Koordinierungsstelle
für IT-Standards

OSCI-Transport 1.2
– 12/2020 –
Status: Final

Korrigenda Nr. 7

gültig ab: 01.02.2021

Koordinierungsstelle für IT-Standards (KoSIT)

Bremen, 15. Dezember 2020

Inhaltsverzeichnis

1 Einleitung

1.1 Anlass der Korrigenda

Die vorliegende siebte Korrigenda zu OSCI Transport 1.2 [OSCI12] gibt die Verwendung eines 96 Bit Initialisierungsvektors als Standardwert für AES-GCM vor und stellt die Verwendung der Attribute ConversationId und SequenceNumber im Abwicklungsauftrag (MediateDelivery) frei (optionale Attribute).

Mit dieser Korrigenda entsteht die Version 9 der Spezifikation OSCI Transport 1.2 (kurz: OSCI 1.2 Version 9) und sie begleitet die Änderungen an der OSCI 1.2-Bibliothek zur Version 2.0.0.

Die Vorgabe eines Initialisierungsvektors 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 der bisherigen verwendeten Länge von 128 Bit vorzuziehen ist. Aus diesen Gründen muss die OSCI-Bibliothek eine Länge von 96 Bit für Initialisierungsvektoren standardmäßig vorgeben.

Um einen geordneten Umstieg und eine Rückwärtskompatibilität zu ermöglichen, können Initialisierungsvektoren der Längen 64 Bit oder 128 Bit zwar weiterhin verwendet werden, ihre Verwendung und damit die Abweichung von den Vorgaben der W3C Spezifikation und der Vorgabe des BSI muss jedoch mit dem Warnhinweis „Non-standard initialization vector“ protokolliert werden.

Im Abwicklungsauftrag (MediateDelivery) ist kein Dialog erforderlich, die zugehörigen, dialogspezifischen Attribute ConversationId und SequenceNumber sind dementgegen in der Struktur ControlBlockType („Schema für Abwicklungsaufträge“ auf Seite 123 der Spezifikation) jedoch als Pflichtangaben festgelegt („required“). Im Rahmen der Qualitätssicherung wurden die Vorgabe für diese Attribute von vormals „required“ auf nunmehr „optional“ geändert und somit die Deklaration der Spezifikation angepasst.

Die vorliegende Korrigenda ist gültig ab dem 01.02.2021.

1.2 Copyright

Die vorliegende siebte 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 zugrundeliegende 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 geändert:

Der Initialisierungsvektor für AES-GCM muss immer mit einer Länge von 96 Bit erzeugt und verwendet werden. Aus Gründen der Rückwärtskompatibilität und um einen Wechsel der Länge des Initialisierungsvektors zu unterstützen, kann abweichend weiterhin ein Initialisierungsvektor mit einer Länge von 128 Bit oder 64 Bit verwendet werden. Wird ein Initialisierungsvektor mit einer anderen Länge als 96 Bit verwendet, müssen Implementierungen dies deutlich ausweisen (Warnhinweis: „Non-standard initialization vector“).

2.2 Kapitel 6.6.10 Zustellungsabholantwort

Auf Seite 90 unten wird der responseToFetchDeliveryType wie folgt geändert:

```
<xsd:complexType name="responseToFetchDeliveryType">
    <xsd:complexContent>
      <xsd:extension base="osci:DefaultHeaderBlockTemplate">
        <xsd:sequence>
          <xsd:element name="Feedback" type="osci:FeedbackType" />
          <xsd:element name="fetchDelivery">
            <xsd:complexType>
              <xsd:sequence>
                <xsd:any namespace="http://www.osci.de/2002/04/osci"
                 minOccurs="0" maxOccurs="unbounded" processContents="strict"/>
              </xsd:sequence>
            </xsd:complexType>
          </xsd:element>
          <xsd:element name="ProcessCardBundle"
           type="osci:ProcessCardBundleType" minOccurs="0" />
        </xsd:sequence>
      </xsd:extension>
    </xsd:complexContent>
  </xsd:complexType>
</xsd:complexType>
```

2.3 Kapitel 6.6.14 Weiterleitungsantwort

Auf Seite 108 und 109 unten wird der ControlBlockType wie folgt geändert:

```
<xsd:complexType name="ControlBlockType">
  <xsd:complexContent>
    <xsd:restriction base="osci:ControlBlockTemplate">
      <xsd:sequence>
        <xsd:element name="Response" type="xsd:string" minOccurs="1" />
```

```
        <xsd:element name="Challenge" type="xsd:string" minOccurs="0" />
      </xsd:sequence>
      <xsd:attribute name="ConversationId" type="osci:Number" use="optional" />
      <xsd:attribute name="SequenceNumber" type="osci:Number" use="optional" />
    </xsd:restriction>
  </xsd:complexContent>
</xsd:complexType>
```

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/