XML Definition der Personenbindung		Konvention xml-pb 1.2.2 Empfehlung
Kurzbeschreibung	Die Personenbindung ist integraler Bestandteil des Konzepts Bürgerkarte. Sie ist eine von der Behörde signierte Struktur, welche ein eindeutiges Identifikationsmerkmal einer Person (zum Beispiel eine Registernummer) einem oder mehreren Zertifikaten dieser Person zuordnet. Als solches dient die Personenbindung der eindeutigen, automatisierbaren Identifikation einer Person, wenn sie im Zuge eines Verfahrens an die Behörde herantritt. Dieses Papier beschreibt die XML-Spezifikation der Personenbindung. *Dieses Dokument wurde im Zuge der Konsolidierung der E-Government Spezifikationen und Koventionen in einen formellen Status übergeführt. Editorelle Änderungen, wie das Hinzufügen des Deckblattes, wurden vorgenommen; inhaltlich blieb das Dokument unverändert.*	
Autor(en):	Arno Hollosi, BKA Gregor Karlinger, BKA	Projektteam / Arbeitsgruppe AG Bürgerkarte
Beiträge von:		

Version 1.2.2: **19.11.2007** Fristablauf: **10.12.2007**

Inhalt

Dieses Dokument verwendet die Schlüsselwörter MUSS, DARF NICHT, ERFORDERLICH, SOLLTE, SOLLTE NICHT, EMPFOHLEN, DARF, und OPTIONAL zur Kategorisierung der Anforderungen. Diese Schlüsselwörter sind analog zu ihren englischsprachigen Entsprechungen MUST, MUST NOT, REQUIRED, SHOULD, SHOULD NOT, RECOMMENDED, MAY, und OPTIONAL zu handhaben, deren Interpretation in RFC 2119 festgelegt ist.

1 Einleitung und Basisdaten

Im Zuge von elektronischen Verfahren ist es für die Behörde wichtig, eine Person eindeutig zu identifizieren. Zertifikate wie sie für die elektronische Signatur verwendet werden, reichen für eine automatisierte, eindeutige Identifikation nicht aus, da sie meist nur den Namen der Person enthalten. Der Name einer Person ist für eine eineindeutige Identifikation aber nicht ausreichend.

Aus diesem Grund wird die Person über ihre Stammzahl identifiziert, die für die Lebensdauer der Person konstant ist.

Die Personenbindung enthält neben der Stammzahl (dem Ordnungsbegriff für die Person) auch noch einen eindeutigen Bezeichner für jedes Zertifikat, dem die Stammzahl zugeordnet wird. Damit ist eine kryptographisch gesicherte Bindung zwischen der elektronischen Unterschrift einer Person (dem Signator) und eines für diese Person eindeutigen Identifikationsmerkmals gegeben.

2 XML-Grundstruktur

Die XML-Grundstruktur basiert auf der Security Assertion Markup Language [SAML 1.0] definiert von OASIS (Organization for the Advancement of Structured Information Standards). [SAML 1.0] definiert XML-Strukturen, die die Bestätigung (Assertions) von bestimmten Sachverhalten bzw. Beziehungen zwischen Subjekten durch Dritte (so genannte Authorities) zum Inhalt haben.

Im Falle der Personenbindung bestätigt dabei die Stammzahlenregisterbehörde die Beziehung der Stammzahl zu einem oder mehreren Zertifikaten.

Die Stammzahlenregisterbehörde sichert dabei durch ihre Signatur diese Beziehung kryptographisch gegen Veränderung ab. Die Signatur garantiert also die Authentizität der Daten und identifiziert die ausstellende Behörde über ihr Zertifikat.

Für die Personenbindung kommen folgende Standards und Spezifikationen zum Einsatz:

- Security Assertion Markup Language (SAML) – OASIS : Rahmenstruktur
  Namespace: `urn:oasis:names:tc:SAML:1.0:assertion`, Präfix: `saml`
- XML Digital Signatures (XMLDSIG) – W3C : elektronische Signaturen
  Namespace: `http://www.w3.org/2000/09/xmldsig#`, Präfix: `dsig`
- PersonData – CIO Austria : Platzhalter für Personendaten
  Namespace: `http://reference.e-government.gv.at/namespace/persondata/20020228#`, Präfix: `pr`
- Vorschlag zur komprimierten Personenbindung – CIO Austria : Schema zur komprimierten Speicherung der Personenbindung
  Namespace: `http://www.buergerkarte.at/namespaces/personenbindung/20020506#`, Präfix: `il`

2.1 SAML Assertion (Rahmenstruktur)

Basis der Personenbindung ist die `saml:Assertion` Struktur aus [SAML 1.0].

