OSCI-Transport 1.2

– Korrigenda 02/2008 –

Status: Final

OSCI Leitstelle

Bremen, 10. April 2008

Inhaltsverzeichnis

1 Einleitung

1.1 Anlass der Korrigenda

Diese Korrigenda zu OSCI Transport 1.2 [OSCI12] berücksichtigt Anpassungen, die sich ergeben aus der „Bekanntmachung zur elektronischen Signatur nach Signaturgesetz und Signaturverordnung (Übersicht über geeignete Algorithmen)“, veröffentlicht im Bundesanzeiger Nr. 69 vom 22. April 2007 [BNetzA_Alg]. In diesem Algorithmenkatalog ist eine generelle Eignung von SHA-1 zur Erstellung qualifizierter elektronischer Signaturen bis Ende 2009 angegeben.

Dazu hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) wie folgt Stellung genommen: „Diese Frist wird im nächsten Algorithmenkatalog deutlich verkürzt werden. Es ist daher dringend geboten, falls noch nicht geschehen, umgehend eine entsprechende Umstellung der für das Signieren "im Feld" verwendeten Kryptokomponenten auf weiterhin kollisionsresistente Hashfunktionen einzuleiten.“[1] Mit [BSI_Alg2008] hat das BSI einen Entwurf für einen Algorithmenkatalog vorgelegt, der nach Abstimmung in der Fachöffentlichkeit im Januar 2008 vorgelegt werden soll; der Entwurf enthält folgende Hinweise:

„Folgende Hashfunktionen mit verschiedenen Hashwert-Längen (SHA-224 ist eine 224-Bit Hashfunktion etc.) sind geeignet, ein langfristiges Sicherheitsniveau zu gewährleisten:

• SHA-224, SHA-256, SHA-384, SHA-512 [2].

Diese vier letzteren Hashfunktionen sind (mindestens) in den **kommenden sieben Jahren**, d.h. **bis Ende 2014**, für die Anwendung bei qualifizierten elektronischen Signaturen geeignet.

Die folgende Tabelle fasst die Eignung der Hashfunktionen zusammen.

geeignet bis Ende **2007**	Erzeugung qualifizierter Zertifikate*: geeignet bis Ende **2009**	geeignet bis Ende **2009**	Erzeugung qualifizierter Zertifikate**: geeignet bis Ende **2010**	geeignet bis Ende **2014**[1]
SHA-1	SHA-1	RIPEMD-160	SHA-1, RIPEMD-160	SHA-224, SHA-256, SHA-384, SHA-512 (SHA-1***, RIPEMD-160)

*d.h. zur Erzeugung qualifizierter Zertifikate, nicht aber zur Erzeugung und Prüfung anderer qualifiziert signierter Daten. ** d.h. zur Erzeugung qualifizierter Zertifikate bei ≥20 Bit Entropie der Seriennummer, nicht aber zur Erzeugung und Prüfung anderer qualifiziert signierter Daten. ***ausschließlich zur Prüfung qualifizierter Zertifikate.“ (S.3, [BSI_Alg2008])

Bzgl. des Modulus des RSA-Signaturverfahrens wird die Empfehlung einer Schlüssellänge von 2048 Bit mit einer voraussichtlichen Reichweite bis zum Jahr 2014 gegeben.

Es wird allgemein davon ausgegangen, dass es bzgl. der Reichweite des Einsatzes von SHA-1 eine Übergangsfrist geben wird, die seine Verwendung für die Erstellung von qualifizierten elektronischen Signaturen auch im 1. Halbjahr 2008 noch zulässt.

[1] Siehe http://www.bsi.de/esig/kryptoalg.htm

Folgende Firmen und Institutionen waren an der Erstellung dieser Korrigenda beteiligt:

- bremen online services GmbH & Co. KG, Bremen
- OSCI Leitstelle, Bremen (Herausgeber)

Weitere Informationen finden Sie im Internet unter der Adresse http://www.osci.de .

1.2 Copyright

Die vorliegende zweite Korrigenda der OSCI-Transport 1.2 - Spezifikation wurde im Auftrag der OSCI-Leitstelle als Herausgeber erarbeitet.

Diese Korrigenda ist urheberrechtlich geschützt. Alle Nutzungsrechte liegen bei dem Herausgeber. Herstellern wird zur Implementation von Bürger-, Kommunal-, Intermediär- oder Dienstleistersystemen unentgeltlich ein einfaches Nutzungsrecht eingeräumt. Im Rahmen des genannten Zwecks darf dieses Dokument in unveränderter Form vervielfältigt und zu den nachstehenden Bedingungen verbreitet werden.

Umgestaltungen, Bearbeitungen, Übersetzungen und jegliche Änderungen sind nur nach Rücksprache mit dem Herausgeber zulässig. Kennzeichnungen, Copyright-Vermerke und Eigentumsangaben sind beizubehalten.

Haftung für Mängel dieses Dokuments wird nur bei Vorsatz und grober Fahrlässigkeit übernommen. Hersteller der oben genannten Systeme sind gebeten, Fehler, Unklarheiten oder Interpretationsfreiräume dieser Spezifikation, die die ordnungsgemäße Funktion oder die Interoperabilität behindern, dem Herausgeber zu melden.

Eine Weitergabe dieses Dokuments an Dritte darf nur unentgeltlich, in unveränderter Form und zu den vorstehenden Bedingungen erfolgen.

