Studiengesellschaft für Zusammenarbeit im Zahlungsverkehr
Tel. +43/1/505 32 80-0 • Fax: +43/1/505 32 80-77
Internet: www.stuzza.at • E-Mail: office@stuzza.at
A-1070 Wien, Stiftgasse 15-17

e-Identity Signaturprofil

Version: **1.0**
Datum: **30.06.2015**
Autor: **Thomas Pircher / ARZ Allgemeines Rechenzentrum GmbH**

Inhaltsverzeichnis

1. EINLEITUNG

Das vorliegende Dokument ist eine Ergänzung zur technischen Beschreibung des e-Identity Service [eIdentity]. Es spezifiziert das Signaturprofil für jene Protokollnachrichten, die beim Einsatz des e-Identity Service im Bereich des E-Government eine elektronische Unterschrift enthalten müssen.

Darunter fällt die *Initiierung der e-Identity Service Transaktion* durch den Händler, welche an die Kundenbank übermittelt wird. Diese Initiierung trägt die elektronische Signatur des Händlers. In weiterer Folge muss die *Confirmation zur e-Identity Service Transaktion* die elektronische Signatur der Kundenbank enthalten. Die *Statusabfrage zur e-Identity Service Transaktion* enthält wiederum die elektronische Signatur des Händlers.

Die elektronischen Signaturen sind nach [XMLDSIG] zu kodieren, und an die in [eIdentity] spezifizierten Positionen einzufügen. Die nachfolgenden Abschnitte beschreiben detailliert die Vorgaben für alle Signaturen.

1.1. Referenzen

[EC14N]
John Boyer, Donald Eastlake und Joseph Reagle: Exclusive XML Canonicalization Version 1.0. W3C Recommendation, Juli 2002. http://www.w3.org/TR/2002/REC-xml-exc-c14n-20020718/

[eIdentity]
Alexander Schilling, Joachim Geisler, Markus Brejla und Thomas Pircher: e-Identity Pflichtenheft, Version 1.0.4, Juni 2015. http://www.stuzza.at

[XMLDSIG]
Donald Eastlake, Joseph Reagle und David Solo: XML-Signature Syntax and Processing. W3C Recommendation, Februar 2002. http://www.w3.org/TR/2002/REC-xmldsig-core-20020212

[ISIS-MTT]
Brauckmann, Jürgen et. al: ISIS-MTT-Specification. Version 1.0.2, July 19th, 2002. http://www.teletrust.de/Dokumente%5Cag8_isis-mtt-corespec-v1.0.2.pdf

1.2. Verwendete XML Namenraum-Präfixe

In den nachfolgenden Kapiteln werden zur Beschreibung der Protokollelemente folgende Namenraum-Präfixe verwendet:

Präfix	Namenraum

eIdentity	http://www.stuzza.at/namespaces/eIdentity/2014
dsig	http://www.w3.org/2000/09/xmldsig#

2. ANFORDERUNGEN AN EINE TRUSTED CA

Folgende Anforderungen müssen an eine Trusted CA erfüllt werden:

- Einsatz von X.509 v3 Zertifikaten
- Das Zertifikat muss die Zertifikatserweiterung CRL Distribution Points aufweisen. In dieser Zertifikatserweiterung muss zumindest ein LDAP Distribution Point enthalten sein. Weitere Distribution Points (z.B. http oder https) sind zulässig.
- Die Revozierungsliste (CRL) für das Zertifikat sowie für die CA-Zertifikate muss per LDAP von einem Server des Zertifizierungsdienstanbieters geladen werden können. Alle dazu notwendigen Informationen (LDAP-Host, LDAP-Port, LDAP-DN, ggf. LDAP-User und LDAP Passwort, ggf. weitere LDAP-Attribute) müssen dem Scheme Operator bekannt gegeben werden.
    - Beispiel: ldap://ldap-test.a-trust.at:389/ou=TrustTest-VSC-01,o=A-Trust,c=AT?certificaterevocationlist?
- Zertifikate und CA-Zertifikate müssen per LDAP von einem Server des Zertifizierungsdienstanbieters durch Identifikation des Zertifikats mittels IssuerDN und SerialNumber geladen werden können. Alle dazu notwendigen Informationen (LDAP-Host, LDAP-Port, LDAP-DN, ggf. LDAP-User und LDAP Passwort, ggf. weitere LDAP-Attribute) müssen dem Scheme Operator bekannt gegeben werden.
    - Beispiel: ldap://ldap-test.a-trust.at:389/eidCertificateSerialNumber=1234, ou=a-sign-Premium-Sig-01,o=A-Trust,c=AT?userCertificate;binary?
- Die Zertifikatskettenprüfung für das Zertifikat muss entsprechend dem Gültigkeitsmodell nach [ISIS-MTT], Teil 5 durchgeführt werden können.
- Zu jeder elektronischen Signatur einer e-Identity Nachricht muss der Händler bzw. die Kundenbank zumindest das Signatorzertifikat mitsenden, um die Zertifikatskettenbildung zu erleichtern. Desweiteren wird empfohlen, auch die zur Bildung einer vollständigen Zertifikatskette benötigten Zertifikate bis hin zu einem Wurzelzertifikat mit der Signatur mitzusenden.
- Certification Practice Statement und Certificate Policy der vom Creditor verwendeten CA müssen dem Scheme Operator zugänglich gemacht werden; auf Grund dieser Informationen wird eine CA vom Scheme Operator akzeptiert oder abgelehnt.