Folgende verpflichtende Attribute sind im `saml:Assertion` Element enthalten:

Name	Wert	Beschreibung
`MajorVersion`	1	SAML Versionsnummer
`MinorVersion`	0	SAML Versionsnummer
`AssertionID`	xs:string	ID für die Assertion
`Issuer`	xs:string	Name des Ausstellers der Assertion.
`IssueInstant`	xs:dateTime	Zeitpunkt der Ausstellung der Personenbindung

Die `AssertionID` SOLLTE über die Applikationsgrenze hinweg eindeutig sein. Es wird EMPFOHLEN den Domainnamen der ausstellenden Behörde plus eine laufende Nummer bzw. die aktuelle Zeit zu verwenden (z.B. `bka.gv.at+2004-02-24T12:00:00.000Z`).

`Issuer` bezeichnet den Aussteller der `saml:Assertion` und MUSS im Kontext der Personenbindung ein URL sein, welcher auf eine Ressource verweist, die Namen, Anschrift und Signaturzertifikat des Ausstellers sowie optional weitere Informationen beinhaltet. Üblicherweise wird diese Information auf einer öffentlich zugänglichen Webseite

zusammengefasst werden. Der angegebene URL SOLLTE über einen großen Zeitraum konstant sein, da er in verschiedenen Programmen als Parameter inkludiert sein kann.

Weiters sind im Kontext der Personenbindung genau folgende Elemente in der `saml:Assertion` Struktur verpflichtend einzubinden:

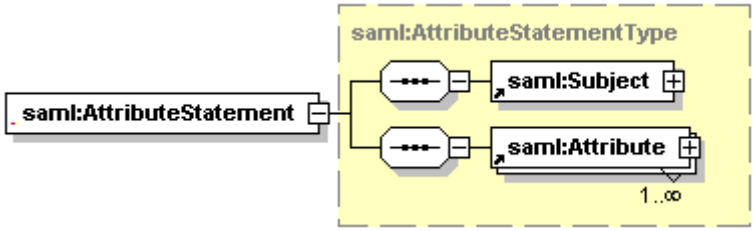
Name	Beschreibung
`saml:AttributeStatement`	Enthält die Kerndaten der Personenbindung
`dsig:Signature`	Die elektronische Signatur des Ausstellers der Bindung.

