



<b>XML Definition of the Person Identity Link 2005-02-14</b>	<b>Convention</b>
	Person Identity Link – 1.2.2
	<b>Public Draft</b>

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	<p>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.</p> <p>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.</p> <p>This paper describes the XML specification of the person identity link.</p>
Authors	Arno Hollosi, <a href="mailto:arno.hollosi@cio.gv.at">arno.hollosi@cio.gv.at</a> Gregor Karlinger, <a href="mailto:gregor.karlinger@cio.gv.at">gregor.karlinger@cio.gv.at</a>
Work group	Federal Staff Unit for ICT Strategy, Technology and Standards

# Table of contents

1	<b>Table of contents</b>	
2	Table of contents .....	2
3	1 Introduction and basic data.....	3
4	2 Basic XML structure .....	4
5	2.1 SAML assertion (framework structure).....	4
6	2.1.1 Example .....	5
7	2.2 SAML Attribute Statement.....	5
8	2.2.1 Personal data.....	5
9	2.2.2 Attributes .....	7
10	2.2.3 Example .....	7
11	2.3 The electronic signature.....	8
12	3 Encoding rules .....	10
13	4 Compressed representation.....	11
14	4.1 ASN.1 specification.....	11
15	4.1.1 Explanation of individual fields .....	13
16	5 Example .....	14
17	5.1 Example of a person identity link.....	14
18	5.2 Example of compressed representation .....	15
19	References .....	17
20	History .....	18

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

## 24 **1 Introduction and basic data**

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

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

31 In addition to the sourcePIN (a person's identification), the person identity link also contains a  
32 unique identifier for each certificate to which the sourcePIN is assigned. This ensures a  
33 cryptographically secured link between the electronic signature of a person (the signatory) and a  
34 unique identification feature for this person.

35

## 2 Basic XML structure

36

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).

37

38

39

40

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

41

42

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.

43

44

45

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

46

- Security Assertion Markup Language (SAML) – OASIS : Framework structure  
Namespace: `urn:oasis:names:tc:SAML:1.0:assertion`, prefix: `saml`

47

48

- XML Digital Signatures (XMLDSIG) – W3C : Electronic signatures  
Namespace: `http://www.w3.org/2000/09/xmlsig#`, prefix: `dsig`

49

50

- PersonData – CIO Austria : Placeholder for personal data  
Namespace: `http://reference.e-government.gv.at/namespace/persondata/20020228#`, prefix: `pr`

51

52

53

- 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`

54

55

56

57

### 2.1 SAML assertion (framework structure)

58

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

59

The `saml:Assertion` element contains the following mandatory attributes:

Name	Value	Description
MajorVersion	1	SAML version number
MinorVersion	0	SAML version number
AssertionID	xs:string	ID for the assertion
Issuer	xs:string	Name of the assertion issuer
IssueInstant	xs:dateTime	Time at which the person identity link was issued.

60

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`).

61

62

63

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

64

65

66 summarised on a publically available web page. Since the specified URL can be included in  
 67 various programs as a parameter, it SHOULD remain unchanged over a long period.

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

70

Name	Description
<code>saml:AttributeStatement</code>	Contains the core data of the person identity link.
<code>dsig:Signature</code>	The electronic signature of the issuer of the link

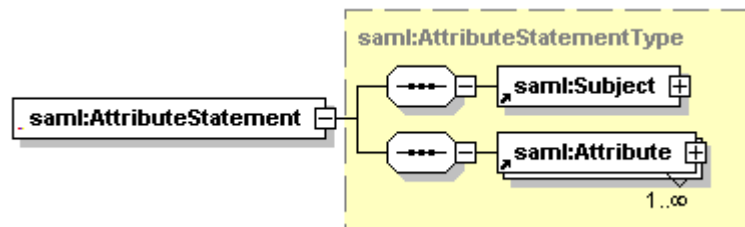
### 71 2.1.1 Example

```

72 <?xml version="1.0" encoding="UTF-8"?>
73 <saml:Assertion
74   AssertionID="bka.gv.at+2004-02-24T12:00:00.000Z"
75   IssueInstant="2004-02-24T12:00:00.000Z"
76   Issuer="http://www.bka.gv.at/datenschutz/Stammzahlenregisterbehoerde"
77   MajorVersion="1"
78   MinorVersion="0"
79   <saml:AttributeStatement>
80     ...
81   </saml:AttributeStatement>
82   <dsig:Signature>
83     ...
84   </dsig:Signature>
85 </saml:Assertion>
  
