| | [**Overview**](http://docs.google.com/overview-summary.html) | [**Package**](http://docs.google.com/package-summary.html) | **Class** | [**Use**](http://docs.google.com/class-use/X509Extension.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/cert/X509CRLSelector.html)   NEXT CLASS | [**FRAMES**](http://docs.google.com/index.html?java/security/cert/X509Extension.html)    [**NO FRAMES**](http://docs.google.com/X509Extension.html)     [**All Classes**](http://docs.google.com/allclasses-noframe.html) |
| SUMMARY: NESTED | FIELD | CONSTR | [METHOD](#3znysh7) | DETAIL: FIELD | CONSTR | [METHOD](#2et92p0) |

## **java.security.cert**

Interface X509Extension

**All Known Implementing Classes:** [X509Certificate](http://docs.google.com/java/security/cert/X509Certificate.html), [X509CRL](http://docs.google.com/java/security/cert/X509CRL.html), [X509CRLEntry](http://docs.google.com/java/security/cert/X509CRLEntry.html)

public interface **X509Extension**

Interface for an X.509 extension.

The extensions defined for X.509 v3 [Certificates](http://docs.google.com/java/security/cert/X509Certificate.html) and v2 [CRLs](http://docs.google.com/java/security/cert/X509CRL.html) (Certificate Revocation Lists) provide methods for associating additional attributes with users or public keys, for managing the certification hierarchy, and for managing CRL distribution. The X.509 extensions format also allows communities to define private extensions to carry information unique to those communities.

Each extension in a certificate/CRL may be designated as critical or non-critical. A certificate/CRL-using system (an application validating a certificate/CRL) must reject the certificate/CRL if it encounters a critical extension it does not recognize. A non-critical extension may be ignored if it is not recognized.

The ASN.1 definition for this is:

Extensions ::= SEQUENCE SIZE (1..MAX) OF Extension  
  
 Extension ::= SEQUENCE {  
 extnId OBJECT IDENTIFIER,  
 critical BOOLEAN DEFAULT FALSE,  
 extnValue OCTET STRING  
 -- contains a DER encoding of a value  
 -- of the type registered for use with  
 -- the extnId object identifier value  
 }

Since not all extensions are known, the getExtensionValue method returns the DER-encoded OCTET STRING of the extension value (i.e., the extnValue). This can then be handled by a *Class* that understands the extension.

| **Method Summary** | |
| --- | --- |
| [Set](http://docs.google.com/java/util/Set.html)<[String](http://docs.google.com/java/lang/String.html)> | [**getCriticalExtensionOIDs**](http://docs.google.com/java/security/cert/X509Extension.html#getCriticalExtensionOIDs())()            Gets a Set of the OID strings for the extension(s) marked CRITICAL in the certificate/CRL managed by the object implementing this interface. |
| byte[] | [**getExtensionValue**](http://docs.google.com/java/security/cert/X509Extension.html#getExtensionValue(java.lang.String))([String](http://docs.google.com/java/lang/String.html) oid)            Gets the DER-encoded OCTET string for the extension value (*extnValue*) identified by the passed-in oid String. |
| [Set](http://docs.google.com/java/util/Set.html)<[String](http://docs.google.com/java/lang/String.html)> | [**getNonCriticalExtensionOIDs**](http://docs.google.com/java/security/cert/X509Extension.html#getNonCriticalExtensionOIDs())()            Gets a Set of the OID strings for the extension(s) marked NON-CRITICAL in the certificate/CRL managed by the object implementing this interface. |
| boolean | [**hasUnsupportedCriticalExtension**](http://docs.google.com/java/security/cert/X509Extension.html#hasUnsupportedCriticalExtension())()            Check if there is a critical extension that is not supported. |

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

### hasUnsupportedCriticalExtension

boolean **hasUnsupportedCriticalExtension**()

Check if there is a critical extension that is not supported.

