| | [**Overview**](http://docs.google.com/overview-summary.html) | [**Package**](http://docs.google.com/package-summary.html) | **Class** | [**Use**](http://docs.google.com/class-use/PSSParameterSpec.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/PKCS8EncodedKeySpec.html)   [**NEXT CLASS**](http://docs.google.com/java/security/spec/RSAKeyGenParameterSpec.html) | [**FRAMES**](http://docs.google.com/index.html?java/security/spec/PSSParameterSpec.html)    [**NO FRAMES**](http://docs.google.com/PSSParameterSpec.html)     [**All Classes**](http://docs.google.com/allclasses-noframe.html) |
| SUMMARY: NESTED | [FIELD](#3znysh7) | [CONSTR](#2et92p0) | [METHOD](#tyjcwt) | DETAIL: [FIELD](#1t3h5sf) | [CONSTR](#2s8eyo1) | [METHOD](#26in1rg) |

## **java.security.spec**

Class PSSParameterSpec

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

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

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

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

RSASSA-PSS-params ::= SEQUENCE {  
 hashAlgorithm [0] OAEP-PSSDigestAlgorithms DEFAULT sha1,  
 maskGenAlgorithm [1] PKCS1MGFAlgorithms DEFAULT mgf1SHA1,  
 saltLength [2] INTEGER DEFAULT 20,  
 trailerField [3] INTEGER DEFAULT 1  
 }

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 --  
 }

Note: the PSSParameterSpec.DEFAULT uses the following: message digest -- "SHA-1" mask generation function (mgf) -- "MGF1" parameters for mgf -- MGF1ParameterSpec.SHA1 SaltLength -- 20 TrailerField -- 1

**Since:** 1.4 **See Also:**[MGF1ParameterSpec](http://docs.google.com/java/security/spec/MGF1ParameterSpec.html), [AlgorithmParameterSpec](http://docs.google.com/java/security/spec/AlgorithmParameterSpec.html), [Signature](http://docs.google.com/java/security/Signature.html)

| **Field Summary** | |
| --- | --- |
| static [PSSParameterSpec](http://docs.google.com/java/security/spec/PSSParameterSpec.html) | [**DEFAULT**](http://docs.google.com/java/security/spec/PSSParameterSpec.html#DEFAULT)            The PSS parameter set with all default values. |

| **Constructor Summary** | |
| --- | --- |
| [**PSSParameterSpec**](http://docs.google.com/java/security/spec/PSSParameterSpec.html#PSSParameterSpec(int))(int saltLen)            Creates a new PSSParameterSpec using the specified salt length and other default values as defined in PKCS#1. |
| [**PSSParameterSpec**](http://docs.google.com/java/security/spec/PSSParameterSpec.html#PSSParameterSpec(java.lang.String,%20java.lang.String,%20java.security.spec.AlgorithmParameterSpec,%20int,%20int))([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, int saltLen, int trailerField)            Creates a new PSSParameterSpec as defined in the PKCS #1 standard using the specified message digest, mask generation function, parameters for mask generation function, salt length, and trailer field values. |

| **Method Summary** | |
| --- | --- |
| [String](http://docs.google.com/java/lang/String.html) | [**getDigestAlgorithm**](http://docs.google.com/java/security/spec/PSSParameterSpec.html#getDigestAlgorithm())()            Returns the message digest algorithm name. |
| [String](http://docs.google.com/java/lang/String.html) | [**getMGFAlgorithm**](http://docs.google.com/java/security/spec/PSSParameterSpec.html#getMGFAlgorithm())()            Returns the mask generation function algorithm name. |
| [AlgorithmParameterSpec](http://docs.google.com/java/security/spec/AlgorithmParameterSpec.html) | [**getMGFParameters**](http://docs.google.com/java/security/spec/PSSParameterSpec.html#getMGFParameters())()            Returns the parameters for the mask generation function. |
| int | [**getSaltLength**](http://docs.google.com/java/security/spec/PSSParameterSpec.html#getSaltLength())()            Returns the salt length in bits. |
| int | [**getTrailerField**](http://docs.google.com/java/security/spec/PSSParameterSpec.html#getTrailerField())()            Returns the value for the trailer field, i.e. |

| **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 [PSSParameterSpec](http://docs.google.com/java/security/spec/PSSParameterSpec.html) **DEFAULT**

The PSS parameter set with all default values.

**Since:** 1.5

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

### PSSParameterSpec

public **PSSParameterSpec**([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,  
 int saltLen,  
 int trailerField)

Creates a new PSSParameterSpec as defined in the PKCS #1 standard using the specified message digest, mask generation function, parameters for mask generation function, salt length, and trailer field values.

**Parameters:**mdName - the algorithm name of the hash function.mgfName - the algorithm name of the mask generation function.mgfSpec - the parameters for the mask generation function. If null is specified, null will be returned by getMGFParameters().saltLen - the length of salt.trailerField - the value of the trailer field. **Throws:** [NullPointerException](http://docs.google.com/java/lang/NullPointerException.html) - if mdName, or mgfName is null. [IllegalArgumentException](http://docs.google.com/java/lang/IllegalArgumentException.html) - if saltLen or trailerField is less than 0.**Since:** 1.5

### PSSParameterSpec

public **PSSParameterSpec**(int saltLen)

Creates a new PSSParameterSpec using the specified salt length and other default values as defined in PKCS#1.

**Parameters:**saltLen - the length of salt in bits to be used in PKCS#1 PSS encoding. **Throws:** [IllegalArgumentException](http://docs.google.com/java/lang/IllegalArgumentException.html) - if saltLen is less than 0.

| **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.**Since:** 1.5

### 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.**Since:** 1.5

### 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.**Since:** 1.5

### getSaltLength

public int **getSaltLength**()

Returns the salt length in bits.

**Returns:**the salt length.

### getTrailerField

public int **getTrailerField**()

Returns the value for the trailer field, i.e. bc in PKCS#1 v2.1.

**Returns:**the value for the trailer field, i.e. bc in PKCS#1 v2.1.**Since:** 1.5

| | [**Overview**](http://docs.google.com/overview-summary.html) | [**Package**](http://docs.google.com/package-summary.html) | **Class** | [**Use**](http://docs.google.com/class-use/PSSParameterSpec.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/PKCS8EncodedKeySpec.html)   [**NEXT CLASS**](http://docs.google.com/java/security/spec/RSAKeyGenParameterSpec.html) | [**FRAMES**](http://docs.google.com/index.html?java/security/spec/PSSParameterSpec.html)    [**NO FRAMES**](http://docs.google.com/PSSParameterSpec.html)     [**All Classes**](http://docs.google.com/allclasses-noframe.html) |
| SUMMARY: NESTED | [FIELD](#3znysh7) | [CONSTR](#2et92p0) | [METHOD](#tyjcwt) | DETAIL: [FIELD](#1t3h5sf) | [CONSTR](#2s8eyo1) | [METHOD](#26in1rg) |

[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).