```

## 86 2.2 SAML Attribute Statement

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



89

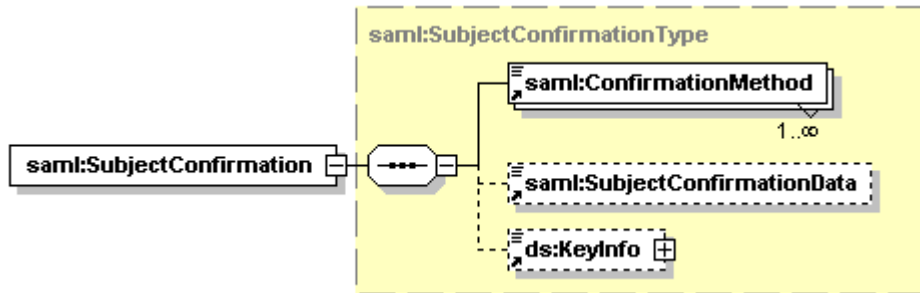
Name	Description
<code>saml:Subject</code>	Personal data
<code>saml:Attribute</code>	Identifier for a certificate to which the sourcePIN is to be assigned (the identifier used is the public key from the certificate).

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

### 93 2.2.1 Personal data

94 The `saml:Subject` structure contains precisely the element `saml:SubjectConfirmation`.  
 95 In this element, `saml:ConfirmationMethod` is set to the value

96 urn:oasis:names:tc:SAML:1.0:cm:sender-vouches<sup>1</sup>, while  
 97 saml:SubjectConfirmationData contains the person's data in the form of a pr:Person  
 98 element.



99

### 2.2.1.1 Personal data for natural persons

100 The `pr:Person` element type MUST be `pr:PhysicalPersonType` and MUST contain  
 101 precisely the following data:  
 102

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

### Example

```

103
104 <pr:Person
105   xsi:type="pr:PhysicalPersonType"
106   xmlns:pr="http://reference.e-government.gv.at/namespace/persondata/20020228#">
107   <pr:Identification>
108     <pr:Value>MDEyMzQ1Njc4OWFiY2RlZg==</pr:Value>
109     <pr:Type>urn:publicid:gv.at:baseid</pr:Type>
110   </pr:Identification>
111   <pr:Name>
112     <pr:GivenName>Herbert</pr:GivenName>
113     <pr:FamilyName primary="undefined">Gramgebeugt</pr:FamilyName>
114   </pr:Name>
115   <pr:DateOfBirth>1950-12-31</pr:DateOfBirth>
116 </pr:Person>
  
```

### 2.2.1.2 Personal data for non-natural persons

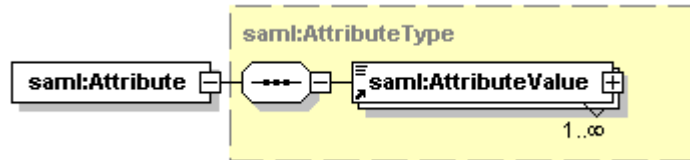
117 Personal data for non-natural persons (companies, associations, etc.) will be defined in a later  
 118 version of this document.  
 119

<sup>1</sup> 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).

