Leitfaden

MOA-SP und Trust-Service Status Listen (TSL)

Integration und Verwendung von Trust-Service Status Listen in MOA-SP

Version 1.0, 17.03.2014

Klaus Stranacher – klaus.stranacher@egiz.gv.at

Zusammenfassung: Trust-Service Status Listen (TSL) sind ein ETSI Standard der es erlaubt Aussagen über den Status von Service Providern (wie beispielsweise Zertifizierungsdiensteanbieter) zu treffen. Dieser Leitfaden beschreibt die für Applikationsbetreiber notwendigen Schritte zur Integration bzw. zur Verwendung von TSL in MOA-SP. Dies umfasst einen Überblick über die Einbindung von TSL in MOA-SP, eine detaillierte Konfigurations-Beschreibung für MOA-SP und zeigt eine beispielhafte Anwendung.

E-Government Innovationszentrum
Inffeldgasse 16/a, A-8010 Graz
Tel. +43 316 873 5514
Fax. +43 316 873 5520
E-Mail post@egiz.gv.at
www.egiz.gv.at

Das E-Government Innovationszentrum ist eine gemeinsame Einrichtung des Bundeskanzleramtes und der TU-Graz

Inhaltsverzeichnis

Abbildungsverzeichnis

1 Einleitung

1.1 Begriffsdefinitionen und Abkürzungen

In diesem Dokument werden die folgenden Abkürzungen verwendet:

ETSI	European Telecommunications Standards Institute
MOA	Module für Online Applikationen
MOA-SP	MOA Signaturprüfung
QC	Qualified Certificate
SSCD	Secure Signature Creation Device
TSL	Trust-Service Status Listen
ZDA	Zertifzierungsdiensteanbieter

1.2 Inhalt

Trust-Service Status Listen (TSL) sind ein ETSI Standard der es erlaubt Aussagen über den Status von Service Providern (wie beispielsweise Zertifizierungsdiensteanbieter) zu treffen. Das ermöglicht Anwendern der TSL Entscheidung über den Vertrauensstatus von Service Providern zu treffen, insbesondere in Zusammenhang mit der Zertifikatsüberprüfung. TSL ermöglichen die Entscheidung ob ein Zertifikat qualifiziert[1] ist bzw. ob die zugrundeliegende Signatur mittels einer sicheren Signaturerstellungseinheit[2] erstellt wurde. Von Seiten der EU wird eine EU-TSL herausgegeben[3], die auf den einzelnen länderspezifischen TSL referenziert. Mit Hilfe dieser EU-TSL ist es möglich, Vertrauensentscheidung im europäischen Umfeld zu treffen. Speziell im Hinblick auf die österreichische E-Government Gleichwertigkeitsverordnung, die EU Dienstleistungs-Richtlinie sowie den von der Europäischen Kommission definierten Mindestanforderungen für die grenzüberschreitende Verarbeitung von Dokumenten, ist dies eine wichtige Anforderung.

Dieser Leitfaden beschreibt die für Applikationsbetreiber notwendigen Schritte zur Integration bzw. zur Verwendung von TSL in MOA-SP. Dies umfasst einen Überblick über die Einbindung von TSL in MOA-SP sowie eine detaillierte Konfigurations-Beschreibung für MOA-SP. Des Weiteren enthält der Anhang eine beispielhafte `VerifyXMLSignatureResponse` sowie ein Auflistung aller Mitgliedsstaaten, die eine entsprechend korrekte TSL ausstellen und daher von MOA-SP unterstützt werden.

---

[1] QC = qualified certificate

[2] SSCD = secure signature creation device

[3] Siehe http://ec.europa.eu/information_society/policy/esignature/eu_legislation/trusted_lists/index_en.htm

2 Einbindung von TSL in MOA-SP

2.1 Einleitung

Abbildung 2.1 skizziert die Einbindung der TSL in MOA-SP. Zentrales Element ist die TSL Bibliothek. Diese Bibliothek übernimmt die Abwicklung mit der EU-TSL und speichert sämtliche Daten in einer internen Datenbank[4]. Innerhalb von MOA-SP wird nun auf die von der Library zur Verfügung gestellten Funktionen zugegriffen. Aufgrund der Implementierung der TSL Library muss für ein MOA-SP mit aktivierten TSL Java Version 5 eingesetzt werden. Hierbei besitzt die Bibliothek folgende zwei Hauptfunktionen:

- Aktualisierung von Vertrauensprofilen
- Überprüfung auf qualifiziertes Zertifikat und sichere Signaturerstellungseinheit

