OSCI-Transport 1.2

– Korrigenda 02/2014 –

Status: Final

Koordinierungsstelle für IT-Standards (KoSIT)

Bremen, 20. Februar 2014

Inhaltsverzeichnis

1 Einleitung

1.1 Anlass der Korrigenda

Diese vierte Korrigenda zu OSCI Transport 1.2 [OSCI12] trägt den aktuellen Änderungen in der „Bekanntmachung zur elektronischen Singnatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen)“ der Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen vom 13. Januar 2014 [BNetzA_Alg] Rechnung.

Die Anpassungen betreffen RSA-Formatierungsverfahren für die Erzeugung von elektronischen Signaturen. In Verbindung mit den geeigneten und in der OSCI-Bibliothek bisher verwendeten Hashalgorithmen ergeben sich damit folgende Signaturalgorithmen:

Signaturalgorithmus	**geeignet bis Ende**
SHA-256 mit RSA und PKCS#1-v1_5	2016
SHA-256 mit RSA und PKCS#1-PSS	2020
SHA-512 mit RSA und PKCS#1-v1_5	2016
SHA-512 mit RSA und PKCS#1-PSS	2020

Alle diese Algorithmen sind für die angegebenen Zeiträume sowohl für die Anbringung als auch für die Prüfung qualifizierter elektronischer Signaturen von Zertifikaten und Inhaltsdaten zugelassen.

Des Weiteren wird die Liste der zulässigen Algorithmen für den Schlüsseltransport erweitert um den Algorithmus RSA-OAEP.

1.2 Copyright

Die vorliegende vierte Korrigenda der OSCI-Transport 1.2 - Spezifikation wurde im Auftrag der Koordinierungsstelle für IT-Standards als Herausgeber von der bremen online services GmbH & Co. KG erarbeitet.

1.3 Konventionen zur Textauszeichnung

Für diese Korrigenda gelten die gleichen Konventionen wie für die zugrunde liegende Spezifikation:

- Normative Absätze sind hellgrau unterlegt. Beispiel:

  Dieser Absatz ist normativ.

  In Zweifelsfällen gelten die Festlegungen in Schemata dieser Spezifikation *vor* normativen Textpassagen dieser Spezifikation. Diese gelten wiederum *vor* normativen Teilen referenzierter Dokumente und diese schließlich *vor* nicht normativen Teilen dieser Spezifikation.
- Änderungen der Korrigenda zur Spezifikation sind innerhalb der normativen Textpassagen **fett** gesetzt.
- Jede Art von Code ist in `Schreibmaschinenschrift` gesetzt.

2 Fortschreibungen der Spezifikation

Im Folgenden werden die einzelnen Änderungen mit Bezug auf die entsprechenden Kapitel der Spezifikation OSCI Transport 1.2 [OSCI12] detailliert beschrieben.

2.1 Kap. 4.1: Digitale Signaturen

Die Signaturalgorithmen, die von OSCI-Transport unterstützt werden, sind in der folgenden Tabelle aufgelistet.

Signatur-Algorithmus	**Algorithmus-Identifier**[1]
Signaturschema RSASSA-PKCS1-v1_5 [PKCS_1] mit Hash-Algorithmus SHA-256. Modullänge des RSA-Schlüsselpaares mind. 2048 Bit	**http://www.w3.org/2001/04/xmldsig-more#rsa-sha256**
Signaturschema RSASSA-PKCS1-v1_5 [PKCS_1] mit Hash-Algorithmus SHA-512. Modullänge des RSA-Schlüsselpaares mind. 2048 Bit	**http://www.w3.org/2001/04/xmldsig-more#rsa-sha512**
Signaturschema RSASSA-PKCS1-PSS [PKCS_1] (ohne Parameter) mit Hash-Algorithmus SHA-256 gemäß RFC 6931 [RFC6931]. Modullänge des RSA-Schlüsselpaares mind. 2048 Bit	**http://www.w3.org/2007/05/xmldsig-more#sha256-rsa-MGF1**
Signaturschema RSASSA-PKCS1-PSS [PKCS_1] (ohne Parameter) mit Hash-Algorithmus SHA-512 gemäß RFC 6931 [RFC6931]. Modullänge des RSA-Schlüsselpaares mind. 2048 Bit	**http://www.w3.org/2007/05/xmldsig-more#sha512-rsa-MGF1**
Signaturschema RSASSA-PKCS1-v1_5 [PKCS_1] mit Hash-Algorithmus RIPEMD-160[2]. Modullänge des RSA-Schlüsselpaares mind. 2048 Bit.	**http://www.w3.org/2001/04/xmldsig-more#rsa-ripemd160**
Signaturschema ECDSA-SHA* gemäß RFC 6931 [RFC6931] mit Hash-Algorithmus SHA-256	**http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha256**
Signaturschema ECDSA-SHA* gemäß RFC 6931 [RFC6931] mit Hash-Algorithmus SHA-512	**http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha512**

