| | [**Overview**](http://docs.google.com/overview-summary.html) | [**Package**](http://docs.google.com/package-summary.html) | **Class** | [**Use**](http://docs.google.com/class-use/MGF1ParameterSpec.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/java/security/spec/KeySpec.html)   [**NEXT CLASS**](http://docs.google.com/java/security/spec/PKCS8EncodedKeySpec.html) | [**FRAMES**](http://docs.google.com/index.html?java/security/spec/MGF1ParameterSpec.html)    [**NO FRAMES**](http://docs.google.com/MGF1ParameterSpec.html)     [**All Classes**](http://docs.google.com/allclasses-noframe.html) |
| SUMMARY: NESTED | [FIELD](#3znysh7) | [CONSTR](#2et92p0) | [METHOD](#tyjcwt) | DETAIL: [FIELD](#1t3h5sf) | [CONSTR](#26in1rg) | [METHOD](#35nkun2) |

## **java.security.spec**

Class MGF1ParameterSpec

[java.lang.Object](http://docs.google.com/java/lang/Object.html)  
 **java.security.spec.MGF1ParameterSpec**

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

public class **MGF1ParameterSpec**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 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.

Its ASN.1 definition in PKCS#1 standard is described below:

MGF1Parameters ::= OAEP-PSSDigestAlgorthms

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 --  
 }

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

| **Field Summary** | |
| --- | --- |
| static [MGF1ParameterSpec](http://docs.google.com/java/security/spec/MGF1ParameterSpec.html) | [**SHA1**](http://docs.google.com/java/security/spec/MGF1ParameterSpec.html#SHA1)            The MGF1ParameterSpec which uses "SHA-1" message digest. |
| static [MGF1ParameterSpec](http://docs.google.com/java/security/spec/MGF1ParameterSpec.html) | [**SHA256**](http://docs.google.com/java/security/spec/MGF1ParameterSpec.html#SHA256)            The MGF1ParameterSpec which uses "SHA-256" message digest. |
| static [MGF1ParameterSpec](http://docs.google.com/java/security/spec/MGF1ParameterSpec.html) | [**SHA384**](http://docs.google.com/java/security/spec/MGF1ParameterSpec.html#SHA384)            The MGF1ParameterSpec which uses "SHA-384" message digest. |
| static [MGF1ParameterSpec](http://docs.google.com/java/security/spec/MGF1ParameterSpec.html) | [**SHA512**](http://docs.google.com/java/security/spec/MGF1ParameterSpec.html#SHA512)            The MGF1ParameterSpec which uses SHA-512 message digest. |

| **Constructor Summary** | |
| --- | --- |
| [**MGF1ParameterSpec**](http://docs.google.com/java/security/spec/MGF1ParameterSpec.html#MGF1ParameterSpec(java.lang.String))([String](http://docs.google.com/java/lang/String.html) mdName)            Constructs a parameter set for mask generation function MGF1 as defined in the PKCS #1 standard. |

| **Method Summary** | |
| --- | --- |
| [String](http://docs.google.com/java/lang/String.html) | [**getDigestAlgorithm**](http://docs.google.com/java/security/spec/MGF1ParameterSpec.html#getDigestAlgorithm())()            Returns the algorithm name of the message digest used by the mask generation function. |

| **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** |
| --- |

### SHA1

public static final [MGF1ParameterSpec](http://docs.google.com/java/security/spec/MGF1ParameterSpec.html) **SHA1**

The MGF1ParameterSpec which uses "SHA-1" message digest.

### SHA256

public static final [MGF1ParameterSpec](http://docs.google.com/java/security/spec/MGF1ParameterSpec.html) **SHA256**

The MGF1ParameterSpec which uses "SHA-256" message digest.

### SHA384

public static final [MGF1ParameterSpec](http://docs.google.com/java/security/spec/MGF1ParameterSpec.html) **SHA384**

The MGF1ParameterSpec which uses "SHA-384" message digest.

### SHA512

public static final [MGF1ParameterSpec](http://docs.google.com/java/security/spec/MGF1ParameterSpec.html) **SHA512**

The MGF1ParameterSpec which uses SHA-512 message digest.

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

### MGF1ParameterSpec

public **MGF1ParameterSpec**([String](http://docs.google.com/java/lang/String.html) mdName)

Constructs a parameter set for mask generation function MGF1 as defined in the PKCS #1 standard.

**Parameters:**mdName - the algorithm name for the message digest used in this mask generation function MGF1. **Throws:** [NullPointerException](http://docs.google.com/java/lang/NullPointerException.html) - if mdName is null.

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

### getDigestAlgorithm

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

Returns the algorithm name of the message digest used by the mask generation function.

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

| | [**Overview**](http://docs.google.com/overview-summary.html) | [**Package**](http://docs.google.com/package-summary.html) | **Class** | [**Use**](http://docs.google.com/class-use/MGF1ParameterSpec.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/java/security/spec/KeySpec.html)   [**NEXT CLASS**](http://docs.google.com/java/security/spec/PKCS8EncodedKeySpec.html) | [**FRAMES**](http://docs.google.com/index.html?java/security/spec/MGF1ParameterSpec.html)    [**NO FRAMES**](http://docs.google.com/MGF1ParameterSpec.html)     [**All Classes**](http://docs.google.com/allclasses-noframe.html) |
| SUMMARY: NESTED | [FIELD](#3znysh7) | [CONSTR](#2et92p0) | [METHOD](#tyjcwt) | DETAIL: [FIELD](#1t3h5sf) | [CONSTR](#26in1rg) | [METHOD](#35nkun2) |

[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).