## 120 2.2.2 Attributes

### 121 2.2.2.1 Attributes for natural persons

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



125

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

### 129 2.2.2.2 Attributes for non-natural persons

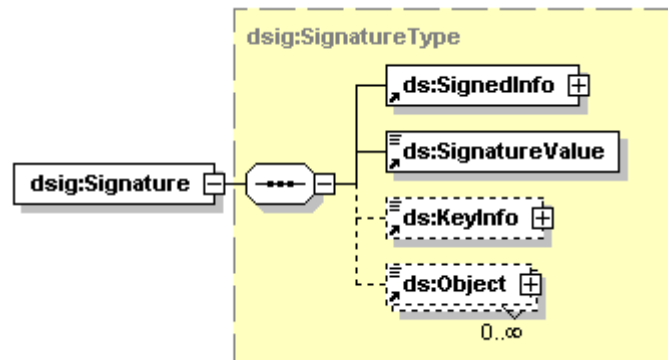
130 Attributes for non-natural persons (companies, associations, etc.) are still to be defined.

## 131 2.2.3 Example

```
132 <saml:AttributeStatement
133   xmlns:pr="http://reference.e-government.gv.at/namespaces/persondata/20020228#"
134   xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion"
135   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
136   <saml:Subject>
137     <saml:SubjectConfirmation>
138       <saml:ConfirmationMethod>
139         urn:oasis:names:tc:SAML:1.0:cm:sender-vouches</saml:ConfirmationMethod>
140       <saml:SubjectConfirmationData>
141         <pr:Person xsi:type="pr:PhysicalPersonType">
142           <pr:Identification>
143             <pr:Value>MDEyMzQ1Njc4OWFiY2RlZg==</pr:Value>
144             <pr:Type>urn:publicid:gv.at:baseid</pr:Type>
145           </pr:Identification>
146           <pr:Name>
147             <pr:GivenName>Herbert</pr:GivenName>
148             <pr:FamilyName primary="undefined">Gramgebeugt</pr:FamilyName>
149           </pr:Name>
150           <pr:DateOfBirth>1950-12-31</pr:DateOfBirth>
151         </pr:Person>
152       </saml:SubjectConfirmationData>
153     </saml:SubjectConfirmation>
154   </saml:Subject>
155   <saml:Attribute
156     AttributeName="CitizenPublicKey"
157     AttributeNamespace="urn:publicid:gv.at:namespaces:identitylink:1.2">
158     <saml:AttributeValue>
159       <dsig:RSAKeyValue xmlns:dsig="http://www.w3.org/2000/09/xmldsig#">
160         <dsig:Modulus>...</dsig:Modulus>
161         <dsig:Exponent>dG+9</dsig:Exponent>
162       </dsig:RSAKeyValue>
163     </saml:AttributeValue>
164   </saml:Attribute>
165   <saml:Attribute
166     AttributeName="CitizenPublicKey"
167     AttributeNamespace="urn:publicid:gv.at:namespaces:identitylink:1.2">
168     <saml:AttributeValue>
169       <dsig:RSAKeyValue xmlns:dsig="http://www.w3.org/2000/09/xmldsig#">
170         <dsig:Modulus>...</dsig:Modulus>
171         <dsig:Exponent>Q9Hf8w1UM3mKwROWcuWiZ6Aucq8=</dsig:Exponent>
172       </dsig:RSAKeyValue>
173     </saml:AttributeValue>
174   </saml:Attribute>
175 </saml:AttributeStatement>
```

