**Designation**: XML definition of the person identity link

**Short name**: Person identity link

**Version**: 1.2.2

**Date**: 2005-02-14

**Document class**: Convention

**Document status**: Public draft

**Brief description**: The person identity link is an integral part of the Citizen Card concept. It is a structure signed by the issuing public authority that assigns a unique identification feature of a person (for example a registration number) to one or more certificates belonging to this person.

As such, the person identity link can be used for the unique, automated identification of a person when that person approaches the public authority during the course of a procedure.

This paper describes the XML specification of the person identity link.

**Authors**: Arno Hollosi, arno.hollosi@cio.gv.at
Gregor Karlinger, gregor.karlinger@cio.gv.at

**Work group**: Federal Staff Unit for ICT Strategy, Technology and Standards
## Table of contents

1 Introduction and basic data ......................................................................................................... 3
2 Basic XML structure .................................................................................................................. 4
   2.1 SAML assertion (framework structure) ............................................................................. 4
       2.1.1 Example .................................................................................................................. 5
   2.2 SAML Attribute Statement .............................................................................................. 5
       2.2.1 Personal data .......................................................................................................... 5
       2.2.2 Attributes .............................................................................................................. 7
       2.2.3 Example ................................................................................................................ 7
   2.3 The electronic signature ..................................................................................................... 8
3 Encoding rules .......................................................................................................................... 10
4 Compressed representation ...................................................................................................... 11
   4.1 ASN.1 specification ....................................................................................................... 11
       4.1.1 Explanation of individual fields ......................................................................... 13
5 Example .................................................................................................................................... 14
   5.1 Example of a person identity link .................................................................................. 14
   5.2 Example of compressed representation ....................................................................... 15
References ................................................................................................................................... 17
History ......................................................................................................................................... 18

This document uses the following keywords to categorise requirements: MUST, MUST NOT, REQUIRED, SHOULD, SHOULD NOT, RECOMMENDED, MAY and OPTIONAL. The interpretation of these keywords is set down in RFC 2119.
1 Introduction and basic data

As part of electronic procedures, it is important for the public authority to be able to identify a person clearly. As used for the electronic signature, certificates are not sufficient for automated, unique identification because they usually only contain the person’s name. However, a person’s name is not enough for a unique identification.

This is why the person is identified with the sourcePIN (source identification number), which remains unchanged for the person’s lifetime.

In addition to the sourcePIN (a person’s identification), the person identity link also contains a unique identifier for each certificate to which the sourcePIN is assigned. This ensures a cryptographically secured link between the electronic signature of a person (the signatory) and a unique identification feature for this person.
2 Basic XML structure

The basic XML structure is based on the Security Assertion Markup Language [SAML 1.0] defined by OASIS (Organization for the Advancement of Structured Information Standards). [SAML 1.0] defines XML structures that contain assertions of particular matters or relations between subjects made by third parties (so-called authorities).

In the case of the person identity link, the SourcePIN Register Authority confirms the link between the sourcePIN and one or more certificates.

The SourcePIN Register Authority cryptographically secures this link against change by means of its signature. The signature thus guarantees the authenticity of the data and identifies the issuing public authority with its certificate.

The following standards and specifications are used for the person identity link:

- Security Assertion Markup Language (SAML) – OASIS: Framework structure
  Namespace: urn:oasis:names:tc:SAML:1.0:assertion, prefix: saml
- XML Digital Signatures (XMLDSIG) – W3C: Electronic signatures
  Namespace: http://www.w3.org/2000/09/xmldsig#, prefix: dsig
- PersonData – CIO Austria: Placeholder for personal data
- Proposal for a compressed person identity link – CIO Austria: Schema for the compressed storage of a person identity link
  Namespace: http://www.buergerkarte.at/namespaces/personenbindung/20020506#, prefix: il

2.1 SAML assertion (framework structure)

The person identity link is based on the saml:Assertion structure from [SAML 1.0].

