**Java Cryptography Architecture (JCA) Reference Guide**

[Skip Table of Contents](https://docs.oracle.com/javase/8/docs/technotes/guides/security/crypto/CryptoSpec.html#javasemaincontent)

* [Introduction](https://docs.oracle.com/javase/8/docs/technotes/guides/security/crypto/CryptoSpec.html#Introduction)
  + [Design Principles](https://docs.oracle.com/javase/8/docs/technotes/guides/security/crypto/CryptoSpec.html#Design)
  + [Architecture](https://docs.oracle.com/javase/8/docs/technotes/guides/security/crypto/CryptoSpec.html#Architecture)
  + [JCA Concepts](https://docs.oracle.com/javase/8/docs/technotes/guides/security/crypto/CryptoSpec.html#Concepts)
* [Core Classes and Interfaces](https://docs.oracle.com/javase/8/docs/technotes/guides/security/crypto/CryptoSpec.html#CoreClasses)
  + [The Provider Class](https://docs.oracle.com/javase/8/docs/technotes/guides/security/crypto/CryptoSpec.html#Provider)
    - [How Provider Implementations are Requested and Supplied](https://docs.oracle.com/javase/8/docs/technotes/guides/security/crypto/CryptoSpec.html#ProviderImplReq)
    - [Installing Providers](https://docs.oracle.com/javase/8/docs/technotes/guides/security/crypto/CryptoSpec.html#ProviderInstalling)
  + [The Security Class](https://docs.oracle.com/javase/8/docs/technotes/guides/security/crypto/CryptoSpec.html#Security)
  + [The SecureRandom Class](https://docs.oracle.com/javase/8/docs/technotes/guides/security/crypto/CryptoSpec.html#SecureRandom)
  + [The MessageDigest Class](https://docs.oracle.com/javase/8/docs/technotes/guides/security/crypto/CryptoSpec.html#MessageDigest)
  + [The Signature Class](https://docs.oracle.com/javase/8/docs/technotes/guides/security/crypto/CryptoSpec.html#Signature)
  + [The Cipher Class](https://docs.oracle.com/javase/8/docs/technotes/guides/security/crypto/CryptoSpec.html#Cipher)
  + [Other Cipher-based Classes](https://docs.oracle.com/javase/8/docs/technotes/guides/security/crypto/CryptoSpec.html#CipherBased)
    - [The Cipher Stream Classes](https://docs.oracle.com/javase/8/docs/technotes/guides/security/crypto/CryptoSpec.html#CipherStream)
      * [The CipherInputStream Class](https://docs.oracle.com/javase/8/docs/technotes/guides/security/crypto/CryptoSpec.html#CipherInput)
      * [The CipherOutputStream Class](https://docs.oracle.com/javase/8/docs/technotes/guides/security/crypto/CryptoSpec.html#CipherOutput)
    - [The SealedObject Class](https://docs.oracle.com/javase/8/docs/technotes/guides/security/crypto/CryptoSpec.html#SealedObject)
  + [The Mac Class](https://docs.oracle.com/javase/8/docs/technotes/guides/security/crypto/CryptoSpec.html#Mac)
  + [Key Interfaces](https://docs.oracle.com/javase/8/docs/technotes/guides/security/crypto/CryptoSpec.html#Key)
  + [The KeyPair Class](https://docs.oracle.com/javase/8/docs/technotes/guides/security/crypto/CryptoSpec.html#KeyPair)
  + [Key Specification Interfaces and Classes](https://docs.oracle.com/javase/8/docs/technotes/guides/security/crypto/CryptoSpec.html#KeySpecs)
    - [The KeySpec Interface](https://docs.oracle.com/javase/8/docs/technotes/guides/security/crypto/CryptoSpec.html#KeySpec)
    - [The KeySpec Subinterfaces](https://docs.oracle.com/javase/8/docs/technotes/guides/security/crypto/CryptoSpec.html#KeySpecSubs)
    - [The EncodedKeySpec Class](https://docs.oracle.com/javase/8/docs/technotes/guides/security/crypto/CryptoSpec.html#EncodedKeySpec)
      * [The PKCS8EncodedKeySpec Class](https://docs.oracle.com/javase/8/docs/technotes/guides/security/crypto/CryptoSpec.html#PKCS8EncodedKeySpec)
      * [The X509EncodedKeySpec Class](https://docs.oracle.com/javase/8/docs/technotes/guides/security/crypto/CryptoSpec.html#X509EncodedKeySpec)
  + [Of Factories and Generators](https://docs.oracle.com/javase/8/docs/technotes/guides/security/crypto/CryptoSpec.html#GeneratorFactory)
  + [The KeyFactory Class](https://docs.oracle.com/javase/8/docs/technotes/guides/security/crypto/CryptoSpec.html#KeyFactory)
  + [The SecretKeyFactory Class](https://docs.oracle.com/javase/8/docs/technotes/guides/security/crypto/CryptoSpec.html#SecretKeyFactory)
  + [The KeyPairGenerator Class](https://docs.oracle.com/javase/8/docs/technotes/guides/security/crypto/CryptoSpec.html#KeyPairGenerator)
  + [The KeyGenerator Class](https://docs.oracle.com/javase/8/docs/technotes/guides/security/crypto/CryptoSpec.html#KeyGenerator)
