| | [**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/interfaces/package-summary.html)   [**NEXT PACKAGE**](http://docs.google.com/java/sql/package-summary.html) | [**FRAMES**](http://docs.google.com/index.html?java/security/spec/package-summary.html)    [**NO FRAMES**](http://docs.google.com/package-summary.html)     [**All Classes**](http://docs.google.com/allclasses-noframe.html) |

## Package java.security.spec

Provides classes and interfaces for key specifications and algorithm parameter specifications.

**See:**

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

| **Interface Summary** | |
| --- | --- |
| [**AlgorithmParameterSpec**](http://docs.google.com/java/security/spec/AlgorithmParameterSpec.html) | A (transparent) specification of cryptographic parameters. |
| [**ECField**](http://docs.google.com/java/security/spec/ECField.html) | This interface represents an elliptic curve (EC) finite field. |
| [**KeySpec**](http://docs.google.com/java/security/spec/KeySpec.html) | A (transparent) specification of the key material that constitutes a cryptographic key. |

| **Class Summary** | |
| --- | --- |
| [**DSAParameterSpec**](http://docs.google.com/java/security/spec/DSAParameterSpec.html) | This class specifies the set of parameters used with the DSA algorithm. |
| [**DSAPrivateKeySpec**](http://docs.google.com/java/security/spec/DSAPrivateKeySpec.html) | This class specifies a DSA private key with its associated parameters. |
| [**DSAPublicKeySpec**](http://docs.google.com/java/security/spec/DSAPublicKeySpec.html) | This class specifies a DSA public key with its associated parameters. |
| [**ECFieldF2m**](http://docs.google.com/java/security/spec/ECFieldF2m.html) | This immutable class defines an elliptic curve (EC) characteristic 2 finite field. |
| [**ECFieldFp**](http://docs.google.com/java/security/spec/ECFieldFp.html) | This immutable class defines an elliptic curve (EC) prime finite field. |
| [**ECGenParameterSpec**](http://docs.google.com/java/security/spec/ECGenParameterSpec.html) | This immutable class specifies the set of parameters used for generating elliptic curve (EC) domain parameters. |
| [**ECParameterSpec**](http://docs.google.com/java/security/spec/ECParameterSpec.html) | This immutable class specifies the set of domain parameters used with elliptic curve cryptography (ECC). |
| [**ECPoint**](http://docs.google.com/java/security/spec/ECPoint.html) | This immutable class represents a point on an elliptic curve (EC) in affine coordinates. |
| [**ECPrivateKeySpec**](http://docs.google.com/java/security/spec/ECPrivateKeySpec.html) | This immutable class specifies an elliptic curve private key with its associated parameters. |
| [**ECPublicKeySpec**](http://docs.google.com/java/security/spec/ECPublicKeySpec.html) | This immutable class specifies an elliptic curve public key with its associated parameters. |
| [**EllipticCurve**](http://docs.google.com/java/security/spec/EllipticCurve.html) | This immutable class holds the necessary values needed to represent an elliptic curve. |
| [**EncodedKeySpec**](http://docs.google.com/java/security/spec/EncodedKeySpec.html) | This class represents a public or private key in encoded format. |
| [**MGF1ParameterSpec**](http://docs.google.com/java/security/spec/MGF1ParameterSpec.html) | This class specifies the set of parameters used with mask generation function MGF1 in OAEP Padding and RSA-PSS signature scheme, as defined in the [PKCS #1 v2.1](http://www.ietf.org/rfc/rfc3447.txt) standard. |
| [**PKCS8EncodedKeySpec**](http://docs.google.com/java/security/spec/PKCS8EncodedKeySpec.html) | This class represents the ASN.1 encoding of a private key, encoded according to the ASN.1 type PrivateKeyInfo. |
| [**PSSParameterSpec**](http://docs.google.com/java/security/spec/PSSParameterSpec.html) | This class specifies a parameter spec for RSA-PSS signature scheme, as defined in the [PKCS#1 v2.1](http://www.ietf.org/rfc/rfc3447.txt) standard. |
| [**RSAKeyGenParameterSpec**](http://docs.google.com/java/security/spec/RSAKeyGenParameterSpec.html) | This class specifies the set of parameters used to generate an RSA key pair. |
| [**RSAMultiPrimePrivateCrtKeySpec**](http://docs.google.com/java/security/spec/RSAMultiPrimePrivateCrtKeySpec.html) | This class specifies an RSA multi-prime private key, as defined in the PKCS#1 v2.1, using the Chinese Remainder Theorem (CRT) information values for efficiency. |
| [**RSAOtherPrimeInfo**](http://docs.google.com/java/security/spec/RSAOtherPrimeInfo.html) | This class represents the triplet (prime, exponent, and coefficient) inside RSA's OtherPrimeInfo structure, as defined in the PKCS#1 v2.1. |
| [**RSAPrivateCrtKeySpec**](http://docs.google.com/java/security/spec/RSAPrivateCrtKeySpec.html) | This class specifies an RSA private key, as defined in the PKCS#1 standard, using the Chinese Remainder Theorem (CRT) information values for efficiency. |
| [**RSAPrivateKeySpec**](http://docs.google.com/java/security/spec/RSAPrivateKeySpec.html) | This class specifies an RSA private key. |
| [**RSAPublicKeySpec**](http://docs.google.com/java/security/spec/RSAPublicKeySpec.html) | This class specifies an RSA public key. |
| [**X509EncodedKeySpec**](http://docs.google.com/java/security/spec/X509EncodedKeySpec.html) | This class represents the ASN.1 encoding of a public key, encoded according to the ASN.1 type SubjectPublicKeyInfo. |

| **Exception Summary** | |
| --- | --- |
| [**InvalidKeySpecException**](http://docs.google.com/java/security/spec/InvalidKeySpecException.html) | This is the exception for invalid key specifications. |
| [**InvalidParameterSpecException**](http://docs.google.com/java/security/spec/InvalidParameterSpecException.html) | This is the exception for invalid parameter specifications. |

## Package java.security.spec Description

Provides classes and interfaces for key specifications and algorithm parameter specifications.

A key specification is a transparent representation of the key material that constitutes a key. A key may be specified in an algorithm-specific way, or in an algorithm-independent encoding format (such as ASN.1). This package contains key specifications for DSA public and private keys, RSA public and private keys, PKCS #8 private keys in DER-encoded format, and X.509 public and private keys in DER-encoded format.

An algorithm parameter specification is a transparent representation of the sets of parameters used with an algorithm. This package contains an algorithm parameter specification for parameters used with the DSA algorithm.

## Package Specification

* PKCS #1: RSA Encryption Standard, Version 1.5, November 1993
* PKCS #8: Private-Key Information Syntax Standard, Version 1.2, November 1993
* Federal Information Processing Standards Publication (FIPS PUB) 186: Digital Signature Standard (DSS)

## Related Documentation

For documentation that includes information about algorithm parameter and key specifications, please see:

* [**JavaTM Cryptography Architecture API Specification and Reference**](http://docs.google.com/technotes/guides/security/crypto/CryptoSpec.html)
* [**How to Implement a Provider for the JavaTM Cryptography Architecture**](http://docs.google.com/technotes/guides/security/crypto/HowToImplAProvider.html)

**Since:** 1.2

| | [**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/interfaces/package-summary.html)   [**NEXT PACKAGE**](http://docs.google.com/java/sql/package-summary.html) | [**FRAMES**](http://docs.google.com/index.html?java/security/spec/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).