| | [**Overview**](http://docs.google.com/overview-summary.html) | [**Package**](http://docs.google.com/package-summary.html) | **Class** | [**Use**](http://docs.google.com/class-use/TrustAnchor.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/PolicyQualifierInfo.html)   [**NEXT CLASS**](http://docs.google.com/java/security/cert/X509Certificate.html) | [**FRAMES**](http://docs.google.com/index.html?java/security/cert/TrustAnchor.html)    [**NO FRAMES**](http://docs.google.com/TrustAnchor.html)     [**All Classes**](http://docs.google.com/allclasses-noframe.html) |
| SUMMARY: NESTED | FIELD | [CONSTR](#3znysh7) | [METHOD](#2et92p0) | DETAIL: FIELD | [CONSTR](#3dy6vkm) | [METHOD](#17dp8vu) |

## **java.security.cert**

Class TrustAnchor

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

public class **TrustAnchor**extends [Object](http://docs.google.com/java/lang/Object.html)

A trust anchor or most-trusted Certification Authority (CA).

This class represents a "most-trusted CA", which is used as a trust anchor for validating X.509 certification paths. A most-trusted CA includes the public key of the CA, the CA's name, and any constraints upon the set of paths which may be validated using this key. These parameters can be specified in the form of a trusted X509Certificate or as individual parameters.

**Concurrent Access**

All TrustAnchor objects must be immutable and thread-safe. That is, multiple threads may concurrently invoke the methods defined in this class on a single TrustAnchor object (or more than one) with no ill effects. Requiring TrustAnchor objects to be immutable and thread-safe allows them to be passed around to various pieces of code without worrying about coordinating access. This stipulation applies to all public fields and methods of this class and any added or overridden by subclasses.

**Since:** 1.4 **See Also:**[PKIXParameters.PKIXParameters(Set)](http://docs.google.com/java/security/cert/PKIXParameters.html#PKIXParameters(java.util.Set)), [PKIXBuilderParameters.PKIXBuilderParameters(Set, CertSelector)](http://docs.google.com/java/security/cert/PKIXBuilderParameters.html#PKIXBuilderParameters(java.util.Set,%20java.security.cert.CertSelector))

| **Constructor Summary** | |
| --- | --- |
| [**TrustAnchor**](http://docs.google.com/java/security/cert/TrustAnchor.html#TrustAnchor(java.lang.String,%20java.security.PublicKey,%20byte%5B%5D))([String](http://docs.google.com/java/lang/String.html) caName, [PublicKey](http://docs.google.com/java/security/PublicKey.html) pubKey, byte[] nameConstraints)            Creates an instance of TrustAnchor where the most-trusted CA is specified as a distinguished name and public key. |
| [**TrustAnchor**](http://docs.google.com/java/security/cert/TrustAnchor.html#TrustAnchor(javax.security.auth.x500.X500Principal,%20java.security.PublicKey,%20byte%5B%5D))([X500Principal](http://docs.google.com/javax/security/auth/x500/X500Principal.html) caPrincipal, [PublicKey](http://docs.google.com/java/security/PublicKey.html) pubKey, byte[] nameConstraints)            Creates an instance of TrustAnchor where the most-trusted CA is specified as an X500Principal and public key. |
| [**TrustAnchor**](http://docs.google.com/java/security/cert/TrustAnchor.html#TrustAnchor(java.security.cert.X509Certificate,%20byte%5B%5D))([X509Certificate](http://docs.google.com/java/security/cert/X509Certificate.html) trustedCert, byte[] nameConstraints)            Creates an instance of TrustAnchor with the specified X509Certificate and optional name constraints, which are intended to be used as additional constraints when validating an X.509 certification path. |

| **Method Summary** | |
| --- | --- |
| [X500Principal](http://docs.google.com/javax/security/auth/x500/X500Principal.html) | [**getCA**](http://docs.google.com/java/security/cert/TrustAnchor.html#getCA())()            Returns the name of the most-trusted CA as an X500Principal. |
| [String](http://docs.google.com/java/lang/String.html) | [**getCAName**](http://docs.google.com/java/security/cert/TrustAnchor.html#getCAName())()            Returns the name of the most-trusted CA in RFC 2253 String format. |
| [PublicKey](http://docs.google.com/java/security/PublicKey.html) | [**getCAPublicKey**](http://docs.google.com/java/security/cert/TrustAnchor.html#getCAPublicKey())()            Returns the public key of the most-trusted CA. |
| byte[] | [**getNameConstraints**](http://docs.google.com/java/security/cert/TrustAnchor.html#getNameConstraints())()            Returns the name constraints parameter. |
| [X509Certificate](http://docs.google.com/java/security/cert/X509Certificate.html) | [**getTrustedCert**](http://docs.google.com/java/security/cert/TrustAnchor.html#getTrustedCert())()            Returns the most-trusted CA certificate. |
| [String](http://docs.google.com/java/lang/String.html) | [**toString**](http://docs.google.com/java/security/cert/TrustAnchor.html#toString())()            Returns a formatted string describing the TrustAnchor. |

| **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()), [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)) |