[1] gemäß [RFC6931]

[2] **Zu beachten:** ***RIPEMD-160 muss bei Signaturprüfung weiterhin unterstützt werden, die Verwendung bei der Signaturerzeugung ist nicht mehr zulässig!***

2.2 Kap. 4.2: Ver- und Entschlüsselung

Der letzte Absatz dieses Kapitels wird wie folgt geändert:

Die Verschlüsselung des Sitzungsschlüssels erfolgt mittels RSAES-PKCS1-v1_5 (Algorithmus-Identifier: http://www.w3.org/2001/04/xmlenc#rsa-1_5 [XENC1.1], Abschnitt 5.5.1) oder RSAES-OAEP (Algorithmus-Identifier: http://www.w3.org/2009/xmlenc11#rsa-oaep [XENC1.1], Abschnitt 5.5.2]). Die Modullänge des verwendeten RSA-Schlüsselpaares muss dabei mindestens 2048 Bit betragen.

2.3 Kap. 6.4: Ausprägung von XML-Signature

Geändert werden die Restriktionen zu `<SignatureMethodType>` (Algorithmen).

Diese Festlegungen gelten für Signaturprüfung sowie für Signaturerstellung; bei der Erstellung ist zu beachten, dass die RIPEMD-Algorithmen nicht mehr zugelassen sind (Einträge sind dunkel hinterlegt).