2.1.1 Beispiel

```
<?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

Das eingebundene `saml:AttributeStatement` enthält die Kerndaten der Personenbindung:



Name	Beschreibung
`saml:Subject`	Personendaten
`saml:Attribute`	Bezeichner für ein Zertifikat, dem die Stammzahl zugeordnet werden soll (verwendet wird als Bezeichner der öffentliche Schlüssel aus dem Zertifikat).

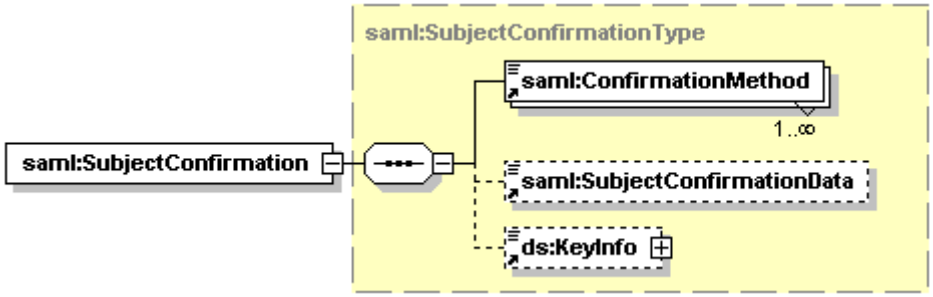
Dabei enthält `saml:Subject` die Daten der Person in Form der Personendaten-Struktur [PDat] und die `saml:Attribute` Elemente jeweils einen öffentlichen Schlüssel als Bezeichner eines zuzuordnenden Zertifikats in Form eines der `dsig:KeyValue` Sub-Elemente.

2.2.1 Personendaten

Die Struktur `saml:Subject` enthält genau das Element `saml:SubjectConfirmation`. In diesem Element wird `saml:ConfirmationMethod` auf den Wert `urn:oasis:names:tc:SAML:1.0:cm:sender-vouches`[1] gesetzt, während

[1] Der Sender (die Behörde) bürgt für den Inhalt. Der Empfänger kann den Wahrheitsgehalt der Kerndaten nicht überprüfen (nicht zu verwechseln mit der Prüfung der Authentizität der Daten mittels der Signatur der Behörde).

`saml:SubjectConfirmationData` enthält die Daten der Person in Form eines `pr:Person` Elements.



2.2.1.1 Personendaten für natürliche Personen

Das Element `pr:Person` MUSS vom Typ `pr:PhysicalPersonType` sein und genau folgende Daten enthalten:

Name	Beschreibung
`pr:Identification`	Die Stammzahl der Person. Enthält genau ein Element `pr:Type` mit Inhalt `urn:publicid:gv.at:baseid`, und ein Element `pr:Value`, das die base64 kodierte Stammzahl als Stringwert enthält.
`pr:Name`	Der Name der natürlichen Person. Enthält genau ein Element `pr:GivenName` (Vorname) und ein Element `pr:FamilyName` mit Attribut `primary="undefined"` (Familienname). Mehrere Vornamen bzw. Mehrfach-Familiennamen MÜSSEN in einem Element zusammengefasst werden.
`pr:DateOfBirth`	Geburtsdatum der Person

Beispiel

```
<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:Name>
    <pr:GivenName>Herbert</pr:GivenName>
    <pr:FamilyName primary="undefined">Gramgebeugt</pr:FamilyName>
  </pr:Name>
  <pr:DateOfBirth>1950-12-31</pr:DateOfBirth>
</pr:Person>
```

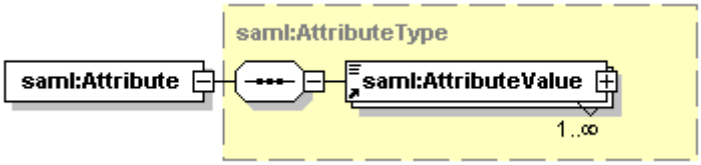
2.2.1.2 Personendaten für nichtnatürliche Personen

Personendaten für nichtnatürliche Personen (Firmen, Vereine, ...) werden in einer späteren Version dieses Dokumentes definiert.

2.2.2 Attribute

2.2.2.1 Attribute für natürliche Personen

Die Struktur `saml:Attribute` MUSS mindestens einmal, KANN auch mehrere Male vorkommen und enthält je einen öffentlichen Schlüssel der Person in Form von `dsig:KeyValue` Sub-Elementen, also `dsig:RSAKeyValue`, `dsig:DSAKeyValue` oder `xsd:any` (zur Speicherung von ECDSA-Schüsselwerten).



Im Attribut `AttributeName` ist der fixe Wert `CititzenPublicKey` anzugeben, im Attribut `AttributeNameSpace` der fixe Wert `urn:publicid:gv.at:namespaces:identitylink:1.2`.

2.2.2.2 Attribute für nichtnatürliche Personen

Attribute für nichtnatürliche Personen (Firmen, Vereine, ...) sind noch zu definieren.

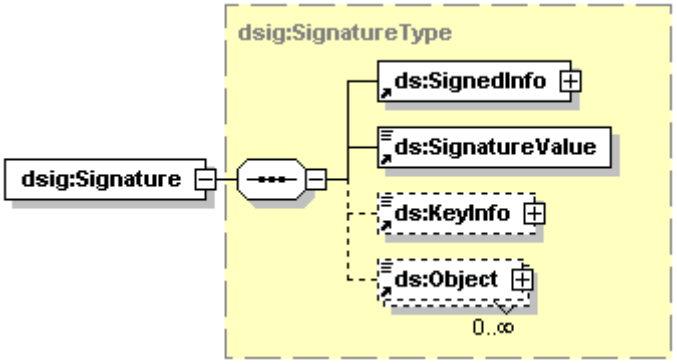
2.2.3 Beispiel