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

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**[2]
SHA-256	**http://www.w3.org/2001/04/xmlenc#sha256**
SHA-512	**http://www.w3.org/2001/04/xmlenc#sha512**
RIPEMD-160	**http://www.w3.org/2001/04/xmlenc#ripemd160**

Um Kompatibilität mit im Markt eingesetzten Implementierungen zu gewärleisten, wir ist für die Erzeugung fortgeschrittener Signaturen sowie Transportsignaturen bis auf weiteres auch zugelassen:

SHA-1	**http://www.w3.org/2000/09/xmldsig#sha1**

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

Signatur-Algorithmus	**Algorithmus-Identifier**[3]
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-v1_5 [PKCS_1] mit Hash-Algorithmus RIPEMD-160. Modullänge des RSA-Schlüsselpaares mind. 2048 Bit	**http://www.w3.org/2001/04/xmldsig-more/rsa-ripemd160**

[2] nach [xenc]

[3] nach [RFC4051]

Um Kompatibilität mit im Markt eingesetzten Implementierungen zu gewärleisten, wir ist für die Erzeugung fortgeschrittener Signaturen sowie Transportsignaturen bis auf weiteres auch zugelassen:

Signatur-Algorithmus	**Algorithmus-Identifier**
Signaturschema RSASSA-PKCS1-v1_5 [PKCS_1] mit Hash-Algorithmus SHA-1. Modullänge des RSA-Schlüsselpaares mind. 1024 Bit	**`http://www.w3.org/2000/09/xmldsig#rsa-sha1`**

Wird SHA-1 als Hash- oder Signaturalgorithmaus eingesetzt, müssen Implementierungen bei der Prüfung der Siganturen und Anzeige der Prüfergebnisse deutlich ausweisen, dass es sich um als schwach zu betrachtende Algorithmen handelt (Warnhinweis: „Week Signature“).

Ein Intermediär hat bei der Signatur von Antworten auf Aufträge grundsätzlich die Digest- und Siggnaturalgorithmen einzusetzen, die ein Client im jeweiligen Auftrag anwendet.

Sind Aufträge eines Client nicht signiert, werden die Digest und Signaturen der Anworten gem. einer konfigurierbaren Default-Einstellung des Intermediärs erzeugt.

2.2 Kap. 6.4: Ausprägung von XML-Signature

Geändert werden die Restriktionen zu

- `<DigestMethodType>` und `<SignatureMethodType>` (Algorithmen).

Für die Signaturerstellung wird dringend empfohlen, auf die Verwendung vom SHA-1 und Schlüssellängen von 1024 zu verzichten; für die Signaturprüfung müssen diese weiterhin auch unterstützt werden.

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/2000/09/xmldsig#sha1" />
              <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/2000/09/xmldsig#rsa-sha1" />
                <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:restriction>
            </xsd:simpleType>
          </xsd:attribute>
        </xsd:restriction>
      </xsd:complexContent>
    </xsd:complexType>
  </xsd:redefine>
</xsd:schema>
```

2.3 Kap. 4.2: Verschlüsselung

In Anpassung an die RSA-Signaturalgorithmen wird auch für die Verschlüsselung die Modullänge von 1024 auf 2048 Bit verdoppelt:

Die Verschlüsselung des Sitzungsschlüssels erfolgt mittels RSAES-PKCS1-v1_5 [PKCS_1] (Algorithmus-Identifier: `http://www.w3.org/2001/04/xmlenc#rsa-1_5`, ([xenc] Abschnitt 5.4.1). **Die Modullänge des verwendeten RSA-Schlüsselpaares muss dabei mindestens 2048 Bit betragen.**

3 Literaturverzeichnis

[BNetzA_Alg] Bekanntmachung zur elektronischen Signatur nach Signaturgesetz und Signaturverordnung (Übersicht über geeignete Algorithmen), Bundesanzeiger Nr. 69 vom 22. April 2007;

http://www.bundesnetzagentur.de/media/archive/9655.pdf.

[BSI_Alg2008] Entwurf: Geeignete Algorithmen zur Erfüllung der Anforderungen nach §17 Abs. 1 bis 3 SigG vom 22. Mai 2001 in Verbindung mit Anlage 1 Abschnitt I Nr. 2 SigV vom 22. November 2001; Bundesamt für Sicherheit in der Informationstechnik, September 2007, http://www.bsi.de/esig/dokumente/krypto/algo_entw2_08.pdf.

[OSCI12] OSCI Transport 1.2 – Spezifikation; OSCI Leitstelle 2002, http://www1.osci.de/sixcms/detail.php?gsid=bremen02.c.1403.de

[PKCS_1] B. Kaliski, J. Staddon: PKCS #1: RSA Cryptography Specifications – Version 2.0. RFC 2437, October 1998. Online verfügbar unter http://www.ietf.org/rfc/rfc2437.txt

[RFC4051] Additional XML Security Uniform Ressource Idnetifiers (URI), Internet Engeneeruig Task Force RFC 4051, April 2005, http://www.ietf.org/rfc/rfc4051.txt

[xenc] World Wide Web Consortium. XML Encryption Syntax and Processing, W3C Recommendation, 10.12.2002; http://www.w3.org/TR/2002/REC-xmlenc-core-20021210/.