Für die Verwendung von XML-Signature bei OSCI-Transport gelten die folgenden Restriktionen:

```
<xsd:schema targetNamespace="http://www.w3.org/2000/09/xmldsig#"
            xmlns:xsd="http://www.w3.org/2001/XMLSchema"
            xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
            xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
            elementFormDefault="qualified">

  <xsd:import namespace="http://www.w3.org/2001/04/xmlenc#"
   schemaLocation="oscienc.xsd" />

  <xsd:annotation>
    <xsd:documentation xml:lang="de">
      OSCI 1.2 - Einschraenkung von XML-Signature Auftragsebene
    </xsd:documentation>
  </xsd:annotation>

  <!-- ### redefinitions ### -->

  <xsd:redefine schemaLocation="http://www.w3.org/TR/2001/CR-xmldsig-core-
20010419/xmldsig-core-schema.xsd">

    <xsd:complexType name="KeyInfoType">
      <xsd:complexContent>
        <xsd:restriction base="ds:KeyInfoType">
          <xsd:choice>
            <xsd:element ref="xenc:EncryptedKey" />
            <xsd:element ref="ds:RetrievalMethod" />
            <xsd:element ref="ds:X509Data" />
          </xsd:choice>
          <xsd:attribute name="Id" type="xsd:ID" use="optional" />
        </xsd:restriction>
      </xsd:complexContent>
    </xsd:complexType>

    <xsd:complexType name="ReferenceType">
      <xsd:complexContent>
        <xsd:restriction base="ds:ReferenceType">
```

```
        <xsd:sequence>
          <xsd:element ref="ds:Transforms" />
          <xsd:element ref="ds:DigestMethod" />
          <xsd:element ref="ds:DigestValue" />
        </xsd:sequence>
        <xsd:attribute name="URI" type="xsd:anyURI" use="optional" />
      </xsd:restriction>
    </xsd:complexContent>
  </xsd:complexType>

  <xsd:complexType name="SignatureType">
    <xsd:complexContent>
      <xsd:restriction base="ds:SignatureType">
        <xsd:sequence>
          <xsd:element ref="ds:SignedInfo" />
          <xsd:element ref="ds:SignatureValue" />
          <xsd:element ref="ds:KeyInfo" />
          <xsd:element ref="ds:Object"
           minOccurs="0" maxOccurs="unbounded"/>
        </xsd:sequence>
      </xsd:restriction>
    </xsd:complexContent>
  </xsd:complexType>

  <xsd:complexType name="SignatureValueType">
    <xsd:simpleContent>
      <xsd:restriction base="ds:SignatureValueType">
        <xsd:attribute name="Id" type="xsd:ID" use="optional"/>
      </xsd:restriction>
    </xsd:simpleContent>
  </xsd:complexType>

  <xsd:complexType name="RetrievalMethodType">
    <xsd:complexContent>
      <xsd:restriction base="ds:RetrievalMethodType">
        <xsd:attribute name="URI" type="xsd:anyURI" use="required" />
        <xsd:attribute name="Type">
          <xsd:simpleType>
            <xsd:restriction base="xsd:anyURI">
              <xsd:enumeration
               value="http://www.w3.org/2000/09/xmldsig#X509Data" />
            </xsd:restriction>
          </xsd:simpleType>
        </xsd:attribute>
      </xsd:restriction>
    </xsd:complexContent>
  </xsd:complexType>

  <xsd:complexType name="X509DataType">
    <xsd:complexContent>
      <xsd:restriction base="ds:X509DataType">
```

```
        <xsd:sequence maxOccurs="1">
          <xsd:element name="X509Certificate" type="xsd:base64Binary" />
        </xsd:sequence>
      </xsd:restriction>
    </xsd:complexContent>
  </xsd:complexType>

  <xsd:complexType name="CanonicalizationMethodType">
    <xsd:complexContent>
      <xsd:restriction base="ds:CanonicalizationMethodType">
        <xsd:attribute name="Algorithm" use="required">
          <xsd:simpleType>
            <xsd:restriction base="xsd:anyURI">
              <xsd:enumeration
               value=”http://www.w3.org/TR/2001/REC-xml-c14n-20010315" />
            </xsd:restriction>
          </xsd:simpleType>
        </xsd:attribute>
      </xsd:restriction>
    </xsd:complexContent>
  </xsd:complexType>

  <xsd:complexType name="DigestMethodType">
    <xsd:complexContent>
      <xsd:restriction base="ds:DigestMethodType">
        <xsd:attribute name="Algorithm" use="required">
          <xsd:simpleType>
            <xsd:restriction base="xsd:anyURI">
              <xsd:enumeration
               value="http://www.w3.org/2001/04/xmlenc#sha256" />
              <xsd:enumeration
               value="http://www.w3.org/2001/04/xmlenc#sha512" />
              <xsd:enumeration
               value="http: //www.w3.org/2001/04/xmlenc#ripemd160" />
            </xsd:restriction>
          </xsd:simpleType>
        </xsd:attribute>
      </xsd:restriction>
    </xsd:complexContent>
  </xsd:complexType>

  <xsd:complexType name="SignatureMethodType">
    <xsd:complexContent>
      <xsd:restriction base="ds:SignatureMethodType">
        <xsd:attribute name="Algorithm" use="required">
          <xsd:simpleType>
            <xsd:restriction base="xsd:anyURI">
              <xsd:enumeration
             value="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256" />
              <xsd:enumeration
             value="http://www.w3.org/2001/04/xmldsig-more#rsa-sha512" />
```

```
                <xsd:enumeration value=
                 "http:// www.w3.org/2001/04/xmldsig-more#rsa-ripemd160" />
                <xsd:enumeration value=
                 "http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha256" />
                <xsd:enumeration value=
                 "http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha512" />
                <xsd:enumeration
          value="http://www.w3.org/2007/05/xmldsig-more#sha256-rsa-MGF1" />
                <xsd:enumeration
          value="http://www.w3.org/2007/05/xmldsig-more#sha512-rsa-MGF1" />
              </xsd:restriction>
            </xsd:simpleType>
          </xsd:attribute>
        </xsd:restriction>
      </xsd:complexContent>
    </xsd:complexType>
  </xsd:redefine>
</xsd:schema>
```