```
<saml:AttributeStatement
  xmlns:pr="http://reference.e-government.gv.at/namespace/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>Q9Hf8w1UM3mKwROWcuWiZ6Aucq8=</dsig:Exponent>
      </dsig:RSAKeyValue>
    </saml:AttributeValue>
  </saml:Attribute>
```

```
</saml:AttributeStatement>
```

2.3 Die elektronische Signatur

Die elektronische Signatur der `saml:Assertion` ist stark an das in [SAML 1.1] spezifizierte Profil von [XMLDSig] angelehnt.



Die Signatur enthält zwei `dsig:Reference` Elemente, die wie folgt ausgeführt werden MÜSSEN:

```
<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/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/TAgbOpxoc46+eEY=</dsig:DigestValue>
    </dsig:Reference>
  </dsig:SignedInfo>
  ...
</dsig:Signature>
```

Die Referenzen DÜRFEN auch mit anderen mit Mitteln und Transformationen ausgeführt werden, solange das Ergebnis identisch mit dem der aus den hier angeführten Referenzen resultierenden Ergebnis ist. Es wird jedoch EMPFOHLEN, den in den Beispielen gezeigten Referenzierungsmechanismus zu verwenden, der aus dem Profil für [XMLDSig] in [SAML 1.1] stammt.

Das zugehörige Manifest MUSS wie folgt aussehen:

```
<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>JaKFnaY5X742Xwk6KWz1Q5faO34=</dsig:DigestValue>
      </dsig:Reference>
    </dsig:Manifest>
  </dsig:Object>
</dsig:Signature>
```

Auch hier gilt wieder, dass die Referenz mit anderen Mitteln und Transformationen ausgeführt werden DARF, solange das Ergebnis identisch mit dem der aus den hier angeführten Referenzen resultierenden Ergebnis ist.

Das erste `dsig:Reference` Element referenziert die ganze `saml:Assertion` mit Ausnahme der Stammzahl. Das Attribut `URI` weist dabei auf das Dokument-Element, die `saml:Assertion`. Es werden der Reihe nach eine XPath-Transformation [XPath] welche die Stammzahl ausnimmt und die Enveloped-Signature Transformation durchgeführt.

Die zweite Referenz bezieht sich auf das Manifest. Das Manifest selbst enthält eine einzelne Referenz, die auf die vollständige `saml:Assertion` verweist. Die Transformation nimmt wieder das `dsig:Signature` Element aus.

Mit diesem Aufbau der Signatur ist es möglich, die Stammzahl aus der Personenbindung zu entfernen und trotzdem eine validierende Signatur nach XMLDSig zu haben.

Bei der erweiterten Validierung (Validierung des Manifests) ist die Stammzahl jedoch mit eingeschlossen.

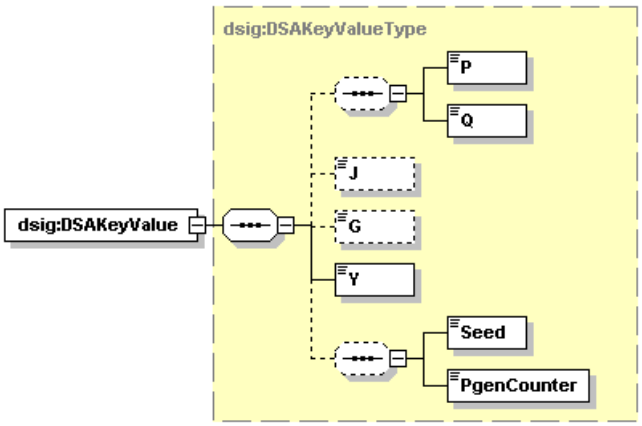
Weiters enthält die Signatur ein `ds:KeyInfo` Element, welches ausreichend Information für eine automatische Validierung der Signatur enthalten muss. Jedenfalls MUSS das X509 Signaturzertifikat eingebunden werden.

Ein vollständiges Beispiel einer Personenbindung ist in Abschnitt 5 zu finden.

3 Kodierungsvorschriften

Um die im folgenden Kapitel beschriebene komprimierte Darstellung nutzen zu können, sind folgende Kodierungsvorschriften verpflichtend umzusetzen:

- Für Base-64 kodierte Werte in `saml:Attribute` sowie in `dsig:DigestValue` darf die Base64-Darstellung ausschließlich die Zeichen “a”-“z”, “A”-“Z”, “0”-“9”, “+” und “/”, sowie abschließend (entsprechend den Base64-Regeln) bis zu zwei “=” verwenden. Zeilenumbrüche müssen nach exakt 76 Zeichen erfolgen; ist die abschließende Zeile 76 Zeichen lang wird vor dem End-Tag kein Zeilenumbruch mehr eingefügt.
- Falls ein `dsig:DSAKeyValue` verwendet wird, dann sind genau die Parameter `P`, `Q`, `G` und `Y` anzugeben. Die Parameter `J`, `seed` und `pGenCounter` dürfen nicht angegeben werden. Siehe auch [RFC3279], Abschnitt 2.3.2.



4 Komprimierte Darstellung

Die nachfolgend beschriebene komprimierte Speicherung ist als Vorschlag zu verstehen und muss nicht verbindlich im Sinne dieser Spezifikation umgesetzt werden.

Die beschriebene XML-Struktur der Personenbindung hat eine Größe von ca. 5KB, was für Speicherung auf Smartcards problematisch sein kann, da diese nur eine sehr begrenzte Speichermöglichkeit haben. Ein großer Teil der Personenbindungsstruktur besteht jedoch aus bekannten und fixierten Werten, welche jederzeit nachgebildet werden können. Für die komprimierte Speicherung bietet es sich daher an, nur die variablen Teile zu speichern.

Der XML-Syntax erlaubt Variabilitäten innerhalb der definierten Struktur (Zeilenumbrüche, Ort der Namespace-Deklarationen, Kommentare, ...). Um die vorliegende Spezifikation allerdings nicht zu restriktiv zu gestalten wird folgendes Vorgehensmodell gewählt: die komprimierte Speicherung enthält eine URL auf einen XSLT-Stylesheet der Personenbindung. Als Protokolle sind HTTP und HTTPS zulässig. Der Stylesheet enthält dabei die komplette XML-Struktur der Personenbindung, der dann die variablen Teile hinzugefügt werden. Die URL des Stylesheets SOLLTE nicht länger als 48 Zeichen sein.

Damit wird einerseits dem Problem der Variabilität begegnet, andererseits ist die konkrete Ausprägung keinen in Zukunft vielleicht einengenden Bestimmungen unterworfen.

Die Kodierung der komprimierten Speicherung erfolgt als ASN.1 DER-kodierte Folge von Zeichen [ASN1] [DER]. Für die Umsetzung mittels Stylesheets ist das komprimierte Format zunächst in ein XML-File zu wandeln (XML-Typ `il:CompressedIdentityLink`). Die Elementnamen entsprechen dabei den Namen der Elemente im ASN.1[2]. Eine Applikation erzeugt ausgehend von den ASN.1 Daten den `il:CompressedIdentityLink`, lädt den XSLT-Stylesheet von der angegebenen URL und führt eine Transformation durch, um die ursprüngliche Personenbindung zu erhalten.

4.1 ASN.1 Spezifikation

```
PersonenBindung ::= SEQUENCE {
   version INTEGER,
   issuerTemplate UTF8String,
   assertionID UTF8String,
   issueInstant UTF8String,
   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 {
   physcialPerson [0] PhysicalPersonData,
   corporateBody [1] CorporateBodyData
}
```

[2] Abgesehen von der Groß- und Kleinschreibung.

```
PhysicalPersonData ::= SEQUENCE {
   baseId UTF8String,
   givenName UTF8String,
   familyName UTF8String,
   dateOfBirth UTF8String
}

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

Der Typ CorporateBodyData ist derzeit noch undefiniert.

