

---

## OCSP-Responder für MOA-ID Single Sign-On (SSO)

Konzept

Dipl.-Ing. Martin Centner ([martin.centner@egiz.gv.at](mailto:martin.centner@egiz.gv.at))

---

### Zusammenfassung

*Sicheres HTTP-Session-Tracking und MOA-ID Single Sign-On (SSO)* [1] präsentiert ein Konzept zur Erweiterung von MOA-ID [2] zur Authentifizierung von SSL/TLS-Sessions mit Client-Zertifikaten. Aufbauend auf diesem Konzept wird hier ein Mechanismus vorgeschlagen, der die Freisaltung von SSL/TLS-Verbindungen für Applikationen erlaubt, in die eine entsprechende Funktionalität nicht direkt integriert werden kann, die jedoch OCSP RFC 2560 [3] zur Prüfung von Client-Zertifikaten unterstützen.

## 1 Einleitung

In *Sicheres HTTP-Session-Tracking und MOA-ID Single Sign-On (SSO)* [1] wurde eine Erweiterung zu MOA-ID vorgeschlagen, die die Authentifizierung von SSL- bzw. TLS-Verbindungen auf Basis von Client-Zertifikaten mit MOA-ID erlaubt. Dabei wird beim Log-On ein Zertifikat des Benutzers an eine MOA-ID-Session gebunden. Für die Dauer dieser Session, kann eine Online-Applikation, auf die unter Verwendung des selben Zertifikats zur Authentifizierung der SSL/TLS-Verbindung zugegriffen wurde, eine SAML-Assertion [4] für dieses Zertifikat als Bestätigung über die erfolgte Authentifizierung von MOA-ID abfragen. Diese SAML-Assertion enthält dann die Identitätsdaten (Personenbindung [5]) des Benutzers. Die Abfrage der SAML-Assertion erfolgt über eine SOAP-Schnittstelle [6] nach dem in [1] definierten *MOA-ID Assertion Query/Request Profile*.

Dieses Konzept ermöglicht die Authentifizierung über MOA-ID für beliebige Anwendungen bzw. Protokolle, die SSL- bzw. TLS-Verbindungen mit Client-Zertifikat-Authentifizierung erlauben. Allerdings setzt es voraus, dass die Funktionalität zur Abfrage der SAML-Assertions in die entsprechende Anwendung integriert werden kann.

## 2 OCSP-Responder für MOA-ID SSO

Um eine Freischaltung von SSL- bzw. TLS-Verbindungen über MOA-ID für Anwendungen zu ermöglichen, in die eine Funktionalität zur Abfrage von SAML-Assertions nicht ohne weiteres integriert werden kann, wird die Implementierung eines OCSP-Responders vorgeschlagen, der die SAML-Anfrage durchführt und einen entsprechenden Zertifikatsstatus zurück gibt. Bietet die Applikation die Möglichkeit, den Zertifikatsstatus per OCSP zu prüfen, dann kann damit die Freischaltung des Zugangs erfolgen. Damit ist es möglich den Zugang zur Applikation auf Benutzer einzuschränken, die sich erfolgreich bei MOA-ID authentifiziert haben.

Die Identität des Benutzers muss dann über die in der Anwendung oder im Protokoll vorgesehenen Authentifizierungsmechanismen festgestellt werden (z.B. Benutzername und Passwort), sofern das Zertifikat nicht personengebunden ist, da die Applikation aus der Abfrage des Zertifikatsstatus über OCSP keine entsprechende Information erhält.

Bei der Prüfung des Zertifikatsstatus sieht OCSP 1.0 die Identifikation des Zertifikats über die in RFC 2560 [3] definierte *CertID* vor:

```
CertID ::= SEQUENCE {
    hashAlgorithm      AlgorithmIdentifier,
    issuerNameHash     OCTET STRING, -- Hash of Issuer's DN
    issuerKeyHash      OCTET STRING, -- Hash of Issuers public key
    serialNumber       CertificateSerialNumber }
```