**Returns:**true if a critical extension is found that is not supported, otherwise false.

### getCriticalExtensionOIDs

[Set](http://docs.google.com/java/util/Set.html)<[String](http://docs.google.com/java/lang/String.html)> **getCriticalExtensionOIDs**()

Gets a Set of the OID strings for the extension(s) marked CRITICAL in the certificate/CRL managed by the object implementing this interface. Here is sample code to get a Set of critical extensions from an X509Certificate and print the OIDs:

InputStream inStrm = new FileInputStream("DER-encoded-Cert");  
 CertificateFactory cf = CertificateFactory.getInstance("X.509");  
 X509Certificate cert = (X509Certificate)cf.generateCertificate(inStrm);  
 inStrm.close();

Set critSet = cert.getCriticalExtensionOIDs();  
 if (critSet != null && !critSet.isEmpty()) {  
 System.out.println("Set of critical extensions:");  
 for (Iterator i = critSet.iterator(); i.hasNext();) {  
 String oid = (String)i.next();  
 System.out.println(oid);  
 }  
 }

**Returns:**a Set (or an empty Set if none are marked critical) of the extension OID strings for extensions that are marked critical. If there are no extensions present at all, then this method returns null.

### getNonCriticalExtensionOIDs

[Set](http://docs.google.com/java/util/Set.html)<[String](http://docs.google.com/java/lang/String.html)> **getNonCriticalExtensionOIDs**()

Gets a Set of the OID strings for the extension(s) marked NON-CRITICAL in the certificate/CRL managed by the object implementing this interface. Here is sample code to get a Set of non-critical extensions from an X509CRL revoked certificate entry and print the OIDs:

InputStream inStrm = new FileInputStream("DER-encoded-CRL");  
 CertificateFactory cf = CertificateFactory.getInstance("X.509");  
 X509CRL crl = (X509CRL)cf.generateCRL(inStrm);  
 inStrm.close();

byte[] certData = <DER-encoded certificate data>  
 ByteArrayInputStream bais = new ByteArrayInputStream(certData);  
 X509Certificate cert = (X509Certificate)cf.generateCertificate(bais);  
 bais.close();  
 X509CRLEntry badCert =  
 crl.getRevokedCertificate(cert.getSerialNumber());

if (badCert != null) {  
 Set nonCritSet = badCert.getNonCriticalExtensionOIDs();

if (nonCritSet != null)  
 for (Iterator i = nonCritSet.iterator(); i.hasNext();) {  
 String oid = (String)i.next();  
 System.out.println(oid);  
 }  
 }

**Returns:**a Set (or an empty Set if none are marked non-critical) of the extension OID strings for extensions that are marked non-critical. If there are no extensions present at all, then this method returns null.

### getExtensionValue

byte[] **getExtensionValue**([String](http://docs.google.com/java/lang/String.html) oid)

Gets the DER-encoded OCTET string for the extension value (*extnValue*) identified by the passed-in oid String. The oid string is represented by a set of nonnegative whole numbers separated by periods.

For example:

| OID *(Object Identifier)* | Extension Name |
| --- | --- |
| 2.5.29.14 | SubjectKeyIdentifier |
| 2.5.29.15 | KeyUsage |
| 2.5.29.16 | PrivateKeyUsage |
| 2.5.29.17 | SubjectAlternativeName |
| 2.5.29.18 | IssuerAlternativeName |
| 2.5.29.19 | BasicConstraints |
| 2.5.29.30 | NameConstraints |
| 2.5.29.33 | PolicyMappings |
| 2.5.29.35 | AuthorityKeyIdentifier |
| 2.5.29.36 | PolicyConstraints |

**Parameters:**oid - the Object Identifier value for the extension. **Returns:**the DER-encoded octet string of the extension value or null if it is not present.

| | [**Overview**](http://docs.google.com/overview-summary.html) | [**Package**](http://docs.google.com/package-summary.html) | **Class** | [**Use**](http://docs.google.com/class-use/X509Extension.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/cert/X509CRLSelector.html)   NEXT CLASS | [**FRAMES**](http://docs.google.com/index.html?java/security/cert/X509Extension.html)    [**NO FRAMES**](http://docs.google.com/X509Extension.html)     [**All Classes**](http://docs.google.com/allclasses-noframe.html) |
| SUMMARY: NESTED | FIELD | CONSTR | [METHOD](#3znysh7) | DETAIL: FIELD | CONSTR | [METHOD](#2et92p0) |

[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).