| | [**Overview**](http://docs.google.com/overview-summary.html) | [**Package**](http://docs.google.com/package-summary.html) | **Class** | [**Use**](http://docs.google.com/class-use/X509TrustManager.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/net/ssl/X509KeyManager.html)   NEXT CLASS | [**FRAMES**](http://docs.google.com/index.html?javax/net/ssl/X509TrustManager.html)    [**NO FRAMES**](http://docs.google.com/X509TrustManager.html)     [**All Classes**](http://docs.google.com/allclasses-noframe.html) |
| SUMMARY: NESTED | FIELD | CONSTR | [METHOD](#3znysh7) | DETAIL: FIELD | CONSTR | [METHOD](#2et92p0) |

## **javax.net.ssl**

Interface X509TrustManager

**All Superinterfaces:** [TrustManager](http://docs.google.com/javax/net/ssl/TrustManager.html)

public interface **X509TrustManager**extends [TrustManager](http://docs.google.com/javax/net/ssl/TrustManager.html)

Instance of this interface manage which X509 certificates may be used to authenticate the remote side of a secure socket. Decisions may be based on trusted certificate authorities, certificate revocation lists, online status checking or other means.

**Since:** 1.4

| **Method Summary** | |
| --- | --- |
| void | [**checkClientTrusted**](http://docs.google.com/javax/net/ssl/X509TrustManager.html#checkClientTrusted(java.security.cert.X509Certificate%5B%5D,%20java.lang.String))([X509Certificate](http://docs.google.com/java/security/cert/X509Certificate.html)[] chain, [String](http://docs.google.com/java/lang/String.html) authType)            Given the partial or complete certificate chain provided by the peer, build a certificate path to a trusted root and return if it can be validated and is trusted for client SSL authentication based on the authentication type. |
| void | [**checkServerTrusted**](http://docs.google.com/javax/net/ssl/X509TrustManager.html#checkServerTrusted(java.security.cert.X509Certificate%5B%5D,%20java.lang.String))([X509Certificate](http://docs.google.com/java/security/cert/X509Certificate.html)[] chain, [String](http://docs.google.com/java/lang/String.html) authType)            Given the partial or complete certificate chain provided by the peer, build a certificate path to a trusted root and return if it can be validated and is trusted for server SSL authentication based on the authentication type. |
| [X509Certificate](http://docs.google.com/java/security/cert/X509Certificate.html)[] | [**getAcceptedIssuers**](http://docs.google.com/javax/net/ssl/X509TrustManager.html#getAcceptedIssuers())()            Return an array of certificate authority certificates which are trusted for authenticating peers. |

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

### checkClientTrusted

void **checkClientTrusted**([X509Certificate](http://docs.google.com/java/security/cert/X509Certificate.html)[] chain,  
 [String](http://docs.google.com/java/lang/String.html) authType)  
 throws [CertificateException](http://docs.google.com/java/security/cert/CertificateException.html)

Given the partial or complete certificate chain provided by the peer, build a certificate path to a trusted root and return if it can be validated and is trusted for client SSL authentication based on the authentication type.

The authentication type is determined by the actual certificate used. For instance, if RSAPublicKey is used, the authType should be "RSA". Checking is case-sensitive.

**Parameters:**chain - the peer certificate chainauthType - the authentication type based on the client certificate **Throws:** [IllegalArgumentException](http://docs.google.com/java/lang/IllegalArgumentException.html) - if null or zero-length chain is passed in for the chain parameter or if null or zero-length string is passed in for the authType parameter [CertificateException](http://docs.google.com/java/security/cert/CertificateException.html) - if the certificate chain is not trusted by this TrustManager.

### checkServerTrusted

void **checkServerTrusted**([X509Certificate](http://docs.google.com/java/security/cert/X509Certificate.html)[] chain,  
 [String](http://docs.google.com/java/lang/String.html) authType)  
 throws [CertificateException](http://docs.google.com/java/security/cert/CertificateException.html)

Given the partial or complete certificate chain provided by the peer, build a certificate path to a trusted root and return if it can be validated and is trusted for server SSL authentication based on the authentication type.

The authentication type is the key exchange algorithm portion of the cipher suites represented as a String, such as "RSA", "DHE\_DSS". Note: for some exportable cipher suites, the key exchange algorithm is determined at run time during the handshake. For instance, for TLS\_RSA\_EXPORT\_WITH\_RC4\_40\_MD5, the authType should be RSA\_EXPORT when an ephemeral RSA key is used for the key exchange, and RSA when the key from the server certificate is used. Checking is case-sensitive.

**Parameters:**chain - the peer certificate chainauthType - the key exchange algorithm used **Throws:** [IllegalArgumentException](http://docs.google.com/java/lang/IllegalArgumentException.html) - if null or zero-length chain is passed in for the chain parameter or if null or zero-length string is passed in for the authType parameter [CertificateException](http://docs.google.com/java/security/cert/CertificateException.html) - if the certificate chain is not trusted by this TrustManager.

### getAcceptedIssuers

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

Return an array of certificate authority certificates which are trusted for authenticating peers.

**Returns:**a non-null (possibly empty) array of acceptable CA issuer certificates.

| | [**Overview**](http://docs.google.com/overview-summary.html) | [**Package**](http://docs.google.com/package-summary.html) | **Class** | [**Use**](http://docs.google.com/class-use/X509TrustManager.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/net/ssl/X509KeyManager.html)   NEXT CLASS | [**FRAMES**](http://docs.google.com/index.html?javax/net/ssl/X509TrustManager.html)    [**NO FRAMES**](http://docs.google.com/X509TrustManager.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).