Koordinierungsstelle
für IT-Standards

OSCI-Transport 1.2

– Korrigenda 2/2020 –

Status: Final

Koordinierungsstelle für IT-Standards (KoSIT)

Bremen, 13. Februar 2020

Inhaltsverzeichnis

1 Einleitung

1.1 Anlass der Korrigenda

Die vorliegende sechste Korrigenda zu OSCI Transport 1.2 [OSCI12] ergänzt eine Angabe der Länge des Initialisierungsvektors für AES-GCM bei der Angabe des Verschlüsselungsalgorithmus. Mit dieser Korrigenda entsteht die Version 8 der Spezifikation OSCI Transport 1.2 (kurz: OSCI 1.2 Version 8) und sie begleitet die Änderungen an der OSCI 1.2-Bibliothek zur Version 1.9.0.

Dies ist notwendig, um alternativ zu Initialisierungsvektoren der Längen 64 Bit oder 128 Bit auch eine Länge von 96 Bit zu ermöglichen. Ein Initialisierungsvektor der Länge 96 Bit entspricht der Vorgabe in der W3C Spezifikation [XENC1.1] und der Vorgabe des Bundesamtes für Sicherheit in der Informationstechnik (BSI) für die Übertragung hoheitlicher Daten. Das BSI stellt mit seiner Vorgabe klar, dass konform zur [XENC1.1] ein Initialisierungsvektor mit einer Länge von 96 Bit gegenüber einer Länge von 128 Bit vorzuziehen ist. Aus diesen Gründen muss die OSCI-Bibliothek eine Länge von 96 Bit für Initialisierungsvektoren standardmäßig vorgeben und einen geordneten Umstieg ermöglichen.

Um einen geordneten Umstieg auf einen Initialisierungsvektor mit einer Länge von 96 Bit (12 Byte) zu ermöglichen, führt diese Korrigenda ein optionales, zusätzliches Element bei der XML-EncryptionMethod ein. Hiermit lässt sich der Initialisierungsvektor umstellen. Das Ziel der Korrigenda ist es, ab Februar 2021 die standardmäßige Verwendung von Initialisierungsvektoren mit der Länge 96 Bit zu erreichen, um den entsprechenden Vorgaben zu genügen.

1.2 Copyright

Die vorliegende sechste Korrigenda der Spezifikation OSCI-Transport 1.2 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 4.2 Ver- und Entschlüsselung

Der erste Absatz wird wie folgt ergänzt:

Der Initialisierungsvektor für AES-GCM soll immer mit einer Länge von 96 Bit erzeugt und verwendet werden. Ein Initialisierungsvektor mit einer Länge von 128 Bit oder 64 Bit sollte nicht verwendet werden.

Sofern ein Initialisierungsvektor mit einer Länge von 128 Bit verwendet wird, wird empfohlen, auf die standardkonforme Länge von 96 Bit des Initialisierungsvektors für AES-GCM zu wechseln.

2.2 Kapitel 6.3 Globale Typdefinitionen

Am Ende Kapitels wird zusätzlich folgende Typdefinition angefügt:

```
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
            xmlns:osci128="http://xoev.de/transport/osci12/8"
            targetNamespace="http://xoev.de/transport/osci12/8"
            elementFormDefault="qualified"
            attributeFormDefault="unqualified">

      <xsd:annotation>

            <xsd:documentation xml:lang="de">

            OSCI 1.2 Version 8 - Definition der Länge des
            Initialisierungsvektors für AES-GCM in Byte

            </xsd:documentation>

      </xsd:annotation>

      <xsd:element name="IvLength" type="osci128:IvLengthType"/>

      <xsd:complexType name="IvLengthType">

            <xsd:attribute name="Value" type="xsd:positiveInteger"
                           use="required"/>

      </xsd:complexType>

</xsd:schema>
```

2.3 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" />

               <!-- Hier wird die Länge des Initialisierungsvektor für
                     AES-GCM angegeben -->

               <any namespace="##other" minOccurs="0"
                     maxOccurs="unbounded"/>

            </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>
```

Als weitere Definition für die Syntax von XML-Encryption wird folgende Definition eingefügt:

Eine Länge des Initialisierungsvektors für AES-GCM von 96Bit bzw. 12 Byte wird folgendermaßen in einem `EncryptionMethod` Element angegeben:

```
<osci128:IvLength xmlns:osci128=”http://xoev.de/transport/osci12/8” Value="12" />
```

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/