The saml:Assertion element contains the following mandatory attributes:

<table>
<thead>
<tr>
<th>Name</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MajorVersion</td>
<td>1</td>
<td>SAML version number</td>
</tr>
<tr>
<td>MinorVersion</td>
<td>0</td>
<td>SAML version number</td>
</tr>
<tr>
<td>AssertionID</td>
<td>xs:string</td>
<td>ID for the assertion</td>
</tr>
<tr>
<td>Issuer</td>
<td>xs:string</td>
<td>Name of the assertion issuer</td>
</tr>
<tr>
<td>IssueInstant</td>
<td>xs:dateTime</td>
<td>Time at which the person identity link was issued.</td>
</tr>
</tbody>
</table>

The AssertionID SHOULD be unique beyond the boundaries of the application. It is RECOMMENDED that the domain name of the issuing public authority plus a serial number and the current time be used (e.g. bka.gv.at+2004-02-24T12:00:00.000Z).

Issuer identifies the issuer of saml:Assertion and, in the context of the person identity link, MUST be a URL that refers to a resource that contains the name, address and signature certificate of the issuer, as well as other optional information. This information is usually
summarised on a publically available web page. Since the specified URL can be included in various programs as a parameter, it SHOULD remain unchanged over a long period.

Furthermore, in the context of the person identity link, precisely the following elements are to be included in the saml:Assertion structure on a mandatory basis:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>saml:AttributeStatement</td>
<td>Contains the core data of the person identity link.</td>
</tr>
<tr>
<td>dsig:Signature</td>
<td>The electronic signature of the issuer of the link</td>
</tr>
</tbody>
</table>

### 2.1.1 Example

```xml
<?xml version="1.0" encoding="UTF-8"?>
<saml:Assertion
  AssertionID="bka.gv.at+2004-02-24T12:00:00.000Z"
  IssueInstant="2004-02-24T12:00:00.000Z"
  Issuer="http://www.bka.gv.at/datenschutz/Stammzahlenregisterbehoerde"
  MajorVersion="1"
  MinorVersion="0"
  <saml:AttributeStatement>
    ...
  </saml:AttributeStatement>
  <dsig:Signature>
    ...
  </dsig:Signature>
</saml:Assertion>
```

### 2.2 SAML Attribute Statement

The incorporated saml:AttributeStatement contains the core data from the person identity link.

- **saml:Subject** contains the person’s data in the form of the personal data structure [PDat], while the saml:Attribute elements each contain a public key in the form of a dsig:KeyValue subelement as the identifier for a certificate to be assigned.

#### 2.2.1 Personal data

The saml:Subject structure contains precisely the element saml:SubjectConfirmation. In this element, saml:ConfirmationMethod is set to the value...
The pr:Person element type MUST be pr:PhysicalPersonType and MUST contain precisely the following data:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>pr:Identification</td>
<td>The person’s sourcePIN contains precisely one pr:Type element containing urn:publicid:gv.at:baseid, and one pr:Value element containing the base64-encoded sourcePIN as a string value.</td>
</tr>
<tr>
<td>pr:Name</td>
<td>The name of the natural person contains precisely one pr:GivenName element (first name) and one pr:FamilyName element with the attribute primary=“undefined” (surname). Multiple first names or surnames MUST be consolidated in a single element.</td>
</tr>
<tr>
<td>pr:DateOfBirth</td>
<td>The person’s date of birth</td>
</tr>
</tbody>
</table>

Example

```xml
<pr:Person
  xsi:type="pr:PhysicalPersonType"
  xmlns:pr="http://reference.e-government.gv.at/namespace/persondata/20020228#">
  <pr:Identification>
    <pr:Value>MDEyMzQ1Njc4OWFiY2RlZg==</pr:Value>
    <pr:Type>urn:publicid:gv.at:baseid</pr:Type>
  </pr:Identification>
  <pr:Identification>
    <pr:Name>
      <pr:GivenName>Herbert</pr:GivenName>
      <pr:FamilyName primary="undefined">Gramgebeugt</pr:FamilyName>
    </pr:Name>
  </pr:Identification>
  <pr:DateOfBirth>1950-12-31</pr:DateOfBirth>
</pr:Person>
```

2.2.1.2 Personal data for non-natural persons

Personal data for non-natural persons (companies, associations, etc.) will be defined in a later version of this document.

