| | [**Overview**](http://docs.google.com/overview-summary.html) | [**Package**](http://docs.google.com/package-summary.html) | **Class** | [**Use**](http://docs.google.com/class-use/OAEPParameterSpec.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 CLASS**](http://docs.google.com/javax/crypto/spec/IvParameterSpec.html)   [**NEXT CLASS**](http://docs.google.com/javax/crypto/spec/PBEKeySpec.html) | [**FRAMES**](http://docs.google.com/index.html?javax/crypto/spec/OAEPParameterSpec.html)    [**NO FRAMES**](http://docs.google.com/OAEPParameterSpec.html)     [**All Classes**](http://docs.google.com/allclasses-noframe.html) |
| SUMMARY: NESTED | [FIELD](#3znysh7) | [CONSTR](#2et92p0) | [METHOD](#tyjcwt) | DETAIL: [FIELD](#1t3h5sf) | [CONSTR](#2s8eyo1) | [METHOD](#3rdcrjn) |

## **javax.crypto.spec**

Class OAEPParameterSpec

[java.lang.Object](http://docs.google.com/java/lang/Object.html)  
 **javax.crypto.spec.OAEPParameterSpec**

**All Implemented Interfaces:** [AlgorithmParameterSpec](http://docs.google.com/java/security/spec/AlgorithmParameterSpec.html)

public class **OAEPParameterSpec**extends [Object](http://docs.google.com/java/lang/Object.html)implements [AlgorithmParameterSpec](http://docs.google.com/java/security/spec/AlgorithmParameterSpec.html)

This class specifies the set of parameters used with OAEP Padding, as defined in the [PKCS #1](http://www.ietf.org/rfc/rfc3447.txt) standard. Its ASN.1 definition in PKCS#1 standard is described below:

RSAES-OAEP-params ::= SEQUENCE {  
 hashAlgorithm [0] OAEP-PSSDigestAlgorithms DEFAULT sha1,  
 maskGenAlgorithm [1] PKCS1MGFAlgorithms DEFAULT mgf1SHA1,  
 pSourceAlgorithm [2] PKCS1PSourceAlgorithms DEFAULT pSpecifiedEmpty  
 }

where

OAEP-PSSDigestAlgorithms ALGORITHM-IDENTIFIER ::= {  
 { OID id-sha1 PARAMETERS NULL }|  
 { OID id-sha256 PARAMETERS NULL }|  
 { OID id-sha384 PARAMETERS NULL }|  
 { OID id-sha512 PARAMETERS NULL },  
 ... -- Allows for future expansion --  
 }  
 PKCS1MGFAlgorithms ALGORITHM-IDENTIFIER ::= {  
 { OID id-mgf1 PARAMETERS OAEP-PSSDigestAlgorithms },  
 ... -- Allows for future expansion --  
 }  
 PKCS1PSourceAlgorithms ALGORITHM-IDENTIFIER ::= {  
 { OID id-pSpecified PARAMETERS OCTET STRING },  
 ... -- Allows for future expansion --  
 }

Note: the OAEPParameterSpec.DEFAULT uses the following: message digest -- "SHA-1" mask generation function (mgf) -- "MGF1" parameters for mgf -- MGF1ParameterSpec.SHA1 source of encoding input -- PSource.PSpecified.DEFAULT

**Since:** 1.5 **See Also:**[MGF1ParameterSpec](http://docs.google.com/java/security/spec/MGF1ParameterSpec.html), [PSource](http://docs.google.com/javax/crypto/spec/PSource.html)

| **Field Summary** | |
| --- | --- |
| static [OAEPParameterSpec](http://docs.google.com/javax/crypto/spec/OAEPParameterSpec.html) | [**DEFAULT**](http://docs.google.com/javax/crypto/spec/OAEPParameterSpec.html#DEFAULT)            The OAEP parameter set with all default values. |

| **Constructor Summary** | |
| --- | --- |
| [**OAEPParameterSpec**](http://docs.google.com/javax/crypto/spec/OAEPParameterSpec.html#OAEPParameterSpec(java.lang.String,%20java.lang.String,%20java.security.spec.AlgorithmParameterSpec,%20javax.crypto.spec.PSource))([String](http://docs.google.com/java/lang/String.html) mdName, [String](http://docs.google.com/java/lang/String.html) mgfName, [AlgorithmParameterSpec](http://docs.google.com/java/security/spec/AlgorithmParameterSpec.html) mgfSpec, [PSource](http://docs.google.com/javax/crypto/spec/PSource.html) pSrc)            Constructs a parameter set for OAEP padding as defined in the PKCS #1 standard using the specified message digest algorithm mdName, mask generation function algorithm mgfName, parameters for the mask generation function mgfSpec, and source of the encoding input P pSrc. |