2.4 Kap. 6.5: Ausprägung von XML-Encryption

Für die Verwendung von XML-Encryption bei OSCI-Transport gelten die folgenden Restriktionen:

```
<xsd:schema targetNamespace="http://www.w3.org/2001/04/xmlenc#"
             xmlns:xsd="http://www.w3.org/2001/XMLSchema"
             xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
             xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
             elementFormDefault="qualified">
    <xsd:annotation>
       <xsd:documentation xml:lang="de">
           OSCI 1.2 - Einschraenkung von XML Encryption Auftragsebene
       </xsd:documentation>
    </xsd:annotation>
<!-- ### redefinitions ### -->
  <xsd:redefine
    schemaLocation="http://www.w3.org/TR/xmlenc-core/xenc-schema.xsd">
      <xsd:complexType name="EncryptionMethodType">
        <xsd:complexContent>
          <xsd:restriction base="xenc:EncryptionMethodType">
            <xsd:sequence>
              <xsd:element name="KeySize" minOccurs="0"
                    type="xenc:KeySizeType" />
            </xsd:sequence>
            <xsd:attribute name="Algorithm" use="required">
            <xsd:simpleType>
              <xsd:restriction base="xsd:anyURI">
                <xsd:enumeration
              value="http://www.w3.org/2001/04/xmlenc#tripledes-cbc" />
                <xsd:enumeration
              value="http://www.w3.org/2001/04/xmlenc#aes128-cbc" />
                <xsd:enumeration
              value="http://www.w3.org/2001/04/xmlenc#aes192-cbc" />
```

```
              <xsd:enumeration
             value="http://www.w3.org/2001/04/xmlenc#aes256-cbc" />
              <xsd:enumeration
             value="http://www.w3.org/2001/04/xmlenc#rsa-1_5" />
              <xsd:enumeration
             value="http://www.w3.org/2009/xmlenc11#rsa-oaep" />
              </xsd:restriction>
             </xsd:simpleType>
           </xsd:attribute>
         </xsd:restriction>
       </xsd:complexContent>
     </xsd:complexType>
     <xsd:complexType name="CipherReferenceType">
       <xsd:complexContent>
         <xsd:restriction base="xenc:CipherReferenceType">
           <xsd:attribute name="URI" type="xsd:anyURI" use="required"/>
         </xsd:restriction>
     </xsd:complexContent>
   </xsd:complexType>
   <xsd:complexType name="EncryptedDataType EncryptedDataType">
     <xsd:complexContent>
       <xsd:restriction base="xenc:EncryptedDataType">
         <xsd:sequence>
           <xsd:element name="EncryptionMethod"
               type="xenc:EncryptionMethodType" minOccurs="0" />
           <xsd:element ref="ds:KeyInfo" minOccurs="0" />
           <xsd:element ref="xenc:CipherData" minOccurs="1" />
         </xsd:sequence>
         <xsd:attribute name="MimeType" type="xsd:string" use="optional" />
       </xsd:restriction>
     </xsd:complexContent>
   </xsd:complexType>
   <xsd:complexType name="EncryptedKeyType">
     <xsd:complexContent>
       <xsd:restriction base="xenc:EncryptedKeyType">
         <xsd:sequence>
           <xsd:element name="EncryptionMethod"
                     type="xenc:EncryptionMethodType" minOccurs="1" />
           <xsd:element ref="ds:KeyInfo" minOccurs="1" />
           <xsd:element ref="xenc:CipherData" minOccurs="1" />
         </xsd:sequence>
       </xsd:restriction>
       </xsd:complexContent>
     </xsd:complexType>
  </xsd:redefine>
</xsd:schema>
```

3 Literaturverzeichnis

[BNetzA_Alg] Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen); die Veröffentlichung des Algorithmenkatalogs der Bundesnetzagentur mit Stand vom 13. Januar 2014 im Bundesanzeiger wird in Kürze erwartet:

http://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/QES/Veroeffentlichungen/Algorithmen/2014Algorithmenkatalog.pdf?__blob=publicationFile&v=1

[OSCI12] OSCI Transport 1.2 – Spezifikation; OSCI Leitstelle 2002, http://www.xoev.de/detail.php?gsid=bremen83.c.2472.de

[PKCS_1] J. Jonsson, J. Staddon: Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1. RFC 3447, February 2003. Online verfügbar unter http://www.ietf.org/rfc/rfc3447.txt

[RFC6931] Additional XML Security Uniform Resource Identifiers (URI), Internet Engeneering Task Force RFC 6931, April 2013, http://www.ietf.org/rfc/rfc6931.txt

[XENC1.1] XML Encryption Syntax and Processing Version 1.1, W3C Recommendation 11 April 2013, http://www.w3.org/TR/2013/REC-xmlenc-core1-20130411/