---

1 The sender (the public authority) guarantees the content. The recipient cannot check the truth of the core data (not to be confused with verifying the authenticity of the data using the public authority’s signature).
2.2.2 Attributes

2.2.2.1 Attributes for natural persons

The saml:Attribute structure MUST occur at least once, but CAN also occur several times and contains a public key of the person in the form of dsig:KeyValue subelements, in other words dsig:RSAKeyValue, dsig:DSAKeyValue or xsd:any (for storing ECDSA key values).

The fixed value CitizenPublicKey is to be specified in the AttributeName attribute, while the fixed value urn:publicid:gv.at:namespaces:identitylink:1.2 is to be specified in the AttributeNameSpace attribute.

2.2.2.2 Attributes for non-natural persons

Attributes for non-natural persons (companies, associations, etc.) are still to be defined.

2.2.3 Example

```xml
<saml:AttributeStatement
 xmlns:pr="http://reference.e-government.gv.at/namespaces/persondata/20020228#"
 xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
 <saml:Subject>
  <saml:SubjectConfirmation>
   <saml:ConfirmationMethod>
    urn:oasis:names:tc:SAML:1.0:cm:sender-vouches</saml:ConfirmationMethod>
   <saml:SubjectConfirmationData>
    <pr:Person xsi:type="pr:PhysicalPersonType">
     <pr:Identification>
      <pr:Value>mDEyMzQ1Njc4OWFiY2RlZg==</pr:Value>
      <pr:Type>urn:publicid:gv.at:baseid</pr:Type>
     </pr:Identification>
     <pr:Name>
      <pr:GivenName>Herbert</pr:GivenName>
      <pr:FamilyName primary="undefined">Gramgebeugt</pr:FamilyName>
     </pr:Name>
     <pr:DateOfBirth>1950-12-31</pr:DateOfBirth>
    </pr:Person>
   </saml:SubjectConfirmationData>
  </saml:SubjectConfirmation>
 </saml:Subject>
 <saml:Attribute
  AttributeName="CitizenPublicKey"
  AttributeNamespace="urn:publicid:gv.at:namespaces:identitylink:1.2">
  <saml:AttributeValue>
   <dsig:RSAKeyValue xmlns:dsig="http://www.w3.org/2000/09/xmldsig#">
    <dsig:Modulus>...</dsig:Modulus>
    <dsig:Exponent>dG+9</dsig:Exponent>
   </dsig:RSAKeyValue>
  </saml:AttributeValue>
 </saml:Attribute>
 <saml:Attribute
  AttributeName="CitizenPublicKey"
  AttributeNamespace="urn:publicid:gv.at:namespaces:identitylink:1.2">
  <saml:AttributeValue>
   <dsig:RSAKeyValue xmlns:dsig="http://www.w3.org/2000/09/xmldsig#">
    <dsig:Modulus>...</dsig:Modulus>
    <dsig:Exponent>q9Hf8w1UM3mKwROcuWiz6Aucq8</dsig:Exponent>
   </dsig:RSAKeyValue>
  </saml:AttributeValue>
 </saml:Attribute>
</saml:AttributeStatement>
```
2.3 The electronic signature

The electronic signature of saml:Assertion is largely based on the profile of [XMLDSig] specified in [SAML 1.1].