## 2.3 The electronic signature

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



179

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

```

181 <dsig:Signature xmlns:dsig="http://www.w3.org/2000/09/xmldsig#">
182   <dsig:SignedInfo>
183     ...
184     <dsig:Reference
185       URI="#bka.gv.at+2004-02-24T12:00:00.000Z">
186       <dsig:Transforms>
187         <dsig:Transform Algorithm="http://www.w3.org/TR/1999/REC-xpath-19991116">
188           <dsig:XPath>not(ancestor-or-self::pr:Identification)</dsig:XPath>
189         </dsig:Transform>
190         <dsig:Transform
191           Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
192         <dsig:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
193       </dsig:Transforms>
194       <dsig:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
195       <dsig:DigestValue>GwNaF71Mc3mnpua+DJxwN8BG9Ww</dsig:DigestValue>
196     </dsig:Reference>
197     <dsig:Reference
198       Type="http://www.w3.org/2000/09/xmldsig#Manifest"
199       URI="#bka.gv.at+2004-02-24T12:00:00.000Z">
200       <dsig:Transforms>
201         <dsig:Transform Algorithm="http://www.w3.org/TR/1999/REC-xpath-19991116">
202           <dsig:XPath>ancestor-or-self::dsig:Manifest</dsig:XPath>
203         </dsig:Transform>
204         <dsig:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
205       </dsig:Transforms>
206       <dsig:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
207       <dsig:DigestValue>1JdggeCTzaZ/TAgbOpxoc46+eEY</dsig:DigestValue>
208     </dsig:Reference>
209   </dsig:SignedInfo>
210   ...
211 </dsig:Signature>

```

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

216 The associated manifest MUST look like this:

```
217 <dsig:Signature xmlns:dsig="http://www.w3.org/2000/09/xmldsig#">
218   <dsig:SignedInfo>
219     ...
220   </dsig:SignedInfo>
221   ...
222   <dsig:Object>
223     <dsig:Manifest>
224       <dsig:Reference
225         URI="#bka.gv.at+2004-02-24T12:00:00.000Z">
226         <dsig:Transforms>
227           <dsig:Transform
228             Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
229           <dsig:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
230         </dsig:Transforms>
231         <dsig:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
232         <dsig:DigestValue>JaKFnaY5X742Xwk6KWz1Q5fa034=</dsig:DigestValue>
233       </dsig:Reference>
234     </dsig:Manifest>
235   </dsig:Object>
236 </dsig:Signature>
```

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

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

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

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

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

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

251 Section 5 contains a full example of a person identity link.

252

## 3 Encoding rules

253

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

254

255

- 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.

256

257

258

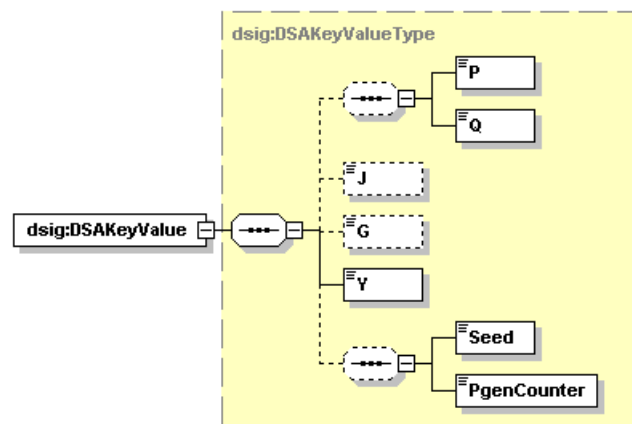
259

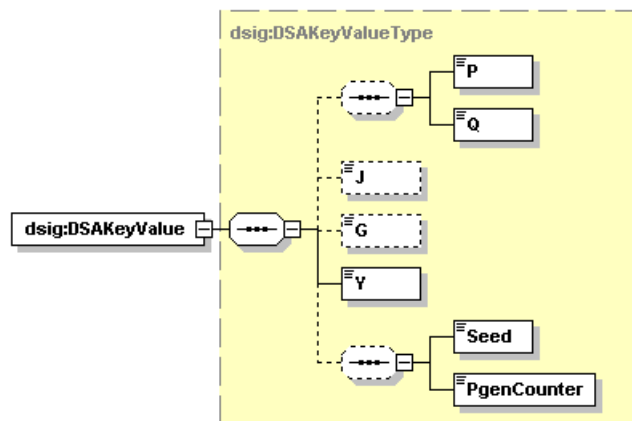
260

- If a `dsig:DSAKeyValue` 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.

