Koordinierungsstelle
für IT-Standards

OSCI-Transport 1.2
- 01/2026-
Status: Entwurf

Korrigenda Nr. 10

Gültig ab: 13.02.2026

Koordinierungsstelle für IT-Standards (KoSIT)

Bremen, 13.02.2026

Inhaltsverzeichnis

Copyright

Die vorliegende, zehnte Korrigenda der Spezifikation OSCI-Transport 1.2 wurde im Auftrag der Koordinierungsstelle für IT-Standards erarbeitet.

Änderungshistorie

Datum	**Änderung**
13.02.2026	Bereitstellung zur internen Kommentierung
13.02.2026	Breitstellung zur Kommentierung durch Mitglieder der Expertengruppe Sicherer Transport
	Einarbeitung der Kommentierungen. Neben redaktionellen Änderungen wurden Gültigkeit und Übergangsfrist angepasst.

1. Einleitung

1.1 Anlass der Korrigenda

Im Rahmen der Arbeiten an der Erstellung einer Korrigenda 9 wurden Signatur-Algorithmen um den Algorithmus ecdsa-sha384 ergänzt. Für die Nutzung des genannten Algorithmus muss ebenfalls der Hash-Algorithmus SHA-384 unterstützt werden. Die Benennung des Hash-Algorithmus wir mit dieser Korrigenda nachgeholt.

1.2 Gültigkeit und Übergangsfrist

Diese Korrigenda tritt rückwirkend mit der Korrigenda 9 in Kraft.

1.3 Konventionen zur Textauszeichnung

Es gelten die gleichen Konventionen der zugrundeliegenden 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. Fortschreibung der Spezifikation

Im Folgenden werden die einzelnen Änderungen mit Bezug auf die entsprechenden Kapitel der Spezifikation OSCI Transport 1.2 [OSCI12] detailliert beschrieben. Über einer geänderten Zeile befindet sich ein Kommentar mit einer kurzen Beschreibung der Änderung.

3. Aktualisierung kryptographischer Verfahren

Die Tabelle mit den für OSCI zugelassenen Algorithmen im Kapitel „Digitale Signaturen“ und die Schemadatei oscisig.xsd wurden um einen neuen Algorithmus erweitert. Die Änderungen wurden **FETT** hervorgehoben.

3.1 Änderung an Kapitel „Digitale Signaturen“

Hashalgorithmus	Algorithmus-Identifier gemäß [RFC6931]
SHA-256	`http://www.w3.org/2001/04/xmlenc#sha256`
SHA-512	`http://www.w3.org/2001/04/xmlenc#sha512`
SHA-384	**`http://www.w3.org/2001/04/xmlenc#sha384`**
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`

3.2 Ausprägung von XML-Encryption

An dieser Stelle lediglich der veränderte Teil in oscienc.xsd:

```
<xsd:complexType name="DigestMethodType">
  <xsd:complexContent>
    <xsd:restriction base="ds:DigestMethodType">
      <xsd:attribute name="Algorithm" use="required">
        <xsd:simpleType>
          <xsd:restriction base="xsd:anyURI">
            <!-- Zeilen neu fuer sha256 und sha512 -->
            <xsd:enumeration
              value="http://www.w3.org/2001/04/xmlenc#sha256" />
            <xsd:enumeration
              value="http://www.w3.org/2001/04/xmlenc#sha512" />
            <!-- [KORR10] Zeile neu fuer sha384 -->
            <xsd:enumeration
              value="http://www.w3.org/2001/04/xmlenc#sha384" />
            <!-- Zeilen neu fuer sha3-256, sha3-384 und sha3-512 -->
            <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" />
            <!-- [KORR3] Zeile entfernt
              xsd:enumeration value="http://www.w3.org/2000/09/xmldsig#sha1"/> -->
            <!-- [KORR4] Zeile entfernt
              xsd:enumeration value="http: //www.w3.org/2001/04/xmlenc#ripemd160"/>
-->
          </xsd:restriction>
        </xsd:simpleType>
      </xsd:attribute>
    </xsd:restriction>
  </xsd:complexContent>
</xsd:complexType>
```

4. Literaturverzeichnis

[OSCI12] OSCI Transport 1.2 – Spezifikation; OSCI Leitstelle 2002, http://www.xoev.de/detail.php?gsid=bremen83.c.2472.de

[EFFI] Ergänzung zur Spezifikation OSCI 1.2 - Effiziente Übertragung großer Datenmengen, KoSIT 2017-10-25, https://www.xoev.de/sixcms/media.php/13/OSCI-1.2_mit_Korrigenda.pdf

[Korr] Korrigenda 1-10 zu OSCI-Transport 1.2, KoSIT 2025, https://www.xoev.de/sixcms/media.php/13/OSCI_Korrigenda.zip