The signature contains two dsig:Reference elements that MUST be executed as follows:

```xml
<dsig:Signature xmlns:dsig="http://www.w3.org/2000/09/xmldsig#">
  <dsig:SignedInfo>
    ...
    <dsig:Reference
      URI="#bka.gv.at+2004-02-24T12:00:00.000Z">
      <dsig:Transforms>
        <dsig:Transform Algorithm="http://www.w3.org/TR/1999/REC-xpath-19991116">
          <dsig:XPath>not(ancestor-or-self::pr:Identification)</dsig:XPath>
        </dsig:Transform>
        <dsig:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
        <dsig:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
        <dsig:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
      </dsig:Transforms>
      <dsig:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
      <dsig:DigestValue>GwNaF71Mc3mnpua+DJxwN8BG9Ww=</dsig:DigestValue>
    </dsig:Reference>
    <dsig:Reference
      Type="http://www.w3.org/2000/09/xmldsig#Manifest"
      URI="#bka.gv.at+2004-02-24T12:00:00.000Z">
      <dsig:Transforms>
        <dsig:Transform Algorithm="http://www.w3.org/TR/1999/REC-xpath-19991116">
          <dsig:XPath>ancestor-or-self::dsig:Manifest</dsig:XPath>
        </dsig:Transform>
        <dsig:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
      </dsig:Transforms>
      <dsig:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
      <dsig:DigestValue>1JdggeCTzaZ/TAgb0pxoc46+eEY=</dsig:DigestValue>
    </dsig:Reference>
  </dsig:SignedInfo>
  ...
</dsig:Signature>
```

The references may also be executed with other resources and transformations, provided that the result is identical with the result from the references listed here. However, it is recommended that the referencing mechanism shown in the examples be used; this is derived from the profile for [XMLDSig] in [SAML 1.1].
The associated manifest MUST look like this:

```
<dsig:Signature xmlns:dsig="http://www.w3.org/2000/09/xmldsig#">
  <dsig:SignedInfo>
    ...
  </dsig:SignedInfo>
  ...
  <dsig:Object>
    <dsig:Manifest>
      <dsig:Reference
        URI="#bka.gv.at+2004-02-24T12:00:00.000Z">
        <dsig:Transforms>
          <dsig:Transform
            Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
          <dsig:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
        </dsig:Transforms>
        <dsig:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
        <dsig:DigestValue>JaKFnaY5X742Xwk6Kz1Q5faO34=</dsig:DigestValue>
      </dsig:Reference>
    </dsig:Manifest>
  </dsig:Object>
</dsig:Signature>
```

Here again the references MAY also be executed with other resources and transformations, provided that the result is identical with the result from the references listed here.

The first `dsig:Reference` element references the whole `saml:Assertion` except for the sourcePIN. The URI attribute refers to the document element `saml:Assertion`. An XPath transformation [XPath] that removes the sourcePIN and executes the Enveloped Signature transformation is implemented in sequence.

The second reference relates to the manifest. The manifest itself contains a single reference that relates to the complete `saml:Assertion`. The transformation removes the `dsig:Signature` element again.

With this signature structure, the sourcePIN can be removed from the person identity link, while still retaining a validating XMLDSig signature.

The sourcePIN is included with extended validation (validation of the manifest).

The signature also includes a `ds:KeyInfo` element that must contain sufficient information for automatic signature validation. In all cases the X.509 signature certificate MUST be included.

Section 5 contains a full example of a person identity link.
3 Encoding rules

The following encoding rules must be met in order to be able to use the compressed representation described in this chapter:

- For base64-encoded values in saml:Attribute and in dsig:DigestValue, the base64 representation may only use the following characters: “a”–“z”, “A”–“Z”, “0”–“9”, “+” and “/”, and finally (in line with the base64 rules) up to two “=” Line breaks must occur after precisely 76 characters; if the final line is 76 characters long, a further line break is not inserted before the end tag.

- If a dsig:DSAPKeyValu Value is used, the parameters $P$, $Q$, $G$ and $Y$ are to be specified. The parameters $J$, seed and pGenCounter must not be specified. See also [RFC3279], section 2.3.2.
4 Compressed representation

The compressed storage described below should be regarded as a suggestion and is not mandatory under the terms of this specification.

The XML structure of the person identity link described has around 5KB, which can be a problem for storage on smartcards because these only have a very limited storage capacity. However, a large part of the person identity link structure consists of known and fixed values that can be reproduced at any time. Thus, for compressed storage, it is possible to store only the variable parts.

