Key Stor vs. Trust Store für Java und https

Key Store

Schlüssel-Speicher

Server

Verwendung

Enthält private Schlüssel und die zugehörigen öffentlichen Zertifikate und wird zur Identifizierung und Authentifizierung von Entitäten (Server oder Client) verwendet.

Zweck

Bereitstellung von Identifikation und Authentifizierung für Server (in Server-Key-Stores) oder Client (in Client-Key-Stores) in einer verschlüsselten Kommunikation.

Inhalt

Private Schlüssel und öffentliche Zertifikate, die zur Authentifizierung verwendet werden.

Dateiformat

Normalerweise im PKCS12-, JKS- oder PEM-Format.

Standardeinstellungen

Es gibt keinen vordefinierten Standard-Key Store. Die Anwendung oder der Server muss ihren eigenen Key Store konfigurieren.

Ort auf dem Dateisystem (typisch)

Anwendungsabhängig und kann in verschiedenen Verzeichnissen liegen.

Anpassbarkeit

Sie können benutzerdefinierte Key Stores erstellen und verwenden, um private Schlüssel und Zertifikate nach Bedarf zu verwalten.

Verwendung in SSL/TLS-Kommunikation

Wird von SSL/TLS-Servern (für Server-Key-Stores) und Clients (für Client-Key-Stores) verwendet, um sich bei der Kommunikation zu authentifizieren.

vs.

Trust Store

Vertrauens-Speicher

Client

Verwendung

Enthält Zertifikate von vertrauenswürdigen CAs (Certification Authorities) und wird verwendet, um die Glaubwürdigkeit von Serverzertifikaten zu überprüfen.

Zweck

Sicherstellung, dass Remote-Serverzertifikate von vertrauenswürdigen CAs ausgestellt wurden und daher vertrauenswürdig sind.

Inhalt

Root-Zertifikate oder Zwischenzertifikate von vertrauenswürdigen CAs.

Dateiformat

Normalerweise im PEM- oder JKS-Format.

Standardeinstellungen

Java verfügt über einen Standard-Trust Store mit vorinstallierten Root-Zertifikaten.

Ort auf dem Dateisystem (typisch)

/etc/ssl/certs/ oder /etc/pki/tls/certs/ oder /etc/pki/java/cacerts auf Linux-Systemen.

Anpassbarkeit

Sie können benutzerdefinierte Trust Stores erstellen und verwenden, um spezielle Validierungsanforderungen zu erfüllen.

X509TrustManager

- checkServerTrusted
- getAcceptedIssuers
- checkClientTrusted

www.wenzlaff.de