  + [The KeyAgreement Class](https://docs.oracle.com/javase/8/docs/technotes/guides/security/crypto/CryptoSpec.html#KeyAgreement)
  + [Key Management](https://docs.oracle.com/javase/8/docs/technotes/guides/security/crypto/CryptoSpec.html#KeyManagement)
    - [Keystore Location](https://docs.oracle.com/javase/8/docs/technotes/guides/security/crypto/CryptoSpec.html#KeystoreLocation)
    - [Keystore Implementation](https://docs.oracle.com/javase/8/docs/technotes/guides/security/crypto/CryptoSpec.html#KeystoreImplementation)
    - [The KeyStore Class](https://docs.oracle.com/javase/8/docs/technotes/guides/security/crypto/CryptoSpec.html#KeyStore)
  + [Algorithm Parameters Classes](https://docs.oracle.com/javase/8/docs/technotes/guides/security/crypto/CryptoSpec.html#AlgSpec)
    - [The AlgorithmParameterSpec Interface](https://docs.oracle.com/javase/8/docs/technotes/guides/security/crypto/CryptoSpec.html#AlgorithmParameterSpec)
    - [The AlgorithmParameters Class](https://docs.oracle.com/javase/8/docs/technotes/guides/security/crypto/CryptoSpec.html#AlgorithmParameters)
    - [The AlgorithmParameterGenerator Class](https://docs.oracle.com/javase/8/docs/technotes/guides/security/crypto/CryptoSpec.html#AlgorithmParameterGenerator)
  + [The CertificateFactory Class](https://docs.oracle.com/javase/8/docs/technotes/guides/security/crypto/CryptoSpec.html#CertificateFactory)
* [How the JCA Might Be Used in a SSL/TLS Implementation](https://docs.oracle.com/javase/8/docs/technotes/guides/security/crypto/CryptoSpec.html#SSLTLS)
* [How to Make Applications "Exempt" from Cryptographic Restrictions](https://docs.oracle.com/javase/8/docs/technotes/guides/security/crypto/CryptoSpec.html#ExemptApps)
* [Code Examples](https://docs.oracle.com/javase/8/docs/technotes/guides/security/crypto/CryptoSpec.html#Examples)
  + [Computing a MessageDigest Object](https://docs.oracle.com/javase/8/docs/technotes/guides/security/crypto/CryptoSpec.html#MDEx)
  + [Generating a Pair of Keys](https://docs.oracle.com/javase/8/docs/technotes/guides/security/crypto/CryptoSpec.html#KPGEx)
  + [Generating and Verifying a Signature Using Generated Keys](https://docs.oracle.com/javase/8/docs/technotes/guides/security/crypto/CryptoSpec.html#SigEx)
  + [Generating/Verifying Signatures Using Key Specifications and KeyFactory](https://docs.oracle.com/javase/8/docs/technotes/guides/security/crypto/CryptoSpec.html#KeyFactoryEx)
  + [Determining If Two Keys Are Equal](https://docs.oracle.com/javase/8/docs/technotes/guides/security/crypto/CryptoSpec.html#Equal)
  + [Reading Base64-Encoded Certificates](https://docs.oracle.com/javase/8/docs/technotes/guides/security/crypto/CryptoSpec.html#ReadCert)
  + [Parsing a Certificate Reply](https://docs.oracle.com/javase/8/docs/technotes/guides/security/crypto/CryptoSpec.html#ParseCert)
  + [Using Encryption](https://docs.oracle.com/javase/8/docs/technotes/guides/security/crypto/CryptoSpec.html#SimpleEncrEx)
  + [Using Password-Based Encryption](https://docs.oracle.com/javase/8/docs/technotes/guides/security/crypto/CryptoSpec.html#PBEEx)
  + [Using Key Agreement](https://docs.oracle.com/javase/8/docs/technotes/guides/security/crypto/CryptoSpec.html#KeyAgreeEx)
* [Appendix A: Standard Names](https://docs.oracle.com/javase/8/docs/technotes/guides/security/crypto/CryptoSpec.html#AppA)
* [Appendix B: Jurisdiction Policy File Format](https://docs.oracle.com/javase/8/docs/technotes/guides/security/crypto/CryptoSpec.html#AppB)
* [Appendix C: Cryptographic Strength Configuration](https://docs.oracle.com/javase/8/docs/technotes/guides/security/crypto/CryptoSpec.html#AppC)
* [Appendix D: Sample Programs](https://docs.oracle.com/javase/8/docs/technotes/guides/security/crypto/CryptoSpec.html#AppD)
  + [Diffie-Hellman Key Exchange between 2 Parties](https://docs.oracle.com/javase/8/docs/technotes/guides/security/crypto/CryptoSpec.html#DH2Ex)
  + [Diffie-Hellman Key Exchange between 3 Parties](https://docs.oracle.com/javase/8/docs/technotes/guides/security/crypto/CryptoSpec.html#DH3Ex)
  + [Blowfish Cipher Example](https://docs.oracle.com/javase/8/docs/technotes/guides/security/crypto/CryptoSpec.html#BlowKeyEx)
  + [HMAC-SHA256 Example](https://docs.oracle.com/javase/8/docs/technotes/guides/security/crypto/CryptoSpec.html#HmacEx)
  + [Reading ASCII Passwords From an InputStream Example](https://docs.oracle.com/javase/8/docs/technotes/guides/security/crypto/CryptoSpec.html#ReadPassword)