The XML syntax permits variabilities within the defined structure (line breaks, location of the namespace declarations, comments, etc.). The following procedural model is chosen to prevent the current specification from being too restrictive: Compressed storage includes a URL for an XSLT style sheet of the person identity link. HTTP and HTTPS are permitted as protocols. The style sheet contains the complete XML structure of the person identity link, to which the variable parts are then added. The URL of the style sheet SHOULD not be longer than 48 characters.

This addresses the issue of variability on the one hand, while on the other, there will be no limitation on future enhancements of the person identity link specification.

The compressed storage is encoded as an ASN.1 DER-encoded sequence of characters [ASN1] [DER]. For implementation using style sheets, the compressed format should first be converted to an XML file (XML type il:CompressedIdentityLink). The element names are the same as the names of the elements in ASN.1. Based on the ASN.1 data, an application creates the il:CompressedIdentityLink, loads the XSLT style sheet from the specified URL and performs a transformation so as to obtain the original person identity link.

4.1 ASN.1 specification

```plaintext
PersonenBindung ::= SEQUENCE {
    version INTEGER,
    issuerTemplate UTF8String,
    assertionID UTF8String,
    issueInstant UTF8String,
}
```

2 Apart from the use of upper and lower case letters.
personData PersonData,
citizenPublicKey SEQUENCE SIZE (1..MAX) OF CitizenPublicKey,
signatureValue BIT STRING,
referenceDigest [0] BIT STRING OPTIONAL,
referenceManifestDigest [1] BIT STRING OPTIONAL,
manifestReferenceDigest [2] BIT STRING OPTIONAL,
}

PersonData ::= CHOICE {
  physicalPerson [0] PhysicalPersonData,
  corporateBody [1] CorporateBodyData
}
PhysicalPersonData ::= SEQUENCE {
    baseId UTF8String, 
    givenName UTF8String, 
    familyName UTF8String, 
    dateOfBirth UTF8String
}

CitizenPublicKey ::= CHOICE {
    onToken [0] INTEGER, 
    referenceURL [1] UTF8String, 
    x509Data [2] SubjectPublicKeyInfo
}

The CorporateBodyData type is currently undefined.

4.1.1 Explanation of individual fields

- **version**: identifies the version of the format for compressed storage (not transferred to XML representation). In the current ASN.1 structure, the value of the field is to be set to "1".

- **issuerTemplate**: is the URL from which the style sheet can be loaded. Because it can be assumed that the number of style sheets is very limited, Citizen Card Environments can also cache the style sheets.

- **assertionID**: is to be filled in in the AssertionID attribute of saml:Assertion. Please note that the assertionID is appended if the template in this attribute already contains characters. This means, for example, that the unchanging part that distinguishes the issuers from each other can also be included in the template.

- **personData** and associated PhysicalPersonData type: should be inserted at the appropriate points.

- **citizenPublicKey**: offers three options for saving a public key as an identifier for the certificate:
  - **onToken**: the information on retrieving the public key is located on the security token (e.g. in the form of a certificate) The number acts as an identification if there are several examples of such information on the card; the token determines the numbering.
  - **referenceURL**: specifies a URL under which the corresponding DER-encoded X.509 certificate can be retrieved.
  - **x509Data**: this contains the public key (X.509 type SubjectPublicKeyInfo) in line with the X.509 specification [RFC2459].
  - For the XML representation, onToken and referenceURL are to be resolved appropriately and the key value is to be inserted.

- **signatureValue**: the value of the signature – has to be encoded in base64 before it can be inserted in the XML structure.

- **referenceDigest, referenceManifestDigest, manifestReferenceDigest**: as an option, the hash values for the two references in the signature and the hash value for the reference in the manifest (manifestReferenceDigest). The values also have to be encoded in base64 before they can be inserted in the XML structure. This is optional because these values can be calculated when filling in the XML structure. However, these fields must be
listed in the compressed XML structure (input data for the style sheet) to ensure that the
style sheet can complete the relevant fields in the person identity link.

With this structure, a person identity link can be saved in 100 to 150 bytes if the public keys are
available on the token, or in approximately 400 bytes if the public keys are included.