261

262





## 263 4 Compressed representation

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

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

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

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

280 The compressed storage is encoded as an ASN.1 DER-encoded sequence of characters [ASN1]  
281 [DER]. For implementation using style sheets, the compressed format should first be converted  
282 to an XML file (XML type `il:CompressedIdentityLink`). The element names are the same  
283 as the names of the elements in ASN.1<sup>2</sup>. Based on the ASN.1 data, an application creates the  
284 `il:CompressedIdentityLink`, loads the XSLT style sheet from the specified URL and  
285 performs a transformation so as to obtain the original person identity link.

### 286 4.1 ASN.1 specification

```
287 PersonenBindung ::= SEQUENCE {
288     version INTEGER,
289     issuerTemplate UTF8String,
290     assertionID UTF8String,
291     issueInstant UTF8String,
```

<sup>2</sup> Apart from the use of upper and lower case letters.

```
292     personData PersonData,
293     citizenPublicKey SEQUENCE SIZE (1..MAX) OF CitizenPublicKey,
294     signatureValue BIT STRING,
295     referenceDigest [0] BIT STRING OPTIONAL,
296     referenceManifestDigest [1] BIT STRING OPTIONAL,
297     manifestReferenceDigest [2] BIT STRING OPTIONAL,
298 }
299
300 PersonData ::= CHOICE {
301     physcialPerson [0] PhysicalPersonData,
302     corporateBody [1] CorporateBodyData
303 }
```

```

304 PhysicalPersonData ::= SEQUENCE {
305     baseId UTF8String,
306     givenName UTF8String,
307     familyName UTF8String,
308     dateOfBirth UTF8String
309 }
310
311 CitizenPublicKey ::= CHOICE {
312     onToken [0] INTEGER,
313     referenceURL [1] UTF8String,
314     x509Data [2] SubjectPublicKeyInfo
315 }
316

```

317 The CorporateBodyData type is currently undefined.

### 318 4.1.1 Explanation of individual fields

- 319 • *version*: identifies the version of the format for compressed storage (not transferred to  
320 XML representation). In the current ASN.1 structure, the value of the field is to be set to  
321 “1”.
- 322 • *issuerTemplate*: is the URL from which the style sheet can be loaded. Because it can be  
323 assumed that the number of style sheets is very limited, Citizen Card Environments can  
324 also cache the style sheets.
- 325 • *assertionID*: is to be filled in in the AssertionID attribute of saml:Assertion.  
326 Please note that the *assertionID* is appended if the template in this attribute already  
327 contains characters. This means, for example, that the unchanging part that distinguishes  
328 the issuers from each other can also be included in the template.
- 329 • *personData* and associated *PhysicalPersonData* type: should be inserted at the  
330 appropriate points.
- 331 • *citizenPublicKey*: offers three options for saving a public key as an identifier for the  
332 certificate:
  - 333 ○ *onToken*: the information on retrieving the public key is located on the security  
334 token (e.g. in the form of a certificate) The number acts as an identification if  
335 there are several examples of such information on the card; the token determines  
336 the numbering.
  - 337 ○ *referenceURL*: specifies a URL under which the corresponding DER-encoded  
338 X.509 certificate can be retrieved.
  - 339 ○ *x509Data*: this contains the public key (X.509 type *SubjectPublicKeyInfo*) in line  
340 with the X.509 specification [RFC2459].
  - 341 ○ For the XML representation, *onToken* and *referenceURL* are to be resolved  
342 appropriately and the key value is to be inserted.
- 343 • *signatureValue*: the value of the signature – has to be encoded in base64 before it can be  
344 inserted in the XML structure.
- 345 • *referenceDigest*, *referenceManifestDigest*, *manifestReferenceDigest*: as an option, the  
346 hash values for the two references in the signature and the hash value for the reference in  
347 the manifest (*manifestReferenceDigest*). The values also have to be encoded in base64  
348 before they can be inserted in the XML structure. This is optional because these values  
349 can be calculated when filling in the XML structure. However, these fields must be

350 listed in the compressed XML structure (input data for the style sheet) to ensure that the  
351 style sheet can complete the relevant fields in the person identity link.

