| | [**Overview**](http://docs.google.com/overview-summary.html) | **Package** | Class | [**Use**](http://docs.google.com/package-use.html) | [**Tree**](http://docs.google.com/package-tree.html) | [**Deprecated**](http://docs.google.com/deprecated-list.html) | [**Index**](http://docs.google.com/index-files/index-1.html) | [**Help**](http://docs.google.com/help-doc.html) | | --- | --- | --- | --- | --- | --- | --- | --- | | | ***Java™ Platform***  ***Standard Ed. 6*** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| [**PREV PACKAGE**](http://docs.google.com/java/security/cert/package-summary.html)   [**NEXT PACKAGE**](http://docs.google.com/java/security/spec/package-summary.html) | [**FRAMES**](http://docs.google.com/index.html?java/security/interfaces/package-summary.html)    [**NO FRAMES**](http://docs.google.com/package-summary.html)     [**All Classes**](http://docs.google.com/allclasses-noframe.html) |

## 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.

**See:**

[**Description**](#3znysh7)

| **Interface Summary** | |
| --- | --- |
| [**DSAKey**](http://docs.google.com/java/security/interfaces/DSAKey.html) | The interface to a DSA public or private key. |
| [**DSAKeyPairGenerator**](http://docs.google.com/java/security/interfaces/DSAKeyPairGenerator.html) | An interface to an object capable of generating DSA key pairs. |
| [**DSAParams**](http://docs.google.com/java/security/interfaces/DSAParams.html) | Interface to a DSA-specific set of key parameters, which defines a DSA *key family*. |
| [**DSAPrivateKey**](http://docs.google.com/java/security/interfaces/DSAPrivateKey.html) | The standard interface to a DSA private key. |
| [**DSAPublicKey**](http://docs.google.com/java/security/interfaces/DSAPublicKey.html) | The interface to a DSA public key. |
| [**ECKey**](http://docs.google.com/java/security/interfaces/ECKey.html) | The interface to an elliptic curve (EC) key. |
| [**ECPrivateKey**](http://docs.google.com/java/security/interfaces/ECPrivateKey.html) | The interface to an elliptic curve (EC) private key. |
| [**ECPublicKey**](http://docs.google.com/java/security/interfaces/ECPublicKey.html) | The interface to an elliptic curve (EC) public key. |
| [**RSAKey**](http://docs.google.com/java/security/interfaces/RSAKey.html) | The interface to an RSA public or private key. |
| [**RSAMultiPrimePrivateCrtKey**](http://docs.google.com/java/security/interfaces/RSAMultiPrimePrivateCrtKey.html) | The interface to an RSA multi-prime private key, as defined in the PKCS#1 v2.1, using the *Chinese Remainder Theorem* (CRT) information values. |
| [**RSAPrivateCrtKey**](http://docs.google.com/java/security/interfaces/RSAPrivateCrtKey.html) | The interface to an RSA private key, as defined in the PKCS#1 standard, using the *Chinese Remainder Theorem* (CRT) information values. |
| [**RSAPrivateKey**](http://docs.google.com/java/security/interfaces/RSAPrivateKey.html) | The interface to an RSA private key. |
| [**RSAPublicKey**](http://docs.google.com/java/security/interfaces/RSAPublicKey.html) | The interface to an RSA public key. |

## Package java.security.interfaces Description

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 for the JavaTM Cryptography Architecture**](http://docs.google.com/technotes/guides/security/crypto/HowToImplAProvider.html)

## Package Specification

* PKCS #1: RSA Encryption Standard, Version 1.5, November 1993
* Federal Information Processing Standards Publication (FIPS PUB) 186: Digital Signature Standard (DSS)

## Related Documentation

For further documentation, please see:

* [**JavaTM Cryptography Architecture API Specification and Reference**](http://docs.google.com/technotes/guides/security/crypto/CryptoSpec.html)

**Since:** JDK1.1

| | [**Overview**](http://docs.google.com/overview-summary.html) | **Package** | Class | [**Use**](http://docs.google.com/package-use.html) | [**Tree**](http://docs.google.com/package-tree.html) | [**Deprecated**](http://docs.google.com/deprecated-list.html) | [**Index**](http://docs.google.com/index-files/index-1.html) | [**Help**](http://docs.google.com/help-doc.html) | | --- | --- | --- | --- | --- | --- | --- | --- | | | ***Java™ Platform***  ***Standard Ed. 6*** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| [**PREV PACKAGE**](http://docs.google.com/java/security/cert/package-summary.html)   [**NEXT PACKAGE**](http://docs.google.com/java/security/spec/package-summary.html) | [**FRAMES**](http://docs.google.com/index.html?java/security/interfaces/package-summary.html)    [**NO FRAMES**](http://docs.google.com/package-summary.html)     [**All Classes**](http://docs.google.com/allclasses-noframe.html) |

[Submit a bug or feature](http://bugs.sun.com/services/bugreport/index.jsp)

For further API reference and developer documentation, see [Java SE Developer Documentation](http://docs.google.com/webnotes/devdocs-vs-specs.html). That documentation contains more detailed, developer-targeted descriptions, with conceptual overviews, definitions of terms, workarounds, and working code examples.

Copyright 2006 Sun Microsystems, Inc. All rights reserved. Use is subject to [license terms](http://docs.google.com/legal/license.html). Also see the [documentation redistribution policy](http://java.sun.com/docs/redist.html).