When the person identity link is converted to compressed ASN.1 representation or to
compressed XML representation (il:CompressedIdentityLink), it is necessary to ensure
that values are transferred in identical form; in particular, leading or closing blanks or line
breaks are to be included for element values so as to permit bit-identical reconstruction.

5 Example

The example shows a complete person identity link for a natural person with the exception of
the values of the cryptographic data (hash, signature, key and certificate values).

5.1 Example of a person identity link

<?xml version="1.0" encoding="UTF-8"?>
<saml:Assertion
  AssertionID="bka.gv.at+2004-02-24T12:00:00.000Z"
  IssueInstant="2004-02-24T12:00:00.000Z"
  Issuer="http://www.bka.gv.at/datenschutz/Stammzahlenregisterbehoerde"
  MajorVersion="1"
  MinorVersion="0"
  xmlns:pr="http://reference.e-government.gv.at/namespaces/persondata/20020228#"
  xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <saml:Assertion>
    <saml:Subject>
      <saml:SubjectConfirmation>
        <saml:ConfirmationMethod>
          urn:oasis:names:tc:SAML:1.0:cm:sender-vouches
        </saml:ConfirmationMethod>
        <saml:SubjectConfirmationData>
          <pr:Person xsi:type="pr:PhysicalPersonType">
            <pr:Identification>
              <pr:Value>MDEyMzQ1Njc4OWFiY2RlZg==</pr:Value>
              <pr:Type>urn:publicid:gv.at:baseid</pr:Type>
            </pr:Identification>
            <pr:Name>
              <pr:GivenName>Herbert</pr:GivenName>
              <pr:FamilyName primary="undefined">Gramgebeugt</pr:FamilyName>
            </pr:Name>
            <pr:DateOfBirth>1950-12-31</pr:DateOfBirth>
          </pr:Person>
        </saml:SubjectConfirmationData>
      </saml:SubjectConfirmation>
    </saml:Subject>
    <saml:Attribute
      AttributeName="CitizenPublicKey"
      AttributeNamespace="urn:publicid:gv.at:namespaces:identitylink:1.2">
      <saml:AttributeValue>
        <dsig:RSAKeyValue xmlns:dsig="http://www.w3.org/2000/09/xmldsig#">
          <dsig:Modulus>...</dsig:Modulus>
          <dsig:Exponent>...</dsig:Exponent>
        </dsig:RSAKeyValue>
      </saml:AttributeValue>
    </saml:Attribute>
    <saml:Attribute
      AttributeName="CitizenPublicKey"
      AttributeNamespace="urn:publicid:gv.at:namespaces:identitylink:1.2">
      <saml:AttributeValue>
        <dsig:RSAKeyValue xmlns:dsig="http://www.w3.org/2000/09/xmldsig#">
          <dsig:Modulus>...</dsig:Modulus>
          <dsig:Exponent>...</dsig:Exponent>
        </dsig:RSAKeyValue>
      </saml:AttributeValue>
    </saml:Attribute>
  </saml:Assertion>
</saml:Assertion>
5.2 Example of compressed representation

