for future releases)	-	-	+
Sign Detached Signature - Other	(planned for future releases)	-	-	+
Detached Signature - Other Formats - Signature File	(planned for future releases)	-	-	DER, PKCS#7, PEM
Detached Signature - Other Formats - Certificate File	(planned for future releases)	-	-	DER, PKCS#7, PEM

Allow signing using any Key Pair irrespective of Certificate extension	+	+	-	-
Suggest candidate KeyPairs for signing (the ones that have the right extensions for their certificates)	(planned for future releases)	-	-	+
Encrypting Files				
Encrypt file using Secret Key	-	-	-	+
Encrypt file using RSA trusted certificate	-	-	-	+
Encrypt file using private key	-	-	-	+
RSA Encryption Algorithms	-	-	-	RSA/ECB/ PKCS1Padding, RSA/NONE/ PKCS1Padding, RSA/NONE/ OAEPWithSHA1 AndMGF1Padding
Other				
KeyStore Persistence between sessions	+	-	-	-
KeyStore Persistence type	Fully persist (name and passowrd), Only KeyStore names, No persistence	-	-	-
Open Files Using Drag & Drop	+	+	+	-
File Types Supported For Drag & Drop	KeyStore, Certificate, CSR, CRL irrespective of the file extension	KeyStore	Only based on extension: KeyStore, Certificate, CSR, CRL	-
Supported KeyStore file extensions	cacerts, ks, jks, jce, p12, pfx, bks, ubr, keystore	ks, keystore, jks, jceks, bks, uber, pfx, p12	ks, jks, jceks, p12, pfx, bks, cacerts	ubr, jks, ks, jce, bks, pfx, p12
Open Recent Files	+	+	(maximum 4 files)	-
Remember last file directory between sessions	+	+	-	-
Remember last file directory for each specific action (Opening a Key Store, a Certificate, etc.)	+	-	-	-

KeyStore Properties (Tree - like entries structure)/KeyStore Report	(planned for future releases)	+	+	-
KeyStore Properties - Export structure in text and XML formats)	(planned for future releases)	+	(copy in memory)	-
Set Password Quality	(planned for future releases)	+	-	-
Configure/Set Internet Proxy	(planned for future releases)	+	-	-
View Cryptography Strength/Policy Details	+	+	-	-
Detection of Cryptography Strength Policy Limitation when Launching the Application	(planned for future releases)	+	-	-
GUI Support for Upgrading Cryptography Strength	+	+	-	-
Support for Manual Upgrading Cryptography Strength in case automatic upgrade fails	+	+	-	-
Customizable Properties	Certificate expiry notification interval, RSA Key Pair minimum allowed size, RSA Key Pair maximum allowed size, RSA Key Pair default size, Autogenerated certificate serial number maximum bit length, Undo level, Log level, Memory usage maximum threshold level, Keystore persistence type, Recent file list maximum size, JRE CA KeyStore list max size, Certificates Retriever connection type, Inspected	Set CA Certificates Key Store, Minimum Password Quality, Look And Feel, Internet Proxy, Trust Checks	-	-

	and draggable file size limit			
Import/Export Configuration Properties	+	-	-	-
Add extension to file name on export, if the name does not contain an extension from the selected file filter	+	-	-	+
Password Manager (remember passwords after unlocking)	+	+	-	-
Archiving directories into JAR/APK files	(planned for future releases)	-	-	+
OS File Associations	(planned for future releases)	(only for KeyStores)	-	-