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

### TrustAnchor

public **TrustAnchor**([X509Certificate](http://docs.google.com/java/security/cert/X509Certificate.html) trustedCert,  
 byte[] nameConstraints)

Creates an instance of TrustAnchor with the specified X509Certificate and optional name constraints, which are intended to be used as additional constraints when validating an X.509 certification path.

The name constraints are specified as a byte array. This byte array should contain the DER encoded form of the name constraints, as they would appear in the NameConstraints structure defined in RFC 2459 and X.509. The ASN.1 definition of this structure appears below.

NameConstraints ::= SEQUENCE {  
 permittedSubtrees [0] GeneralSubtrees OPTIONAL,  
 excludedSubtrees [1] GeneralSubtrees OPTIONAL }  
  
 GeneralSubtrees ::= SEQUENCE SIZE (1..MAX) OF GeneralSubtree  
  
 GeneralSubtree ::= SEQUENCE {  
 base GeneralName,  
 minimum [0] BaseDistance DEFAULT 0,  
 maximum [1] BaseDistance OPTIONAL }  
  
 BaseDistance ::= INTEGER (0..MAX)  
  
 GeneralName ::= CHOICE {  
 otherName [0] OtherName,  
 rfc822Name [1] IA5String,  
 dNSName [2] IA5String,  
 x400Address [3] ORAddress,  
 directoryName [4] Name,  
 ediPartyName [5] EDIPartyName,  
 uniformResourceIdentifier [6] IA5String,  
 iPAddress [7] OCTET STRING,  
 registeredID [8] OBJECT IDENTIFIER}

Note that the name constraints byte array supplied is cloned to protect against subsequent modifications.

**Parameters:**trustedCert - a trusted X509CertificatenameConstraints - a byte array containing the ASN.1 DER encoding of a NameConstraints extension to be used for checking name constraints. Only the value of the extension is included, not the OID or criticality flag. Specify null to omit the parameter. **Throws:** [IllegalArgumentException](http://docs.google.com/java/lang/IllegalArgumentException.html) - if the name constraints cannot be decoded [NullPointerException](http://docs.google.com/java/lang/NullPointerException.html) - if the specified X509Certificate is null

### TrustAnchor

public **TrustAnchor**([X500Principal](http://docs.google.com/javax/security/auth/x500/X500Principal.html) caPrincipal,  
 [PublicKey](http://docs.google.com/java/security/PublicKey.html) pubKey,  
 byte[] nameConstraints)

Creates an instance of TrustAnchor where the most-trusted CA is specified as an X500Principal and public key. Name constraints are an optional parameter, and are intended to be used as additional constraints when validating an X.509 certification path.

The name constraints are specified as a byte array. This byte array contains the DER encoded form of the name constraints, as they would appear in the NameConstraints structure defined in RFC 2459 and X.509. The ASN.1 notation for this structure is supplied in the documentation for [TrustAnchor(X509Certificate trustedCert, byte[] nameConstraints)](http://docs.google.com/java/security/cert/TrustAnchor.html#TrustAnchor(java.security.cert.X509Certificate,%20byte%5B%5D)) .

Note that the name constraints byte array supplied here is cloned to protect against subsequent modifications.

**Parameters:**caPrincipal - the name of the most-trusted CA as X500PrincipalpubKey - the public key of the most-trusted CAnameConstraints - a byte array containing the ASN.1 DER encoding of a NameConstraints extension to be used for checking name constraints. Only the value of the extension is included, not the OID or criticality flag. Specify null to omit the parameter. **Throws:** [NullPointerException](http://docs.google.com/java/lang/NullPointerException.html) - if the specified caPrincipal or pubKey parameter is null**Since:** 1.5

### TrustAnchor

public **TrustAnchor**([String](http://docs.google.com/java/lang/String.html) caName,  
 [PublicKey](http://docs.google.com/java/security/PublicKey.html) pubKey,  
 byte[] nameConstraints)

Creates an instance of TrustAnchor where the most-trusted CA is specified as a distinguished name and public key. Name constraints are an optional parameter, and are intended to be used as additional constraints when validating an X.509 certification path.