<CompressedIdentityLink
  xmlns="http://www.buergerkarte.at/namespaces/personenbindung/20020506#"
  xmlns:pr="http://reference.e-government.gv.at/namespace/persondata/20020228#"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns:dsig="http://www.w3.org/2000/09/xmldsig#">
  <IssuerTemplate>http://www.bka.gv.at/pathToStylesheet/Sheet.xsl</IssuerTemplate>
  <AssertionID>bka.gv.at+2004-02-24T12:00:00.000Z</AssertionID>
  <IssueInstant>2004-02-24T12:00:00.000Z</IssueInstant>
  <PersonData xsi:type="pr:PhysicalPersonType">
    <pr:Identification>
      <pr:Value>MDEyMzQ1Njc4OWFiY2RlZg==</pr:Value>
      <pr:Type/>
    </pr:Identification>
    <pr:Name>
      <pr:GivenName>Herbert</pr:GivenName>
      <pr:FamilyName>Gramgebeugt</pr:FamilyName>
    </pr:Name>
  </PersonData>
</CompressedIdentityLink>
<pr:DateOfBirth>1950-12-31</pr:DateOfBirth>
</PersonData>
</CitizenPublicKey>
<dsig:RSAKeyValue>
<dsig:Modulus> .... </dsig:Modulus>
<dsig:Exponent> .... </dsig:Exponent>
</dsig:RSAKeyValue>
</CitizenPublicKey>
<dsig:DSAKeyValue>
<dsig:P> .... </dsig:P>
<dsig:Q> .... </dsig:Q>
<dsig:G> .... </dsig:G>
<dsig:Y> .... </dsig:Y>
</dsig:DSAKeyValue>
</CitizenPublicKey>
<SignatureValue> .... </SignatureValue>
<ReferenceDigest> .... </ReferenceDigest>
<ReferenceManifestDigest> .... </ReferenceManifestDigest>
<ManifestReferenceDigest> .... </ManifestReferenceDigest>
</CompressedIdentityLink>
References

ASN1
Abstract Syntax Notation One (ASN.1), Specification of Basic Notation.

DER
ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical
Encoding Rules (CER) and Distinguished Encoding Rules (DER).

PersDat
Hollosi, Arno and Reichstädt, Peter: XML-Spezifikation der Personen-Daten Struktur
[XML Specification of the Personal Data Structure]. Convention for e-Government in
Austria drafted by the Federal Staff Unit for ICT Strategy, Technology and Standards.

RFC3279
W. Polk, R. Housley, L. Bassham: RFC 3279, Algorithms and Identifiers for the Internet
X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile,
April 2002. Downloaded from the World Wide Web on 24 February 2004 under

SAML 1.0
OASIS: Assertions and Protocol for the OASIS Security Assertion Markup Language
http://www.oasis-open.org/committees/security/

SAML 1.1
OASIS: Assertions and Protocol for the OASIS Security Assertion Markup Language
http://www.oasis-open.org/committees/security/

XPath
James Clark, Steve DeRose: XML Path Language (XPath). W3C Recommendation,
November 1999. Downloaded from the World Wide Web on 24 February 2004 under
http://www.w3.org/TR/1999/REC-xpath-19991116.

XMLDSig
Donald Eastlake, Joseph Reagle and David Solo: XML-Signature Syntax and Processing.
W3C Recommendation, February 2002. Downloaded from the World Wide Web on 24
## History

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Created by</th>
<th>Comment</th>
</tr>
</thead>
</table>
| 1.1.0   | 2002-05-06 | Arno Hollosi   | • Upgrade to SAML Version 1.0 dated 19 April 2002.  
• Complete conformity with SAML:  
  o AttributeStatement used instead of separate PersonAttributeStatement type  
  o Assertion without ID attribute – signature references now with XPointer |
|         |            |                | New references: XPointer, XPath |
| 1.1.1   | 2003-05-06 | Gregor Karlinger | • Editorial improvements |
| 1.2.0   | 2003-10-14 | Gregor Karlinger, Arno Hollosi | • Nomenclature updated: SourcePIN, sector-specific personal identifier  
• References updated.  
Examples revised; signature adapted to profile from [SAML 1.1]. |
| 1.2.1   | 2004-02-24 | Gregor Karlinger | • Identifier for the issuer of the person identity link has been changed.  
• Identifier for the sourcePIN has been changed.  
• Namespace for the CitizenPublicKey SAML attribute has been changed. |
| 1.2.2   | 2005-02-14 | Gregor Karlinger | • The formulation “legal person” has been replaced with “non-natural person”.  
• Lines 247 to 250: The first part of the second sentence now reads “The URI attribute refers to the document element,” instead of, as previously, “The URI attribute refers to the document.”  
• Lines 247 to 250: Footnote 2 deleted because it is contradictory.  
• Line 411 has been corrected to read: „<dsig:Modulus>...</dsig:Modulus>“ |