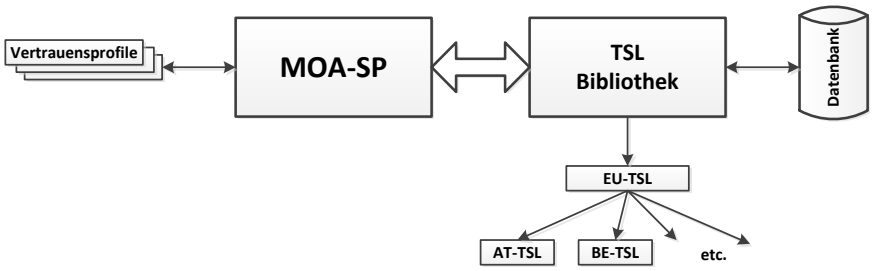

Abbildung 2.1 – Einbindung der TSL in MOA-SP

2.2 Aktualisierung von Vertrauensprofilen

MOA-SP definiert Vertrauensprofile um Ausstellern von bestimmten Zertifikaten zu vertrauen (die entsprechenden Aussteller-Zertifikate sind dabei im Vertrauensprofil hinterlegt). Mit der Einbindung der TSL Bibliothek kann für jedes Vertrauensprofil eine TSL-Unterstützung aktiviert werden. Diese TSL-Vertrauensprofile gelangen über eine Abfrage der EU-TSL zu den jeweiligen vertrauenswürdigen Aussteller-Zertifikaten, welche in das jeweilige Vertrauensprofil importiert werden. Dabei werden all jene Aussteller-Zertifikate importiert, die zum gegenwärtigen Zeitpunkt auf der EU-TSL bzw. den entsprechenden TSL der Mitgliedsstaaten befugt sind qualifizierte Zertifikate auszustellen und dessen Zertifizierungsdiensteanbieter unter dem ServiceLevel "accredited" oder "undersupervision" stehen. Ohne weitere Angabe werden die entsprechenden Zertifikate aller, auf der EU-TSL angeführten Länder, importiert. Über die MOA-SP Konfiguration kann jedoch eine Einschränkung auf bestimmte Länder erfolgen.

[4] Diese Datenbank ist eine SQLite Datenbank (d.h. die Datenbank ist in einer einzigen Datei gespeichert), die im TSL-Arbeitsverzeichnis gespeichert wird (Das Arbeitsverzeichnis ist dabei über die MOA-SP Konfiguration einstellbar – siehe folgenden Abschnitt).

Des Weiteren kann mittels der MOA-SP Konfiguration festgelegt werden in welchem Intervall der Import der Zertifikate von der EU-TSL erfolgen soll.

2.3 Überprüfung auf qualifiziertes Zertifikat und sichere Signaturerstellungseinheit

Die zweite wichtige Funktion ist die Überprüfung ob ein Signaturzertifikat qualifiziert[5] ist und ob die zugrundeliegende Signatur mit einer sicheren Signaturerstellungseinheit[6] erstellt wurde. Diese beiden Überprüfungen werden bei jeder Signaturprüfung durchgeführt (wenn für das angegeben Vertrauensprofil die TSL Unterstützung aktiviert ist) und das Resultat der Überprüfungen wird in der Antwort der Signaturprüfung retourniert. Eine bespielhafte Antwort finden Sie im Anhang 4.1.

Anmerkung: Bei Vertrauensprofilen ohne TSL Unterstützung erfolgt die Ermittlung auf qualifiziertes Zertifikat – wie bisher – direkt über das Signaturzertifikat selbst und nicht über die TSL. Eine Überprüfung auf sichere Signaturerstellungseinheit ist nicht möglich.

Anmerkung: Bei Vertrauensprofilen mit TSL Unterstützung wird bei der Ermittlung auf qualifiziertes Zertifikat nur das Resultat der Überprüfung via TSL herangezogen (und nicht über das Signaturzertifikat selbst).

[5] D.h. ob die Eigenschaft http://uri.etis.org/TrstSvc/Svctype/CA/QC auf der TSL gefunden werden konnte.

[6] D.h. ob die Eigenschaft http://uri.etis.org/TrstSvc/eSigDir-1999-93-ECTrustedList/SvcInfoExt/QCWithSSCD auf der TSL gefunden werden konnte.

3 MOA-SP Konfiguration

3.1 Einleitung

Dieser Abschnitt beschreibt die notwendigen Voraussetzung und die Konfiguration von MOA-SP zur Unterstützung von TSL.