3. INITIIERUNG DER E-IDENTITY SERVICE TRANSAKTION

Für eine sorgfältige und im Nachhinein belegbare Authentisierung des Händlers muss die Initiierung der e-Identity Service Transaktion wahlweise einen SHA256Fingerprint nach [eIdentity] oder eine elektronische Unterschrift des Händlers enthalten.

Um dem Händler das Erzeugen der elektronischen Unterschrift möglichst einfach zu machen, muss der gesamte Transportcontainer eIdentity:IdentityServiceInitiationRequest signiert werden.

Als Kanonisierungsalgorithmus muss Exclusive Canonical XML Version 1.0 [EC14N] verwendet werden, und zwar sowohl für die Kanonisierung von dsig:SignedInfo, als auch zur Kanonisierung der zu unterschreibenden Protokollnachricht.

Damit wird es möglich, eine Enveloped Signature zu erzeugen, welche nur eine einzige Transformation benötigt, und zwar eine Enveloped Signature Transformation (vergleiche das nachfolgende Beispiel).

An Informationen zum verwendeten Signaturschlüssel muss in dsig:KeyInfo zumindest das Signatorzertifikat selbst (als dsig:X509Certificate) enthalten sein. Es wird empfohlen, darüber hinaus auch die zur Bildung einer vollständigen Zertifikatskette notwendigen Zertifikate anzugeben (als zusätzliche Elemente vom Typ dsig:X509Certificate).

3.1. Beispiel

Das folgende Beispiel zeigt eine signierte e-Identity Initiierung eIdentity:IdentityServiceInitiationRequest.

Um die Lesbarkeit zu verbessern, wurden der Signaturwert sowie das Signatorzertifikat ausgeblendet.

```
<?xml version="1.0" encoding="UTF-8"?>
<eIdentity:IdentityServiceInitiationRequest xmlns:dsig="http://www.w3.org/2000/09/xmldsig#"
xmlns:eIdentity="http://www.stuzza.at/namespaces/eIdentity/2014"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://www.stuzza.at/namespaces/eIdentity/2014 eIdentityService_v1.0.xsd
">
 <eIdentity:MsgHeader>
  <eIdentity:MsgId>ARZTAT22XXX_120674XXXXXXX_123456789</eIdentity:MsgId>
  <eIdentity:CreDtTm>2014-10-26T12:00:00Z</eIdentity:CreDtTm>
 </eIdentity:MsgHeader>
 <eIdentity:MerchantData>
  <eIdentity:ReturnUrl>https://shop.example.net/eIdentity-landing</eIdentity:ReturnUrl>
  <eIdentity:ConfirmationUrl>https://routing.example.net/eIdentity-
confirmation</eIdentity:ConfirmationUrl>
  <eIdentity:MerchantName>Mustershop D.O.C. Brown</eIdentity:MerchantName>
 </eIdentity:MerchantData>
 <eIdentity:IdentityData>
  <eIdentity:FirstName>Max</eIdentity:FirstName>
  <eIdentity:LastName>Mustermann</eIdentity:LastName>
  <eIdentity:DateOfBirth>1955-11-12</eIdentity:DateOfBirth>
  <eIdentity:Street>Tschamlerstraße 2</eIdentity:Street>
  <eIdentity:ZipCode>6020</eIdentity:ZipCode>
  <eIdentity:Town>Innsbruck</eIdentity:Town>
  <eIdentity:Country>AT</eIdentity:Country>
 </eIdentity:IdentityData>
 <eIdentity:AuthenticationDetails>
  <eIdentity:UserId>eIdentitySchemeOperator</eIdentity:UserId>
  <dsig:Signature Id="hotVault" xmlns:dsig="http://www.w3.org/2000/09/xmldsig#">
   <dsig:SignedInfo>
    <dsig:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
    <dsig:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />
    <dsig:Reference Id="reference-data-0" URI="">
     <dsig:Transforms>
      <dsig:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
     </dsig:Transforms>
     <dsig:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
```

```
      <dsig:DigestValue>FochNxwXsYw4/xE8XBb24vRwINI=</dsig:DigestValue>
     </dsig:Reference>
    </dsig:SignedInfo>
    <dsig:SignatureValue><!-- Signaturwert --></dsig:SignatureValue>
    <dsig:KeyInfo>
     <dsig:X509Data>
      <dsig:X509Certificate><!-- Zertifikat --></dsig:X509Certificate>
     </dsig:X509Data>
    </dsig:KeyInfo>
   </dsig:Signature>
  </eIdentity:AuthenticationDetails>
</eIdentity:IdentityServiceInitiationRequest>
```

