OSCI-Transport 1.2

– Korrigenda 10/2011 –

Status: Final

OSCI Leitstelle

Bremen, 19. Oktober 2011

Inhaltsverzeichnis

1 Einleitung

1.1 Anlass der Korrigenda

Diese Korrigenda zu OSCI Transport 1.2 [OSCI12] trägt der zunehmenden Verwendung so genannter elliptischer Kurven als Algorithmen für die Erzeugung von elektronischen Signaturen Rechnung (z.b. Signaturfunktion des nPA, Signaturkarte der A-Trust).

Im Bundesanzeiger Nr. 17 vom 1. Februar 2011 [BNetzA_Alg] wird der Algorithmus EC-DSA (DSA auf Basis elliptischer Kurven)

a) für **DSA-Varianten basierend auf Gruppen $E(F_p)$ wie folgt festgelegt:**
Für den Parameter p gibt es keine Einschränkungen. Die Länge von q muss mindestens 224 Bit betragen, und **ab Anfang 2016** sind für q mindestens 250 Bit erforderlich.
b) für DSA-Varianten basierend auf Gruppen $E(F_{2^m})$ wie folgt festgelegt:
An den Parameter m werden keine Bedingungen gestellt. Die Länge von q muss mindestens 224 Bit betragen, und **ab Anfang 2016** sind für q mindestens 250 Bit erforderlich.

Die in Verbindung mit den geeigneten und in der OSCI-Bibliothek bisher verwendeten Hashalgorithmen ergeben sich damit Signaturalgorithmen, die in der folgende Tabelle zusammengefasst sind.

Signaturalgorithmus	**geeignet bis Ende**
SHA-256 mit EC-DSA , Länge q >= 224 Bit	2015
SHA-256 mit EC-DSA , Länge q >= 250 Bit	2017
SHA-512 mit EC-DSA , Länge q >= 224 Bit	2015
SHA-512 mit EC-DSA , Länge q >= 250 Bit	2017

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.

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 dritte Korrigenda der OSCI-Transport 1.2 - Spezifikation wurde im Auftrag der OSCI-Leitstelle als Herausgeber erarbeitet.

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

Die Signieralgorithmen, 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-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**
Signaturschema ECDSA-SHA* gemäß RFC 4051 [RFC4051] mit Hash-Algorithmus SHA-256	**http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha256**
Signaturschema ECDSA-SHA* gemäß RFC 4051 [RFC4051] mit Hash-Algorithmus SHA-512	**http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha512**

2.2 Kap. 6.4: Ausprägung von XML-Signature

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

Diese Festlegungen gelten für die Signaturerstellung und die Signaturprüfung.

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" />
```

[1] nach [RFC4051]

```
  <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:restriction>
            </xsd:simpleType>
          </xsd:attribute>
        </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) vom 22. 12.2010, Bundesanzeiger Nr. 17 vom 1. Februar 2011;

http://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/BNetzA/Sachgebiete/QES/Veroeffentlichungen/Algorithmen/2011AlgoKatpdf.pdf?__blob=publicationFile

[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