Zusammenfassend sind folgende Voraussetzungen notwendig:

- MOA-SPSS mit Version 2.0.0 (mindestens)
- Java Version 5 (mindestens)

Des Weiteren sind folgende Konfigurationsschritte in MOA-ID erforderlich:

- Aktivieren der TSL Unterstützung für Vertrauensprofile
- Optionale allgemeine TSL Konfiguration und TSL Arbeitsverzeichnis

Diese Konfigurationsschritte werden im Folgenden näher beschrieben.

3.2 Allgemeine TSL Konfiguration und TSL Arbeitsverzeichnis

Die allgemeine TSL Konfiguration erfolgt im Element `cfg:SignatureVerification/ cfg:CertificateValidation/cfg:TSLConfiguration` der MOA-SPSS Konfiguration.

Folgende Konfigurationen können vorgenommen werden:

- `cfg:UpdateSchedule`: Dieses Element legt fest wann und in welchem Intervall die EU-TSL erneut eingelesen werden soll. Das Element `cfg:UpdateSchedule` besteht dabei aus folgenden Kind-Elementen:
  - `cfg:UpdateSchedule/cfg:StartTime`: Legt eine Startzeit im Format hh:mm:ss fest.
  - `cfg:UpdateSchedule/cfg:Period`: Legt das Intervall (in Millisekunden) fest, in welchem die EU-TSL erneut eingelesen werden soll.
- `cfg:WorkingDirectory`: Diese Element gibt einen Pfad zum Arbeitsverzeichnis (inkl. Lese- und Schreibrechte) für die TSL an. Enthält dieses Element eine relative Pfadangabe, so wird dieser relativ zum Verzeichnis in dem sich die MOA-SPSS Konfigurationsdatei befindet interpretiert.

Beispielkonfiguration:

```
<cfg:TSLConfiguration>
      <cfg:UpdateSchedule>
```

```
            <cfg:StartTime>02:00:00</cfg:StartTime>
            <cfg:Period>86400000</cfg:Period>
        </cfg:UpdateSchedule>
        <cfg:WorkingDirectory>tslworking</cfg:WorkingDirectory>
</cfg:TSLConfiguration>
```

Hinweis: Der Import der Zertifikate von der EU-TSL benötigt (je nach Verbindung) ca. 90-180 Sekunden. Als Startzeit sollte daher eine Zeit gewählt werden, zu der die Auslastung gering ist.

Die Angabe dieser TSL Konfiguration ist optional. Fehlt diese Konfiguration werden folgende Default-Werte herangezogen:

- `cfg:UpdateSchedule/cfg:StartTime`: 02:00:00
- `cfg:UpdateSchedule/cfg:Period`: 86400000 (= 1 Tag)
- `cfg:WorkingDirectory`: tslworking

Zusätzlich muss das TSL Arbeitsverzeichnis den Unterordner „trust“ aus der Beispielkonfiguration (siehe MOA-SP Release) beinhalten. In dessen Unterordner "eu" sind jene vertrauenswürdigen Zertifikate angegeben werden, mit denen die EU-TSL signiert ist.

Hinweis: Um die TSL Überprüfung zu aktivieren muss auch (zumindest) ein Vertrauensprofil mit TSL Überprüfung konfiguriert werden (siehe folgenden Abschnitt)

3.3 Aktivieren der TSL Unterstützung für Vertrauensprofile

Das Aktivieren der TSL Unterstützung für Vertrauensprofile erfolgt über das Element `cfg:SignatureVerification/cfg:CertificateValidation/cfg:PathValidation/cfg:TrustProfile` der MOA-SPSS Konfiguration. Die Konfiguration der Vertrauensprofile selbst erfolgt wie bisher. Die Aktivierung der TSL-Unterstützung für ein Vertrauensprofil erfolgt über das optionale Element `cfg:EUTSL` unterhalb des Elements `cfg:TrustProfile`. Das Element `cfg:EUTSL` aktiviert bei Vorhandensein die EU-TSL Unterstützung für dieses Vertrauensprofile. D.h. als Vertrauensanker werden jene Aussteller-Zertifikate herangezogen, die zum gegenwärtigen Zeitpunkt auf der EU-TSL bzw. den entsprechenden TSL der Mitgliedsstaaten befugt sind qualifizierte Zertifikate auszustellen und dessen Zertifizierungsdiensteanbieter unter dem ServiceLevel "accredited" oder "undersupervision" stehen. Des Weiteren werden bei TSL-aktivierten Vertrauensprofilen, die Überprüfung auf qualifiziertes Zertifikat (QC-Überprüfung) und die Überprüfung auf sichere Signaturerstellungseinheit (SSCD-Überprüfung) über die EU-TSL durchgeführt.

