OSCI-Transport 1.2

– Korrigenda 3/2017 –

Status: Final

Koordinierungsstelle für IT-Standards (KoSIT)

Bremen, 30. März 2017

Inhaltsverzeichnis

1 Einleitung

1.1 Anlass der Korrigenda

Diese fünfte Korrigenda zu OSCI Transport 1.2 [OSCI12] führt den GCM-Modus für AES-Verfahren als Alternative zum CBC-Modus ein. Für die Verwendung des CBC-Modus sind serverseitig zusätzliche Sicherheitsmaßnahmen nötig [BSITR-02102-1]. Mit dieser Korrigenda wird eine zukünftige Ablösung des CBC-Modus durch den GCM-Modus vorbereitet.

WICHTIG: Für die Kommunikation ist zu beachten, dass beide Kommunikationspartner den verwendeten Modus unterstützen müssen.

Die Anpassungen betreffen die Padding-Verfahren für den Blockverschlüsselungsalgorithmus AES. In Verbindung mit den geeigneten und in der OSCI-Bibliothek bisher verwendeten AES-Algorithmen stehen nunmehr folgende Padding-Verfahren zur Verfügung:

- AES-128 mit CBC
- AES-192 mit CBC
- AES-256 mit CBC
- AES-128 mit GCM
- AES-192 mit GCM
- AES-256 mit GCM

Außerdem trägt diese Korrigenda den Änderungen in der „Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen)“ der Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen vom 15.03.2016 [BNetzA_Alg16] und 30. Dezember 2016 [BNetzA_Alg17] Rechnung.

Es wurde die Liste der geeigneten Hashfunktionen um SHA3-256, SHA3-384 und SHA3-512 erweitert.

Die Unterstützung des Padding-Verfahrens RSA-PKCS#1-v1.5 wurde um ein Jahr, bis Ende 2017, verlängert.

1.2 Copyright

Die vorliegende fünfte Korrigenda der OSCI-Transport 1.2 - Spezifikation wurde im Auftrag der Koordinierungsstelle für IT-Standards als Herausgeber von der Governikus 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 Kapitel 4.1: Digitale Signaturen

In der folgenden Tabelle sind die Algorithmen aufgeführt, die bei OSCI-Transport zur Erzeugung von Hashwerten für qualifizierte Signaturen verwendet werden dürfen.

Hash-Algorithmus	**Algorithmus-Identifier gemäß [RFC6931]**
SHA-256	`http://www.w3.org/2001/04/xmlenc#sha256`
SHA-512	`http://www.w3.org/2001/04/xmlenc#sha512`
SHA3-256	**`http://www.w3.org/2007/05/xmldsig-more#sha3-256`**
SHA3-384	**`http://www.w3.org/2007/05/xmldsig-more#sha3-384`**
SHA3-512	**`http://www.w3.org/2007/05/xmldsig-more#sha3-512`**

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

Signatur-Algorithmus	**Algorithmus-Identifier gemäß [RFC6931]**
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. 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. Modullänge des RSA-Schlüsselpaares mind. 2048 Bit	`http://www.w3.org/2007/05/xmldsig-more#sha512-rsa-MGF1`

Signatur-Algorithmus	**Algorithmus-Identifier gemäß [RFC6931]**
Signaturschema ECDSA-SHA*mit Hash-Algorithmus SHA-256 mit Länge q ≥ 250 Bit	`http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha256`
Signaturschema ECDSA-SHA* mit Hash-Algorithmus SHA-512 mit Länge q ≥ 250 Bit	`http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha512`
Signaturschema RSASSA-PKCS1-PSS [PKCS_1] (ohne Parameter) mit Hash- Algorithmus SHA3-256. Modullänge des RSA-Schlüsselpaares mind. 2048 Bit	**`http://www.w3.org/2007/05/xmldsig-more#sha3-256-rsa-MGF1`**
Signaturschema RSASSA-PKCS1-PSS [PKCS_1] (ohne Parameter) mit Hash- Algorithmus SHA3-384. Modullänge des RSA-Schlüsselpaares mind. 2048 Bit	**`http://www.w3.org/2007/05/xmldsig-more#sha3-384-rsa-MGF1`**
Signaturschema RSASSA-PKCS1-PSS [PKCS_1] (ohne Parameter) mit Hash- Algorithmus SHA3-512. Modullänge des RSA-Schlüsselpaares mind. 2048 Bit	**`http://www.w3.org/2007/05/xmldsig-more#sha3-512-rsa-MGF1`**

2.2 Kapitel 4.2 Ver- und Entschlüsselung

Der erste Absatz wird wie folgt geändert:

Die Verschlüsselung erfolgt gemäß [XENC] wobei ein Hybridverschlüsselungsalgorithmus eingesetzt wird. Für den Einsatz der Verfahren sollten die Empfehlungen des BSI berücksichtigt werden [BSITR02102].

Die Tabelle im vierten Absatz wird wie folgt ergänzt:

Die symmetrischen Verschlüsselungsalgorithmen, die bei OSCI-Transport zur Verschlüsselung der eigentlichen Daten verwendet werden können, sind in der folgenden Tabelle zusammengestellt.