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

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

## 358 5 Example

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

### 361 5.1 Example of a person identity link

```
362 <?xml version="1.0" encoding="UTF-8"?>
363 <saml:Assertion
364   AssertionID="bka.gv.at+2004-02-24T12:00:00.000Z"
365   IssueInstant="2004-02-24T12:00:00.000Z"
366   Issuer="http://www.bka.gv.at/datenschutz/Stammzahlenregisterbehoerde"
367   MajorVersion="1"
368   MinorVersion="0"
369   xmlns:pr="http://reference.e-government.gv.at/namespace/persondata/20020228#"
370   xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion"
371   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
372   <saml:AttributeStatement>
373     <saml:Subject>
374       <saml:SubjectConfirmation>
375         <saml:ConfirmationMethod>
376           urn:oasis:names:tc:SAML:1.0:cm:sender-vouches</saml:ConfirmationMethod>
377         <saml:SubjectConfirmationData>
378           <pr:Person xsi:type="pr:PhysicalPersonType">
379             <pr:Identification>
380               <pr:Value>MDEyMzQ1Njc4OWFiY2RlZg==</pr:Value>
381               <pr:Type>urn:publicid:gv.at:baseid</pr:Type>
382             </pr:Identification>
383             <pr:Name>
384               <pr:GivenName>Herbert</pr:GivenName>
385               <pr:FamilyName primary="undefined">Gramgebeugt</pr:FamilyName>
386             </pr:Name>
387             <pr:DateOfBirth>1950-12-31</pr:DateOfBirth>
388           </pr:Person>
389         </saml:SubjectConfirmationData>
390       </saml:SubjectConfirmation>
391     </saml:Subject>
392     <saml:Attribute
393       AttributeName="CitizenPublicKey"
394       AttributeNamespace="urn:publicid:gv.at:namespaces:identitylink:1.2">
395       <saml:AttributeValue>
396         <dsig:RSAKeyValue xmlns:dsig="http://www.w3.org/2000/09/xmldsig#">
397           <dsig:Modulus>...</dsig:Modulus>
398           <dsig:Exponent>...</dsig:Exponent>
399         </dsig:RSAKeyValue>
400       </saml:AttributeValue>
401     </saml:Attribute>
402     <saml:Attribute
403       AttributeName="CitizenPublicKey"
404       AttributeNamespace="urn:publicid:gv.at:namespaces:identitylink:1.2">
405       <saml:AttributeValue>
406         <dsig:RSAKeyValue xmlns:dsig="http://www.w3.org/2000/09/xmldsig#">
407           <dsig:Modulus>...</dsig:Modulus>
408           <dsig:Exponent>...</dsig:Exponent>
409         </dsig:RSAKeyValue>
```

```

410     </saml:AttributeValue>
411   </saml:Attribute>
412 </saml:AttributesStatement>
413 <dsig:Signature xmlns:dsig="http://www.w3.org/2000/09/xmldsig#">
414   <dsig:SignedInfo>
415     <dsig:CanonicalizationMethod
416       Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
417     <dsig:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
418     <dsig:Reference URI="#bka.gv.at+2004-02-24T12:00:00.000Z">
419       <dsig:Transforms>
420         <dsig:Transform Algorithm="http://www.w3.org/TR/1999/REC-xpath-19991116">
421           <dsig:XPath>not(ancestor-or-self::pr:Identification)</dsig:XPath>
422         </dsig:Transform>
423         <dsig:Transform
424           Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
425         </dsig:Transforms>
426         <dsig:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
427         <dsig:DigestValue>Rv01PzN5sd4WVclcz/PTz/hqUIo=</dsig:DigestValue>
428       </dsig:Reference>
429     <dsig:Reference URI="#bka.gv.at+2004-02-24T12:00:00.000Z"
430       Type="http://www.w3.org/2000/09/xmldsig#Manifest">
431       <dsig:Transforms>
432         <dsig:Transform Algorithm="http://www.w3.org/TR/1999/REC-xpath-19991116">
433           <dsig:XPath>ancestor-or-self::dsig:Manifest</dsig:XPath>
434         </dsig:Transform>
435       </dsig:Transforms>
436       <dsig:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
437       <dsig:DigestValue>K/GKbypaUtsr3Qh0De5uwHM9CU=</dsig:DigestValue>
438     </dsig:Reference>
439   </dsig:SignedInfo>
440   <dsig:SignatureValue>...</dsig:SignatureValue>
441   <dsig:KeyInfo>
442     <dsig:X509Data>
443       <dsig:X509Certificate>...</dsig:X509Certificate>
444       <dsig:X509Certificate>...</dsig:X509Certificate>
445       <dsig:X509Certificate>...</dsig:X509Certificate>
446     </dsig:X509Data>
447   </dsig:KeyInfo>
448   <dsig:Object>
449     <dsig:Manifest>
450       <dsig:Reference URI="#bka.gv.at+2004-02-24T12:00:00.000Z">
451         <dsig:Transforms>
452           <dsig:Transform
453             Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
454           </dsig:Transforms>
455           <dsig:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
456           <dsig:DigestValue>vHj9m+TpUI7zWjM+0QIgaid/Lq0=</dsig:DigestValue>
457         </dsig:Reference>
458       </dsig:Manifest>
459     </dsig:Object>
460   </dsig:Signature>
461 </saml:Assertion>