| **Method Summary** | |
| --- | --- |
| [String](http://docs.google.com/java/lang/String.html) | [**getDigestAlgorithm**](http://docs.google.com/javax/crypto/spec/OAEPParameterSpec.html#getDigestAlgorithm())()            Returns the message digest algorithm name. |
| [String](http://docs.google.com/java/lang/String.html) | [**getMGFAlgorithm**](http://docs.google.com/javax/crypto/spec/OAEPParameterSpec.html#getMGFAlgorithm())()            Returns the mask generation function algorithm name. |
| [AlgorithmParameterSpec](http://docs.google.com/java/security/spec/AlgorithmParameterSpec.html) | [**getMGFParameters**](http://docs.google.com/javax/crypto/spec/OAEPParameterSpec.html#getMGFParameters())()            Returns the parameters for the mask generation function. |
| [PSource](http://docs.google.com/javax/crypto/spec/PSource.html) | [**getPSource**](http://docs.google.com/javax/crypto/spec/OAEPParameterSpec.html#getPSource())()            Returns the source of encoding input P. |

| **Methods inherited from class java.lang.**[**Object**](http://docs.google.com/java/lang/Object.html) |
| --- |
| [clone](http://docs.google.com/java/lang/Object.html#clone()), [equals](http://docs.google.com/java/lang/Object.html#equals(java.lang.Object)), [finalize](http://docs.google.com/java/lang/Object.html#finalize()), [getClass](http://docs.google.com/java/lang/Object.html#getClass()), [hashCode](http://docs.google.com/java/lang/Object.html#hashCode()), [notify](http://docs.google.com/java/lang/Object.html#notify()), [notifyAll](http://docs.google.com/java/lang/Object.html#notifyAll()), [toString](http://docs.google.com/java/lang/Object.html#toString()), [wait](http://docs.google.com/java/lang/Object.html#wait()), [wait](http://docs.google.com/java/lang/Object.html#wait(long)), [wait](http://docs.google.com/java/lang/Object.html#wait(long,%20int)) |

| **Field Detail** |
| --- |

### DEFAULT

public static final [OAEPParameterSpec](http://docs.google.com/javax/crypto/spec/OAEPParameterSpec.html) **DEFAULT**

The OAEP parameter set with all default values.

| **Constructor Detail** |
| --- |

### OAEPParameterSpec

public **OAEPParameterSpec**([String](http://docs.google.com/java/lang/String.html) mdName,  
 [String](http://docs.google.com/java/lang/String.html) mgfName,  
 [AlgorithmParameterSpec](http://docs.google.com/java/security/spec/AlgorithmParameterSpec.html) mgfSpec,  
 [PSource](http://docs.google.com/javax/crypto/spec/PSource.html) pSrc)

Constructs a parameter set for OAEP padding as defined in the PKCS #1 standard using the specified message digest algorithm mdName, mask generation function algorithm mgfName, parameters for the mask generation function mgfSpec, and source of the encoding input P pSrc.

**Parameters:**mdName - the algorithm name for the message digest.mgfName - the algorithm name for the mask generation function.mgfSpec - the parameters for the mask generation function. If null is specified, null will be returned by getMGFParameters().pSrc - the source of the encoding input P. **Throws:** [NullPointerException](http://docs.google.com/java/lang/NullPointerException.html) - if mdName, mgfName, or pSrc is null.

| **Method Detail** |
| --- |

### getDigestAlgorithm

public [String](http://docs.google.com/java/lang/String.html) **getDigestAlgorithm**()

Returns the message digest algorithm name.

**Returns:**the message digest algorithm name.

### getMGFAlgorithm

public [String](http://docs.google.com/java/lang/String.html) **getMGFAlgorithm**()

Returns the mask generation function algorithm name.

**Returns:**the mask generation function algorithm name.

### getMGFParameters

public [AlgorithmParameterSpec](http://docs.google.com/java/security/spec/AlgorithmParameterSpec.html) **getMGFParameters**()

Returns the parameters for the mask generation function.

**Returns:**the parameters for the mask generation function.

### getPSource

public [PSource](http://docs.google.com/javax/crypto/spec/PSource.html) **getPSource**()

Returns the source of encoding input P.

**Returns:**the source of encoding input P.

| | [**Overview**](http://docs.google.com/overview-summary.html) | [**Package**](http://docs.google.com/package-summary.html) | **Class** | [**Use**](http://docs.google.com/class-use/OAEPParameterSpec.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 CLASS**](http://docs.google.com/javax/crypto/spec/IvParameterSpec.html)   [**NEXT CLASS**](http://docs.google.com/javax/crypto/spec/PBEKeySpec.html) | [**FRAMES**](http://docs.google.com/index.html?javax/crypto/spec/OAEPParameterSpec.html)    [**NO FRAMES**](http://docs.google.com/OAEPParameterSpec.html)     [**All Classes**](http://docs.google.com/allclasses-noframe.html) |
| SUMMARY: NESTED | [FIELD](#3znysh7) | [CONSTR](#2et92p0) | [METHOD](#tyjcwt) | DETAIL: [FIELD](#1t3h5sf) | [CONSTR](#2s8eyo1) | [METHOD](#3rdcrjn) |

[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).