Zusätzliche kann ein optionales Kind-Element `cfg:CountrySelection` angegeben werden. Dieses Element definiert eine komma-separierte Liste an zweistelligen Länderkürzeln nach ISO 3166. Ist so eine Liste vorhanden, werden nur die Vertrauensanker der angegebenen Länder herangezogen.

Wichtig: Es können zusätzlich manuelle Vertrauensanker via cfg:TrustAnchorsLocation konfiguriert werden. Hierbei ist jedoch, insbesondere beim Hinzufügen von Enduser-Zertifikaten als Vertrauensanker, zu beachten, dass eine Überprüfung auf qualifiziertes Zertifikat bzw. sichere Signaturerstellungseinheit über die TSL gegebenenfalls nicht erfolgreich durchgeführt werden kann.

Wichtig: Bei aktivierter TSL-Unterstützung muss zumindest ein entsprechendes TSL Arbeitsverzeichnis vorhanden sein (siehe Abschnitt 3.2).

Beispielkonfiguration:

```
<cfg:TrustProfile>
  <cfg:Id>TestTSL</cfg:Id>
  <cfg:TrustAnchorsLocation>trustProfiles/testTSL</cfg:TrustAnchorsLocation>
  <!-- aktiviere TSL-Unterstützung für dieses Vertrauensprofil -->
  <cfg:EUTSL>
  <!-- Optional kann eine Länderliste mit zweistelligen Länderkürzeln
angegeben werden (d.h. nur die Vertrauensanker der angegeben Länder werden
importiert) -->
    <!--<cfg:CountrySelection>AT,BE</cfg:CountrySelection>-->
  </cfg:EUTSL>
</cfg:TrustProfile>
```

4 Anhang

4.1 Antwort Signaturprüfung

Web-Service Antwort auf eine Signaturprüfung mit Hinweis auf qualifiziertes Zertifikat (Element QualifiedCertificate), sichere Signaturerstellungseinheit (Element SecureSignatureCreationDevice) und der Ländercode des ZDA, der das Zertifikat ausgestellt hat (IssuerCountryCode).

Zusätzlich erhält das Element SecureSignatureCreationDevice ein Attribut Source, dass angibt ob die SSCD Information über die TSL (Source=TSL) oder das Zertifikat (Source=Certificate) bezogen wurde.

```
<VerifyXMLSignatureResponse xmlns="http://reference.e-
government.gv.at/namespace/moa/20020822#"
xmlns:dsig="http://www.w3.org/2000/09/xmldsig#">
      <SignerInfo>
            <dsig:X509Data>
<dsig:X509SubjectName>serialNumber=1234567891234,givenName=Max,SN=Mustermann,
CN=Max Mustermann,C=AT</dsig:X509SubjectName>
<dsig:X509IssuerSerial>
      <dsig:X509IssuerName>CN=a-sign-Premium-Sig-02,OU=a-sign-Premium-Sig-
02,O=A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr
GmbH,C=AT</dsig:X509IssuerName>
      <dsig:X509SerialNumber>456364</dsig:X509SerialNumber>
</dsig:X509IssuerSerial>
<dsig:X509Certificate>MIIEwjCCA6qg.../F2X6Y5skg==</dsig:X509Certificate>
                  <QualifiedCertificate/>
                  <SecureSignatureCreationDevice Source="Certificate"/>
                  <IssuerCountryCode>AT</IssuerCountryCode>
            </dsig:X509Data>
      </SignerInfo>
      <SignatureCheck>
            <Code>0</Code>
      </SignatureCheck>
      <SignatureManifestCheck>
            <Code>0</Code>
      </SignatureManifestCheck>
      <CertificateCheck>
            <Code>0</Code>
      </CertificateCheck>
</VerifyXMLSignatureResponse>
```

4.2 Unterstützte TSLs der Mitgliedsstaaten

Durch die sehr divergierende Umsetzung der TSL in den Mitgliedsstaaten, können nur standardkonforme TSLs unterstützt werden. Dies sind aktuell die TSLs folgender Mitgliedsstaaten:

- Österreich
- Tschechien
- Estland
- Ungarn
- Luxemburg
- Norwegen
- Slowakei

Alle anderen TSLs sind aus unterschiedlichen Gründen nicht standardkonform (nicht Schema konform, nicht signiert, etc.)

Dokumentenhistorie

Version	Datum	Autor(en)	Anmerkung
0.9	28.12.2013	K.Stranacher	Dokument erstellt.
1.0	17.03.2014	K.Stranacher	Version 1.0 fertiggestellt