```

## 462 5.2 Example of compressed representation

```

463 <CompressedIdentityLink
464   xmlns="http://www.buergerkarte.at/namespaces/personenbindung/20020506#"
465   xmlns:pr="http://reference.e-government.gv.at/namespace/persondata/20020228#"
466   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
467   xmlns:dsig="http://www.w3.org/2000/09/xmldsig#">
468   <IssuerTemplate>http://www.bka.gv.at/pathToStylesheet/Sheet.xsl</IssuerTemplate>
469   <AssertionID>bka.gv.at+2004-02-24T12:00:00.000Z</AssertionID>
470   <IssueInstant>2004-02-24T12:00:00.000Z</IssueInstant>
471   <PersonData xsi:type="pr:PhysicalPersonType">
472     <pr:Identification>
473       <pr:Value>MDEyMzQ1Njc4OWFiY2RlZg==</pr:Value>
474       <pr:Type/>
475     </pr:Identification>
476     <pr:Name>
477       <pr:GivenName>Herbert</pr:GivenName>
478       <pr:FamilyName>Gramgebeugt</pr:FamilyName>
479     </pr:Name>

```

```
480     <pr:DateOfBirth>1950-12-31</pr:DateOfBirth>
481 </PersonData>
482 <CitizenPublicKey>
483   <dsig:RSAKeyValue>
484     <dsig:Modulus> .... </dsig:Modulus>
485     <dsig:Exponent> .... </dsig:Exponent>
486   </dsig:RSAKeyValue>
487 </CitizenPublicKey>
488 <CitizenPublicKey>
489   <dsig:DSAKeyValue>
490     <dsig:P> .... </dsig:P>
491     <dsig:Q> .... </dsig:Q>
492     <dsig:G> .... </dsig:G>
493     <dsig:Y> .... </dsig:Y>
494   </dsig:DSAKeyValue>
495 </CitizenPublicKey>
496 <SignatureValue> .... </SignatureValue>
497 <ReferenceDigest> .... </ReferenceDigest>
498 <ReferenceManifestDigest> .... </ReferenceManifestDigest>
499 <ManifestReferenceDigest> .... </ManifestReferenceDigest>
500 </CompressedIdentityLink>
```

## 501 **References**

### 502 **ASN1**

503 ITU-T Recommendation X.680 (1997), ISO/IEC 8824-1: 1998, Information Technology –  
504 Abstract Syntax Notation One (ASN.1), Specification of Basic Notation.

