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 signature-profile

Version: **1.0**
Date: **18.12.2015**
Author: **Thomas Pircher / ARZ Allgemeines Rechenzentrum GmbH**

Table of content

1. INTRODUCTION

This document is an addendum to the standard implementation guideline of the e-Identity-Service (e-id). It specifies the signature-profile for those protocol-messages that have to contain an electronic signature for e-id used for e-Government.

This includes the initiation of an e-id transaction by the merchant, which is transferred to the issuer-bank. The initiation contains the electronic signature of the merchant. Subsequently the confirmation of the issuer-bank for the e-id transaction contains the electronic signature of the issuer-bank. The status-request for an e-id transaction again contains the electronic signature of the merchant.

The electronic signatures have to be coded using [XMLDSIG] and positioned like specified in [eIdentity]. The following chapters describe the detailed specifications for all signatures.

1.1. References

[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. XML namespace-prefix

In these chapters the following namespace-prefixes are used to describe the protocol-elements:

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

2. REQUIREMENTS FOR A TRUSTED CA

The following requirements have to be met by a trusted CA:

- Usage of X.509 v3 certificates
- The certificate has to feature the certificate-extension CRL Distribution Points. The certificate-extension has to contain at least one LDAP Distribution Point. Further distribution points (e. g. http or https) are valid.
- The revocation-list (CRL) for the certificate as well as the CA-certificate has to be loadable from a server of the certification-service-provider by LDAP. All necessary information for that (LDAP-Host, LDAP-Port, LDAP-DN, probably LDAP-User and LDAP-Password or other LDAP-attributes) has to be notified to the scheme-operator.
    - Example: ldap://ldap-test.a-trust.at:389/ou=TrustTest-VSC-01,o=A-Trust,c=AT?certificaterevocationlist?
- The certificates and CA-certificates must be loadable by the server of the certification-service-provider via LDAP using IssuerDN and SerialNumber. All necessary information for that (LDAP-Host, LDAP-Port, LDAP-DN, probably LDAP-User and LDAP-Password or other LDAP-attributes) has to be notified to the scheme-operator.
    - Example: ldap://ldap-test.a-trust.at:389/eidCertificateSerialNumber=1234, ou=a-sign-Premium-Sig-01,o=A-Trust,c=AT?userCertificate;binary?
- The check of the certificate-chain for the certificate has to be performed according to the model of [ISIS-MTT], part 5.
- Together with the electronic signature of an e-id-message a merchant or issuer-bank has to send at least the signatory-certificate to facilitate the creation of the certificate-chain. Furthermore it is recommended to additionally send the necessary certificates down to the root-certificate for the creation of an entire certificate-chain.
- Certification Practice Statement and Certificate Policy of the CA used by the creditor have to be accessible by the scheme-operator. Based on this information a CA is either accepted or declined by the scheme-operator.

3. INITIATION OF E-IDENTITY SERVICE TRANSACTIONS

To be able to authenticate the initiation of an e-id transaction of a merchant in retrospect it must either contain a SHA256Fingerprint regarding [eIdentity] or an electronic signature of the merchant.

To make it as simple as possible for a merchant to create an electronic signature the whole transport-container eIdentity:IdentityServiceInitiationRequest needs to be signed.

Exclusive Canonical XML Version 1.0 [EC14N] has to be used as a canonicalization algorithm for the canonicalization of dsig:SignedInfo as well as for the canonicalization of the protocol-message to be signed.

By that it is possible to create an Enveloped Signature which only needs one transformation which is the Enveloped Signature Transformation (see the following example).

At least the signatory-certificate (as dsig:X509Certificate) has to be included into dsig:KeyInfo for information about the used signature-key. It is recommended to state the necessary certificates for the creation of an entire certificate-chain (as additional elements of type dsig:X509Certificate).

3.1. Example

The following example shows a signed e-id initiation eIdentity:IdentityServiceInitiationRequest.

To increase readability the signature-values as well as the signatory-certificate are not included.

```
<?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 OF E-IDENTITY SERVICE TRANSACTION

To be able to use the confirmation of the issuer-bank as an electronic record it has to contain the electronic signature of the issuer-bank.

To make it as simple as possible for the issuer-bank to create an electronic signature the whole transport-container eIdentity:IdentityServiceConfirmation needs to be signed.

Exclusive Canonical XML [EC14N] has to be used as a canonicalization algorithm for the canonicalization of dsig:SignedInfo as well as for the canonicalization of the protocol-message to be signed.

At least the signatory-certificate (as dsig:X509Certificate) has to be included into dsig:KeyInfo for information about the used signature-key. It is recommended to state the necessary certificates for the creation of an entire certificate-chain (as additional elements of type dsig:X509Certificate).

4.1. Example

The following example shows a signed e-id confirmation eIdentity:IdentityServiceConfirmation.

To increase readability the signature-values as well as the signatory-certificate are not included.

```
<?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. STATUS-MESSAGE FOR E-IDENTITY SERVICE TRANSACTION

To ensure that only authorised merchants are able to request verification-results the status-message needs to include a SHA256Fingerprint regarding [eIdentity] or the electronic signature of the merchant.

To make it as simple as possible for the merchant to create an electronic signature the whole transport-container eIdentity:IdentityServiceStatusRequest needs to be signed.

Exclusive XML Cononicalisation [EC14N] has to be used as a canonicalization algorithm for the canonicalization of dsig:SignedInfo as well as for the canonicalization of the protocol-message to be signed.

At least the signatory-certificate (as dsig:X509Certificate) has to be included into dsig:KeyInfo for information about the used signature-key. It is recommended to state the necessary certificates for the creation of an entire certificate-chain (as additional elements of type dsig:X509Certificate).

5.1. Example

The following example shows a signed e-id status-request eIdentity:IdentityServiceStatusRequest.

To increase readability the signature-values as well as the signatory-certificate are not included.

```
<?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>
```