IAIK/Stiftung SIC

http://jce.iaik.tugraz.at

IAIK-CMS with S/MIMEv3

IAIK-CMS with S/MIMEv3 provides a complete implementation of the CMS (successor of PKCS#7), S/MIMEv3 and ESS (Enhanced Security Services for S/MIME) protocols. It can be used for signing, encrypting, digesting, authenticating any kind of digital data and enhances the JavaMail™ API with the cryptographic services of the S/MIME and ESS standards. It comes with a great variety of cryptographic algorithms, supports data compression according to S/MIMEv3.1, and allows easy integration of smartcards or other hardware security modules.

Main Benefits

- Usability: A detailed Javadoc documentation and large set of demo sources makes it easy to learn the API usage of IAIK-CMS. Many step-by-step explanations guide you through the process necessary for signing and/or encrypting digital documents or sending and receiving cryptographically protected electronic mails.
- Pipelined Architecture: The stream based CMS library supports one-pass processing for giving an optimized performance and handling large amounts of data without running into memory problems.
- Compatibility and Interoperability: IAIK-CMS is the CMS and S/MIMEv3 capable successor of the IAIK-JCE PKCS#7 and IAIK-SMIME libraries which are used in several real-world applications for many years. IAIK-CMS has been successfully tested with major CMS and S/MIME applications like OpenSSL, Microsoft Outlook or Mozilla Thunderbird. It is listed in the IETF CMS Draft Standard Implementation Report (http://www.ietf.org/iesg/implementation/report-rfc3852.txt). IAIK-CMS is backwards compatible to PKCS#7 and S/MIMEv2 and is interoperable with any PKCS#7v1.5, CMS and S/MIMEv2/v3 compliant application.
- Extensibility: The architecture of IAIK-CMS makes it easy to plug-in user-written code for extending the core functionality about application specific content types, security policies, or, for instance, additional cryptographic algorithm implementations or certificate and trust validation strategies.

Feature List

- Implemented entirely in the Java™ language guaranteeing cross platform portability

- Works on all JDK Versions 1.1, 1.2, 1.3, 1.4, 1.5, 1.6, 1.7 and compatible
- Special versions for use in applets and with Java™ WebStart
- Centralized security policy configuration
- Stream based CMS implementation for supporting one-pass processing making it possible to handle large amounts of data without running into memory problems
- Compatible with the javax.mail architecture from SUN
- Implements the IETF standardized CMS, S/MIMEv3 and ESS specifications
- Implements all CMS content types Data, Signed-data, Enveloped-data, Digested-data, Encrypted-data, Authenticated-Data, and Compressed-Data (RFC 3274), Authenticated-Enveloped-Data (RFC 5083)
- Implements all CMS RecipientInfo types: KeyTransRecipientInfo, KeyAgreeRecipientInfo, KEKRecipientInfo, PasswordRecipientInfo (RFC 3211), OtherRecipientInfo (user pluggable)
- Supports all algorithms required and recommended for the implemented content types: SHA-1 (and also SHA-224, SHA-256, SHA-384, SHA-512), MD5 (digest), RSA (signature, key transport), DSA (signature), X9.42 Ephemeral Static and Static Static Diffie Hellman - RFC 2631 (key agreement), AES Key Wrap, Triple-DES Key Wrap, RC2 Key Wrap, HMACwith3DESwrap and HMACwithAESwrap (key encryption), AES, Triple-DES and RC2 (content encryption), PBKDF2 with PWRI-KEK (RFC 3211, password-based encryption for CMS)
- Can be used with any alternative algorithm implementation fulfilling the requirements of the CMS / S/MIME protocols
- Supports Elliptic Curve Cryptography (ECDSA, ECDH) when used with the IAIK-ECC library
- Supports DSA with SHA-2 according to FIPS 186-3
- Support for Camellia Encryption and Key Wrap algorithm (RFC 3657)
- Supports X.509 public key and attribute certificates
- Contains basic, extensible certificate verification and trust policy utility
- Supports all content types of S/MIMEv3: multipart/signed with application/pkcs7-signature, application/pkcs7-mime (signed-data, enveloped-data, certs-only, signed-receipt (ESS), compressed-data); + application/pkcs10 from S/MIMEv2
- Supports ESS Triple Wrapping and arbitrary nesting of S/MIME parts
- Supports all Enhanced Security Services (ESS) specified by RFC 2634, 5035:

  - Signing Certificates (+ V2 Signing Certificates)
  - Security Labels
  - Signed Receipts
  - Secure Mailing List
- Supports ESS TripleWrapping and arbitrary nesting of S/MIME parts
- Application Extensible Design:
  - Pluggable custom content-type implementations
  - Pluggable custom certification path verification
  - Pluggable custom cryptographic algorithm implementations
  - Pluggable custom canonicalization (S/MIME) and security label policies (ESS)
- Proven Interoperability
  - Interoperates with any CMS and S/MIMEv3 implementation
  - Backwards compatible to PKCS#7v1.5 and S/MIMEv2
  - Interoperability tested among others with clients Microsoft Outlook Express, Microsoft Outlook, Netscape, Mozilla Messenger and Thunderbird
  - Listed in the IETF CMS Draft Standard Implementation Report http://www.ietf.org/iesg/implementation/report-rfc3852.txt)
- Cryptographic Provider Independence
  - Can be used with any JCA/JCE 1.2 (or later) compliant cryptography provider
  - Can use several different cryptography providers at the same time
  - Easy integration of smartcards and other secure hardware devices
  - Allows plug-in of user written JCA/JCE engines
  - Allows plug-in of user written non JCA/JCE compliant crypto code
  - Comes with the IAIK JCE provider by default (included in license)