4. CONFIRMATION ZUR E-IDENTITY SERVICE TRANSAKTION

Damit die Confirmation der Kundenbank vom Händler dauerhaft im Sinne eines elektronischen Belegs verwendet werden kann, muss sie eine elektronische Signatur der Kundenbank aufweisen.

Um der Bank das Erzeugen der elektronischen Unterschrift möglichst einfach zu machen, muss der gesamte Transportcontainer eIdentity:IdentityServiceConfirmation signiert werden.

Als Kanonisierungsalgorithmus muss Exclusive XML Canonicalisation [EC14N] verwendet werden, und zwar sowohl für die Kanonisierung von dsig:SignedInfo, als auch zur Kanonisierung der zu unterschreibenden Protokollnachricht.

An Informationen zum verwendeten Signaturschlüssel muss in dsig:KeyInfo zumindest das Signatorzertifikat selbst (als dsig:X509Certificate) enthalten sein. Es wird empfohlen, darüber hinaus auch die zur Bildung einer vollständigen Zertifikatskette notwendigen Zertifikate anzugeben (als zusätzliche Elemente vom Typ dsig:X509Certificate).

4.1. Beispiel

Das nachfolgende Beispiel zeigt eine signierte Confirmation eIdentity:IdentityServiceConfirmation.

Um die Lesbarkeit zu verbessern, wurden der Signaturwert sowie das Signatorzertifikat ausgeblendet.

```
<?xml version="1.0" encoding="UTF-8"?>
<eIdentity:IdentityServiceConfirmation xmlns:dsig="http://www.w3.org/2000/09/xmldsig#"
 xmlns:eIdentity="http://www.stuzza.at/namespaces/eIdentity/2014"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:schemaLocation="http://www.stuzza.at/namespaces/eIdentity/2014 eIdentityService_v1.0.xsd
">
 <eIdentity:MsgHeader>
  <eIdentity:MsgId>ARZTAT22XXX_120674XXXXXXX_123456789</eIdentity:MsgId>
  <eIdentity:CreDtTm>2014-10-26T12:00:00Z</eIdentity:CreDtTm>
 </eIdentity:MsgHeader>
 <eIdentity:VerificationDetails>
  <eIdentity:FirstName>OK</eIdentity:FirstName>
  <eIdentity:LastName>OK</eIdentity:LastName>
  <eIdentity:DateOfBirth>OK</eIdentity:DateOfBirth>
  <eIdentity:Street>OK</eIdentity:Street>
  <eIdentity:ZipCode>OK</eIdentity:ZipCode>
  <eIdentity:Town>OK</eIdentity:Town>
  <eIdentity:Country>OK</eIdentity:Country>
 </eIdentity:VerificationDetails>
 <eIdentity:ResponseStatus from="BANK">
```

```
  <eIdentity:ResponseCode>100</eIdentity:ResponseCode>
 </eIdentity:ResponseStatus>
 <eIdentity:BankId>VBOEATWWAPO</eIdentity:BankId>
 <dsig:Signature Id="hotVault" xmlns:dsig="http://www.w3.org/2000/09/xmldsig#">
  <dsig:SignedInfo>
   <dsig:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
   <dsig:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />
   <dsig:Reference Id="reference-data-0" URI="">
    <dsig:Transforms>
     <dsig:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
    </dsig:Transforms>
    <dsig:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
    <dsig:DigestValue>FochNxwXsYw4/xE8XBb24vRwINI=</dsig:DigestValue>
   </dsig:Reference>
  </dsig:SignedInfo>
  <dsig:SignatureValue><!-- Signaturwert --></dsig:SignatureValue>
  <dsig:KeyInfo>
   <dsig:X509Data>
    <dsig:X509Certificate><!-- Zertifikat --></dsig:X509Certificate>
   </dsig:X509Data>
  </dsig:KeyInfo>
 </dsig:Signature>
</eIdentity:IdentityServiceConfirmation>
```