4.1.1 Erklärung zu einzelnen Feldern

- *version:* bezeichnet die Version des Formats zur komprimierten Speicherung (wird nicht in XML Darstellung übernommen). In der vorliegenden ASN.1-Struktur ist das Feld auf den Wert „1“ zu setzen.
- *issuerTemplate:* ist die URL von der der Stylesheet geladen werden kann. Da davon ausgegangen werden kann, dass die Anzahl der Stylesheets sehr beschränkt ist, können Bürgerkarten-Umgebungen die Stylesheets auch cachen.
- *assertionID:* einzufüllen in das Attribut `AssertionID` von `saml:Assertion`. Dabei ist zu beachten, dass falls das Template in diesem Attribut bereits Zeichen enthält, die *assertionID* angehängt wird. Damit kann z.Bsp. der gleich bleibende Teil, der die Issuer voneinander unterscheidet, auch im Template aufgenommen werden.
- *personData* und dazugehörender Typ *PhysicalPersonData:* sind in den entsprechenden Stellen einzusetzen.
- *citizenPublicKey:* bietet drei Möglichkeiten, einen öffentlichen Schlüssel als Bezeichner für das Zertifikat zu speichern:
  - *onToken:* die Information zur Gewinnung des öffentlichen Schlüssels befindet sich auf dem Security-Token (z.Bsp. in Form eines Zertifikats). Die Zahl dient als Ordnungsbegriff, falls mehrere solcher Informationen auf der Karte vorhanden sind – der Token gibt dabei die Nummerierung vor.
  - *referenceURL:* gibt eine URL an, unter der das bezeichnete DER-kodierte X509-Zertifikat abgerufen werden kann.
  - *x509Data:* enthält entsprechend der X509 Spezifikation [RFC2459] den öffentlichen Schlüssel (X509 Typ *SubjectPublicKeyInfo*)
  - Für die XML Darstellung ist *onToken* und *referenceURL* entsprechend aufzulösen und der Schlüsselwert einzusetzen.
- *signatureValue:* Wert der Signatur – muss noch Base64-kodiert werden, bevor er in die XML-Struktur eingefügt werden kann.
- *referenceDigest*, *referenceManigestDigest*, *manifestReferenceDigest:* optional die Hash-Werte der beiden Referenzen in der Signatur, sowie der Hash-Wert der Referenz im Manifest (*manifestReferenceDigest*). Die Werte müssen ebenfalls noch Base64-kodiert werden, bevor sie in die XML-Struktur eingefügt werden können. Optional deshalb, weil beim Befüllen der XML-Struktur diese Werte errechnet werden können. In der komprimierten XML-Struktur (Eingangsdaten für den Stylesheet) sind diese Felder aber

verpflichtend anzuführen, damit der Stylesheet die entsprechenden Felder in der Personenbindung ausfüllen kann.

Mit dieser Struktur kann eine Personenbindung in 100-150 Bytes gespeichert werden, wenn sich die öffentlichen Schlüssel abrufbar auf dem Token befinden, bzw. in ca. 400 Byte gespeichert werden, wenn die öffentlichen Schlüssel inkludiert werden.

Bei der Umwandlung der Personenbindung in die komprimierte ASN.1 Darstellung bzw. in die komprimierte XML-Darstellung (`il:CompressedIdentityLink`) muss darauf geachtet werden, die Werte identisch zu übernehmen, im Speziellen sind bei Elementwerten führende oder abschließende Leerzeichen oder Zeilenumbrüche mit zu übernehmen, um eine Bit-idente Rekonstruktion zu ermöglichen.

5 Beispiel

Das Beispiel zeigt eine vollständige Personenbindung für eine natürliche Person, mit Ausnahme der Werte der kryptographischen Daten (Hash-, Signatur, Schlüssel- und Zertifikatswerte).

5.1 Beispiel einer Personenbindung

```
<?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/namespace/persondata/20020228#"
  xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <saml:AttributeStatement>
    <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:AttributeStatement>
    <dsig:Signature xmlns:dsig="http://www.w3.org/2000/09/xmldsig#">
      <dsig:SignedInfo>
        <dsig:CanonicalizationMethod
          Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
        <dsig:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
        <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/2000/09/xmldsig#enveloped-signature"/>
          </dsig:Transforms>
          <dsig:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
          <dsig:DigestValue>Rv01PzN5sd4WVclcz/PTz/hqUIo=</dsig:DigestValue>
        </dsig:Reference>
        <dsig:Reference URI="#bka.gv.at+2004-02-24T12:00:00.000Z"
          Type="http://www.w3.org/2000/09/xmldsig#Manifest">
          <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:Transforms>
          <dsig:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
          <dsig:DigestValue>K/GKbymPaUtsr3Qh0De5uwHM9CU=</dsig:DigestValue>
        </dsig:Reference>
      </dsig:SignedInfo>
      <dsig:SignatureValue>...</dsig:SignatureValue>
      <dsig:KeyInfo>
        <dsig:X509Data>
          <dsig:X509Certificate>...</dsig:X509Certificate>
          <dsig:X509Certificate>...</dsig:X509Certificate>
          <dsig:X509Certificate>...</dsig:X509Certificate>
        </dsig:X509Data>
      </dsig:KeyInfo>
      <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:Transforms>
            <dsig:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
            <dsig:DigestValue>vHj9m+TpUI7zWjM+0QIgaiD/Lq0=</dsig:DigestValue>
          </dsig:Reference>
        </dsig:Manifest>
      </dsig:Object>
    </dsig:Signature>
</saml:Assertion>
```