Da das zur Abfrage der SAML-Assertion im *MOA-ID Assertion Query/Request Profile* verwendete `<ds:X509Data>`-Element standardmäßig keine entsprechende Datenstruktur zur Identifikation eines Zertifikats vorsieht, muss hier eine entsprechende XML-Datenstruktur definiert und die MOA-ID-SOAP-Schnittstelle entsprechend erweitert werden.

```
1 <?xml version="1.0" encoding="UTF-8"?>
```

```
2 <xsd:schema xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns="http://draft.
   egiz.gv.at/namespace/moa-x509data/20060613" xmlns:xsd="http://www.w3.org
   /2001/XMLSchema" targetNamespace="http://draft.egiz.gv.at/namespace/moa-
   x509data/20060613">
3 <xsd:import namespace="http://www.w3.org/2000/09/xmldsig#" schemaLocation="
   http://www.w3.org/TR/2002/REC-xmldsig-core-20020212/xmldsig-core-schema.
   xsd"/>
4 <xsd:element name="CertID" type="CertIDType"/>
5 <xsd:complexType name="CertIDType">
6 <xsd:sequence>
7 <xsd:element ref="ds:DigestMethod"/>
8 <xsd:element name="IssuerNameHash" type="xsd:base64Binary"/>
9 <xsd:element name="IssuerKeyHash" type="xsd:base64Binary"/>
10 <xsd:element name="SerialNumber" type="xsd:integer"/>
11 </xsd:sequence>
12 </xsd:complexType>
13 </xsd:schema>
```

Erhält der OCSP-Responder eine Anfrage (OCSPRequest), erstellt er eine Anfrage nach dem *MOA-ID Assertion Query/Request Profile* mit dem oben definierten <CertID>-Element für eine SAML-Assertion für das entsprechende Zertifikat und schickt diese an die MOA-ID-SOAP-Schnittstelle. Gibt MOA-ID eine SAML-Assertion für das so identifizierte Zertifikat zurück, dann antwortet der OCSP-Responder mit dem Zertifikatsstatus good. Retourntiert MOA-ID keine SAML-Assertion so wird die Anfrage mit dem Zertifikatsstatus unknown oder bad beantwortet.

Welcher Zertifikatsstatus zurückgegeben werden soll, wenn keine SAML-Assertion für das entsprechende Zertifikat existiert, muss noch untersucht werden. Dabei ist zu klären, wie unterschiedliche Applikationen auf die entsprechenden Zertifikatsstati reagieren. Sollten sich verschiedene Applikationen hier unterschiedlich verhalten, muss eine entsprechende Möglichkeit zur individuellen Konfiguration vorgesehen werden.

### 3 Zusammenfassung

Das hier vorgestellte Konzept stellt eine Erweiterung zum Konzept MOA-ID Single Sign-On dar, die es beliebigen Applikationen, die die Prüfung des Zertifikatsstatus über OCSP unterstützen, erlaubt, den Zugang auf über MOA-ID authentifizierte Benutzer einzuschränken.

### Referenzen

- [1] CENTNER, M. ; RÖSSLER, T.: *Sicheres HTTP-Session-Tracking und MOA-ID Single Sign-On (SSO)*. Konzept. <http://demo.egiz.gv.at/session.html>
- [2] ARGE SPEZIFIKATION MOA: *Spezifikation Module für Online Applikationen (MOA) – ID*. Konvention. [http://www.cio.gv.at/onlineservices/basicmodules/moa-id/specification/MOA\\_ID\\_1.3\\_20060315.pdf](http://www.cio.gv.at/onlineservices/basicmodules/moa-id/specification/MOA_ID_1.3_20060315.pdf). Version: 1.3-20060315, Abruf: 27.5.2006
- [3] MYERS, M. ; ANKNEY, R. ; MALPANI, A. ; GALPERIN, S. ; ADAMS, C.: *X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP*. RFC 2560 (Proposed Standard). <http://www.ietf.org/rfc/rfc2560.txt>. Version: Juni 1999 (Request for Comments)

- 
- [4] S. CANTOR ET AL.: *Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0*. <http://docs.oasisopen.org/security/saml/v2.0/saml-core-2.0-os.pdf>. Version: 2.0, März 2005 (OASIS SSTC)
- [5] HOLLOSI, A. ; KARLINGER, G.: *XML-Definition der Personenbindung*. <http://www.buergerkarte.at/konzept/personenbindung/spezifikation/20050214/Personenbindung-20050214.pdf>. Version: 1.2.2, Abruf: 27.5.2006
- [6] S. CANTOR ET AL.: *Bindings for the OASIS Security Assertion Markup Language (SAML) V2.0*. <http://docs.oasisopen.org/security/saml/v2.0/saml-bindings-2.0-os.pdf>. Version: 2.0, März 2005 (OASIS SSTC)