5. STATUSMELDUNG ZUR E-IDENTITY SERVICE TRANSAKTION

Damit nur ein autorisierter Händler für ihn gültige Verifikationsergebnisse abfragen kann, muss die Statusabfrage wahlweise einen SHA256Fingerprint nach [eIdentity] oder eine elektronische Signatur des Händlers aufweisen.

Um dem Händler das Erzeugen der elektronischen Unterschrift möglichst einfach zu machen, muss der gesamte Transportcontainer eIdentity:IdentityServiceStatusRequest signiert werden.

Als Kanonisierungsalgorithmus muss Exclusive XML Canonicalisation [EC14N] verwendet werden, und zwar sowohl für die Kanonisierung von dsig:SignedInfo, als auch zur Kanonisierung der zu unterschreibenden Protokollnachricht.

An Informationen zum verwendeten Signaturschlüssel muss in dsig:KeyInfo zumindest das Signatorzertifikat selbst (als dsig:X509Certificate) enthalten sein. Es wird empfohlen, darüber hinaus auch die zur Bildung einer vollständigen Zertifikatskette notwendigen Zertifikate anzugeben (als zusätzliche Elemente vom Typ dsig:X509Certificate).

5.1. Beispiel

Das nachfolgende Beispiel zeigt eine signierte Statusabfrage eIdentity:IdentityServiceStatusRequest.

Um die Lesbarkeit zu verbessern, wurden der Signaturwert sowie das Signatorzertifikat ausgeblendet.

```
<?xml version="1.0" encoding="UTF-8"?>
<eIdentity:IdentityServiceStatusRequest xmlns:dsig="http://www.w3.org/2000/09/xmldsig#"
xmlns:eIdentity="http://www.stuzza.at/namespaces/eIdentity/2014"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://www.stuzza.at/namespaces/eIdentity/2014 eIdentityService_v1.0.xsd
">
 <eIdentity:MsgHeader>
  <eIdentity:MsgId>ARZTAT22XXX_120674XXXXXXX_123456789</eIdentity:MsgId>
  <eIdentity:CreDtTm>2014-10-26T12:00:00Z</eIdentity:CreDtTm>
```

```
 </eIdentity:MsgHeader>
 <eIdentity:StatusReference>eisI1QW7IMV3</eIdentity:StatusReference>
 <eIdentity:AuthenticationDetails>
  <eIdentity:UserId>eIdentitySchemeOperator</eIdentity:UserId>
  <dsig:Signature Id="hotVault" xmlns:dsig="http://www.w3.org/2000/09/xmldsig#">
   <dsig:SignedInfo>
    <dsig:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
    <dsig:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />
    <dsig:Reference Id="reference-data-0" URI="">
     <dsig:Transforms>
      <dsig:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
     </dsig:Transforms>
     <dsig:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
     <dsig:DigestValue>FochNxwXsYw4/xE8XBb24vRwINI=</dsig:DigestValue>
    </dsig:Reference>
   </dsig:SignedInfo>
   <dsig:SignatureValue><!-- Signaturwert --></dsig:SignatureValue>
   <dsig:KeyInfo>
    <dsig:X509Data>
     <dsig:X509Certificate><!-- Zertifikat --></dsig:X509Certificate>
    </dsig:X509Data>
   </dsig:KeyInfo>
  </dsig:Signature>
 </eIdentity:AuthenticationDetails>
</eIdentity:IdentityServiceStatusRequest>
```