The name constraints are specified as a byte array. This byte array contains the DER encoded form of the name constraints, as they would appear in the NameConstraints structure defined in RFC 2459 and X.509. The ASN.1 notation for this structure is supplied in the documentation for [TrustAnchor(X509Certificate trustedCert, byte[] nameConstraints)](http://docs.google.com/java/security/cert/TrustAnchor.html#TrustAnchor(java.security.cert.X509Certificate,%20byte%5B%5D)) .

Note that the name constraints byte array supplied here is cloned to protect against subsequent modifications.

**Parameters:**caName - the X.500 distinguished name of the most-trusted CA in RFC 2253 String formatpubKey - the public key of the most-trusted CAnameConstraints - a byte array containing the ASN.1 DER encoding of a NameConstraints extension to be used for checking name constraints. Only the value of the extension is included, not the OID or criticality flag. Specify null to omit the parameter. **Throws:** [IllegalArgumentException](http://docs.google.com/java/lang/IllegalArgumentException.html) - if the specified caName parameter is empty (caName.length() == 0) or incorrectly formatted or the name constraints cannot be decoded [NullPointerException](http://docs.google.com/java/lang/NullPointerException.html) - if the specified caName or pubKey parameter is null

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

### getTrustedCert

public final [X509Certificate](http://docs.google.com/java/security/cert/X509Certificate.html) **getTrustedCert**()

Returns the most-trusted CA certificate.

**Returns:**a trusted X509Certificate or null if the trust anchor was not specified as a trusted certificate

### getCA

public final [X500Principal](http://docs.google.com/javax/security/auth/x500/X500Principal.html) **getCA**()

Returns the name of the most-trusted CA as an X500Principal.

**Returns:**the X.500 distinguished name of the most-trusted CA, or null if the trust anchor was not specified as a trusted public key and name or X500Principal pair**Since:** 1.5

### getCAName

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

Returns the name of the most-trusted CA in RFC 2253 String format.

**Returns:**the X.500 distinguished name of the most-trusted CA, or null if the trust anchor was not specified as a trusted public key and name or X500Principal pair

### getCAPublicKey

public final [PublicKey](http://docs.google.com/java/security/PublicKey.html) **getCAPublicKey**()

Returns the public key of the most-trusted CA.

**Returns:**the public key of the most-trusted CA, or null if the trust anchor was not specified as a trusted public key and name or X500Principal pair

### getNameConstraints

public final byte[] **getNameConstraints**()

Returns the name constraints parameter. The specified name constraints are associated with this trust anchor and are intended to be used as additional constraints when validating an X.509 certification path.

The name constraints are returned as a byte array. This byte array contains the DER encoded form of the name constraints, as they would appear in the NameConstraints structure defined in RFC 2459 and X.509. The ASN.1 notation for this structure is supplied in the documentation for [TrustAnchor(X509Certificate trustedCert, byte[] nameConstraints)](http://docs.google.com/java/security/cert/TrustAnchor.html#TrustAnchor(java.security.cert.X509Certificate,%20byte%5B%5D)) .

Note that the byte array returned is cloned to protect against subsequent modifications.

**Returns:**a byte array containing the ASN.1 DER encoding of a NameConstraints extension used for checking name constraints, or null if not set.

### toString

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

Returns a formatted string describing the TrustAnchor.

**Overrides:**[toString](http://docs.google.com/java/lang/Object.html#toString()) in class [Object](http://docs.google.com/java/lang/Object.html) **Returns:**a formatted string describing the TrustAnchor

| | [**Overview**](http://docs.google.com/overview-summary.html) | [**Package**](http://docs.google.com/package-summary.html) | **Class** | [**Use**](http://docs.google.com/class-use/TrustAnchor.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/PolicyQualifierInfo.html)   [**NEXT CLASS**](http://docs.google.com/java/security/cert/X509Certificate.html) | [**FRAMES**](http://docs.google.com/index.html?java/security/cert/TrustAnchor.html)    [**NO FRAMES**](http://docs.google.com/TrustAnchor.html)     [**All Classes**](http://docs.google.com/allclasses-noframe.html) |
| SUMMARY: NESTED | FIELD | [CONSTR](#3znysh7) | [METHOD](#2et92p0) | DETAIL: FIELD | [CONSTR](#3dy6vkm) | [METHOD](#17dp8vu) |

[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).