Module java.base

Package java.security.interfaces

`package java.security.interfaces`

Provides interfaces for generating RSA (Rivest, Shamir and Adleman AsymmetricCipher algorithm) keys as defined in the RSA Laboratory Technical Note PKCS#1, and DSA (Digital Signature Algorithm) keys as defined in NIST's FIPS-186.

Note that these interfaces are intended only for key implementations whose key material is accessible and available. These interfaces are not intended for key implementations whose key material resides in inaccessible, protected storage (such as in a hardware device).

For more developer information on how to use these interfaces, including information on how to design Key classes for hardware devices, please refer to these cryptographic provider developer guides:

- How to Implement a Provider in the Java Cryptography Architecture

Package Specification

- PKCS #1: RSA Cryptography Specifications, Version 2.2 (RFC 8017)
- Federal Information Processing Standards Publication (FIPS PUB) 186: Digital Signature Standard (DSS)

Related Documentation

For further documentation, please see:

- Java Cryptography Architecture Reference Guide

Since:

1.1

Related Packages

Package	Description
java.security	Provides the classes and interfaces for the security framework.
java.security.cert	Provides classes and interfaces for parsing and managing certificates, certificate revocation lists (CRLs), and certification paths.

java.security.spec	Provides classes and interfaces for key specifications and algorithm parameter specifications.

Interfaces

Class	Description
DSAKey	The interface to a DSA public or private key.
DSAKeyPairGenerator	An interface to an object capable of generating DSA key pairs.
DSAParams	Interface to a DSA-specific set of key parameters, which defines a DSA *key family*.
DSAPrivateKey	The standard interface to a DSA private key.
DSAPublicKey	The interface to a DSA public key.
ECKey	The interface to an elliptic curve (EC) key.
ECPrivateKey	The interface to an elliptic curve (EC) private key.
ECPublicKey	The interface to an elliptic curve (EC) public key.
EdECKey	An interface for an elliptic curve public/private key as defined by RFC 8032: Edwards-Curve Digital Signature Algorithm (EdDSA).
EdECPrivateKey	An interface for an elliptic curve private key as defined by RFC 8032: Edwards-Curve Digital Signature Algorithm (EdDSA).
EdECPublicKey	An interface for an elliptic curve public key as defined by RFC 8032: Edwards-Curve Digital Signature Algorithm (EdDSA).
RSAKey	The interface to a public or private key in PKCS#1 v2.2 standard, such as those for RSA, or RSASSA-PSS algorithms.
RSAMultiPrimePrivateCrtKey	The interface to an RSA multi-prime private key, as defined in the PKCS#1 v2.2 standard, using the *Chinese Remainder Theorem* (CRT) information values.

RSAPrivateCrtKey	The interface to an RSA private key, as defined in the PKCS#1 v2.2 standard, using the *Chinese Remainder Theorem* (CRT) information values.
RSAPrivateKey	The interface to an RSA private key.
RSAPublicKey	The interface to an RSA public key.
XECKey	An interface for an elliptic curve public/private key as defined by RFC 7748.
XECPrivateKey	An interface for an elliptic curve private key as defined by RFC 7748.
XECPublicKey	An interface for an elliptic curve public key as defined by RFC 7748.