### 505 **DER**

506 ITU-T Recommendation X.690 (1997), ISO/IEC 8825-1: 1998, Information Technology –  
507 ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical  
508 Encoding Rules (CER) and Distinguished Encoding Rules (DER).

### 509 **PersDat**

510 Hollosi, Arno and Reichstädter, Peter: XML-Spezifikation der Personen-Daten Struktur  
511 [XML Specification of the Personal Data Structure]. Convention for e-Government in  
512 Austria drafted by the Federal Staff Unit for ICT Strategy, Technology and Standards.  
513 Public Draft, Version 1.0.1, 24 April 2002. Downloaded from the World Wide Web on 25  
514 September 2003 under <http://reference.e-government.at>.

### 515 **RFC3279**

516 W. Polk, R. Housley, L. Bassham: RFC 3279, Algorithms and Identifiers for the Internet  
517 X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile,  
518 April 2002. Downloaded from the World Wide Web on 24 February 2004 under  
519 <http://www.ietf.org/rfc/rfc3279.txt>.

### 520 **SAML 1.0**

521 OASIS: Assertions and Protocol for the OASIS Security Assertion Markup Language  
522 (SAML). OASIS Standard, 5 November 2002.

523 <http://www.oasis-open.org/committees/security/>

### 524 **SAML 1.1**

525 OASIS: Assertions and Protocol for the OASIS Security Assertion Markup Language  
526 (SAML) V1.1. OASIS Standard, 2 September 2003.

527 <http://www.oasis-open.org/committees/security/>

### 528 **XPath**

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

### 532 **XMLDSig**

533 Donald Eastlake, Joseph Reagle and David Solo: XML-Signature Syntax and Processing.  
534 W3C Recommendation, February 2002. Downloaded from the World Wide Web on 24  
535 February 2004 under <http://www.w3.org/TR/2002/REC-xmlsig-core-20020212>.

## History

Version	Date	Comment
1.1.0	2002-05-06	
Created by		<ul style="list-style-type: none"> <li>• Upgrade to SAML Version 1.0 dated 19 April 2002.</li> <li>• Complete conformity with SAML:             <ul style="list-style-type: none"> <li>◦ AttributeStatement used instead of separate PersonAttributeStatement type</li> <li>◦ Assertion without ID attribute – signature references now with XPointer</li> </ul> </li> </ul> <p>New references: XPointer, XPath</p>
Arno Hollosi		
Version	Date	Comment
1.1.1	2003-05-06	
Created by		<ul style="list-style-type: none"> <li>• Editorial improvements</li> </ul>
Gregor Karlinger		
Version	Date	Comment
1.2.0	2003-10-14	
Created by		<ul style="list-style-type: none"> <li>• Nomenclature updated: SourcePIN, sector-specific personal identifier</li> <li>• References updated.</li> </ul> <p>Examples revised; signature adapted to profile from [SAML 1.1].</p>
Gregor Karlinger Arno Hollosi		
Version	Date	Comment
1.2.1	2004-02-24	
Created by		<ul style="list-style-type: none"> <li>• Identifier for the issuer of the person identity link has been changed.</li> <li>• Identifier for the sourcePIN has been changed.</li> <li>• Namespace for the CitizenPublicKey SAML attribute has been changed.</li> </ul>
Gregor Karlinger		
Version	Date	Comment
1.2.2	2005-02-14	
Created by		<ul style="list-style-type: none"> <li>• The formulation “legal person” has been replaced with “non-natural person”.</li> <li>• 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.”</li> <li>• Lines 247 to 250: Footnote 2 deleted because it is contradictory.</li> <li>• Line 411 has been corrected to read: „&lt;dsig:Modulus&gt;...&lt;/dsig:Modulus&gt;“</li> </ul>
Gregor Karlinger		