5.2 Beispiel für komprimierte Darstellung

```
<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>
      <pr:DateOfBirth>1950-12-31</pr:DateOfBirth>
    </PersonData>
    <CitizenPublicKey>
      <dsig:RSAKeyValue>
        <dsig:Modulus> .... </dsig:Modulus>
        <dsig:Exponent> .... </dsig:Exponent>
      </dsig:RSAKeyValue>
    </CitizenPublicKey>
    <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>

```

Referenzen

ASN1

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

DER

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

PersDat

Hollosi, Arno und Reichstädter, Peter: XML-Spezifikation der Personen-Daten Struktur. Konvention zum e-Government Austria erarbeitet vom CIO des Bundes, Operative Unit. Öffentlicher Entwurf, Version 1.0.1, 24. April 2002. Abgerufen aus dem World Wide Web am 24. Februar 2004unter http://reference.e-government.at.

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. Abgerufen aus dem World Wide Web am 24. Februar 2004unter http://www.ietf.org/rfc/rfc3279.txt.

SAML 1.0

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

http://www.oasis-open.org/committees/security/

SAML 1.1

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

http://www.oasis-open.org/committees/security/

XPath

James Clark, Steve DeRose: XML Path Language (XPath). W3C Recommendation, November 1999. Abgerufen aus dem World Wide Web am 24. Februar 2004unter http://www.w3.org/TR/1999/REC-xpath-19991116.

XMLDSig

Donald Eastlake, Joseph Reagle und David Solo: XML-Signature Syntax and Processing. W3C Recommendation, Februar 2002. Abgerufen aus dem World Wide Web am 24. Februar 2004unter http://www.w3.org/TR/2002/REC-xmldsig-core-20020212.

Historie

Version	Datum	Kommentar
1.1.0	6. 5. 2002	• Umstellung auf SAML Version 1.0 vom 19. April 2002. • Vollständige Konformität mit SAML: o Verwendung von `AttributeStatement` statt eigenen Typs `PersonAttributeStatement` o `Assertion` ohne `ID` Attribut – Signatur-Referenzen nun mit XPointer Neue Referenzen: XPointer, XPath
Ersteller: Arno Hollosi		
1.1.1	6. 5. 2003	• Editoriale Verbesserungen
Ersteller: Gregor Karlinger		
1.2.0	14. 10. 2003	• Nomenklatur aktualisiert: Stammzahl, bereichspezifische Personenkennung • Referenzen aktualisiert. Beispiele überarbeitet; Signatur an Profil aus [SAML 1.1] angenähert.
Ersteller: Gregor Karlinger, Arno Hollosi		
1.2.1	24. 02. 2004	• Bezeichner für Austeller der Personenbindung geändert. • Bezeichner für die Stammzahl geändert. • Namenraum für das SAML-Attribut CitizenPublicKey geändert.
Ersteller: Gregor Karlinger		
1.2.2	14. 02. 2005	• Statt der Formulierung „juristische Person“ wird nun die Formulierung „nichtnatürliche Person“ verwendet. • Zeile 247-250: Der erste Teil des zweiten Satzes lautet nun „Das Attribut `URI` weist dabei auf das Dokument-Element,“ statt wie bisher „Das Attribut `URI` weist dabei auf das Dokument,“. • Zeilen 247-250: Fußnote 2 entfernt, da widersinnig. • Zeile 411 lautet nunmehr korrekt: „`<dsig:Modulus>...</dsig:Modulus>`“
Ersteller: Gregor Karlinger		