Verschlüsselungsalgorithmus	**Algorithmus-Identifier**
Two-Key-Triple-DES	`http://www.w3.org/2001/04/xmlenc#tripledes-cbc [XENC1.1, Abschnitt 5.2.2]`
AES-128 mit CBC	`http://www.w3.org/2001/04/xmlenc#aes128-cbc [XENC1.1, Abschnitt 5.2.3]`
AES-192 mit CBC	`http://www.w3.org/2001/04/xmlenc#aes192-cbc [XENC1.1, Abschnitt 5.2.3]`
AES-256 mit CBC	`http://www.w3.org/2001/04/xmlenc#aes256-`

Verschlüsselungsalgorithmus	Algorithmus-Identifier
	`cbc [XENC1.1, Abschnitt 5.2.3]`
AES-128 mit GCM	**`http://www.w3.org/2009/xmlenc11#aes128-gcm [XENC1.1, Abschnitt 5.2.4]`**
AES-192 mit GCM	**`http://www.w3.org/2009/xmlenc11#aes192-gcm [XENC1.1, Abschnitt 5.2.4]`**
AES-256 mit GCM	**`http://www.w3.org/2009/xmlenc11#aes256-gcm [XENC1.1, Abschnitt 5.2.4]`**

Der Absatz 5 wird wie folgt geändert:

[XENC1.1] und [BSITR02102] umfassen Vorgaben, wie diese Algorithmen benutzt werden müssen. Diese Vorgaben sind zu beachten. Darunter sind insbesondere folgende Vorgaben:

- Für den Einsatz des GCM ist zu beachten, dass sich die Initialisierungsvektoren innerhalb der Lebensdauer eines Authentisierungsschlüssels nicht wiederholen dürfen. Für den im GCM integrierten Authentisierungsmechanismus müssen sichere Noncen erzeugt werden. Die Länge der GCM-Prüfsummen sollte mindestens 96 Bit betragen.
- Beim CBC-Mode ist darauf zu achten, dass ein Angreifer nicht anhand von Fehlermeldungen oder anderen Seitenkanälen erfahren kann, ob das Padding eines eingespielten Datenpakets korrekt war.
- Für die Erzeugung von Initialisierungsvektoren sind Verfahren zu verwenden die sicherstellen, dass die Initialisierungsvektoren unvorhersagbar sind, z.B. zufällige oder verschlüsselte Initialisierungsvektoren gem. [BSITR02102] Abschnitt B.2.
- Das Padding ist unter Berücksichtigung der Vorgaben in [XENC1.1] und [BSITR02102] vorzunehmen.

2.3 Kapitel 6.4: Ausprägung von XML-Signature

Geändert werden die Algorithmen in <SignatureMethodType> und <DigestMethodType>

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:complexContnt>
     </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:complexConten
       >
     </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/2007/05/xmldsig-more#sha3-256“ />
                <xsd:enumeration
                 value="http://www.w3.org/2007/05/xmldsig-more#sha3-384“ />
                <xsd:enumeration
                 value="http://www.w3.org/2007/05/xmldsig-more#sha3-512“ />
              </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#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:enumeration value=
                 "http://www.w3.org/2007/05/xmldsig-more#sha3-256-rsa-MGF1"/
                 <xsd:enumeration value=
                 "http://www.w3.org/2007/05/xmldsig-more#sha3-384-rsa-MGF1"/
                 <xsd:enumeration value=
                 "http://www.w3.org/2007/05/xmldsig-more#sha3-512-rsa-MGF1"/
              </xsd:restriction>
            </xsd:simpleType>
          </xsd:attribute>
</xsd:restriction>
</xsd:complexContent>
    </xsd:complexType>
  </xsd:redefine>
</xsd:schema>
```

2.4 Kapitel 6.5: Ausprägung von XML-Encryption

```
<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:enumeration value=
             "http://www.w3.org/2009/xmlenc11#aes128-gcm "/>
```

```
                <xsd:enumeration value=
               "http://www.w3.org/2009/xmlenc11#aes192-gcm" />
                <xsd:enumeration value=
               "http://www.w3.org/2009/xmlenc11#aes256-gcm" />
              </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

Die Literaturquellen werden wie folgt ergänzt bzw. aktualisiert:

[BNetzA_Alg16] Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen); Veröffentlicht auf den Internetseiten des Bundesanzeigers (www.bundesanzeiger.de) unter "**BAnz AT 14.04.2016 B11“**

[BNetzA_Alg17] Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen); Veröffentlicht auf den Internetseiten des Bundesanzeigers (www.bundesanzeiger.de) unter "**BAnz AT 30.12.2016 B5“**

[BSITR02102] Bundesamt für Sicherheit in der Informationstechnik (BSI), Technische Richtlinie Kryptographische Verfahren: Empfehlungen und Schlüssellängen. Februar 2017, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102.pdf.

[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

[XENC] Takeshi Imamura, Blair Dillaway, Ed Simon: XML Encryption Syntax and Processing. W3C Candidate Recommendation 04 March 2002. Online verfügbar unter http://www.w3.org/TR/2002/CR-xmlenc-core-20020304/. Es handelt sich um „Work in progress“. Für diese Spezifikation maßgebend ist die angegebene Version, die von der aktuellen Version (online verfügbar unter http://www.w3.org/TR/xmlenc-core/) abweichen kann

[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/