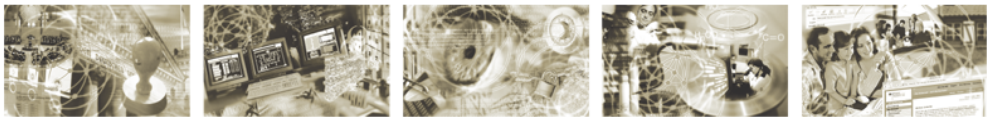
Bundesamt
für Sicherheit in der
Informationstechnik



Technische Richtlinie

Prüfspezifikation zur Technischen Richtlinie BSI TR-03132 Sichere Szenarien für Kommunikationsprozesse im Bereich hoheitlicher Dokumente

Version 1.7

01.04.2014

BSI TR-03133

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: +49 22899 9582-0
E-Mail: tr-pdu@bsi.bund.de
Internet: https://www.bsi.bund.de

Inhaltsverzeichnis

1 Einleitung....5
1.1 Referenzierte Spezifikation....5
1.2 Aufbau des Dokuments....5
2 Prüfmodule....6
2.1 Inhaltsdatenebene....6
2.1.1 Relevante Vorgaben der BSI TR-03132....6
2.1.2 Anwendbarkeit....6
2.1.3 Prüffälle....6
2.2 Prüfmodul OSCI-Client....10
2.2.1 Relevante Vorgaben der BSI TR-03132....10
2.2.2 Anwendbarkeit....10
2.2.3 Prüffälle....10
2.3 Prüfmodul OSCI-Intermediär....11
2.3.1 Relevante Vorgaben der BSI TR-03132....11
2.3.2 Anwendbarkeit....11
2.3.3 Prüffälle....11
2.4 Prüfmodul Empfangssystem des Dokumentenherstellers....12
2.4.1 Relevante Vorgaben der BSI TR-03132....12
2.4.2 Anwendbarkeit....13
2.4.3 Prüffälle....13
3 Literaturverzeichnis....15
4 Abkürzungsverzeichnis....16

Tabellenverzeichnis

Tabelle 1: Prüffall I-001 Inhaltsdatensignatur....7
Tabelle 2: Prüffall I-002 Inhaltsdatenverschlüsselung....9
Tabelle 3: Prüffall I-003: Bezug des Inhaltsdaten-Verschlüsselungszertifikats....9
Tabelle 4: Prüffall O-001: OSCI-Nachrichtenerstellung....11
Tabelle 5: Prüffall IM-001: OSCI-Intermediärsfunktionalität....12
Tabelle 6: Prüffall E-001: OSCI-Eingangsprüfung....13
Tabelle 7: Prüffall E-002: Eingangsprüfung der Inhaltsdatensignatur....14

1 Einleitung

Die technische Richtlinie BSI TR-03132 „Sichere Szenarien für Kommunikationsprozesse im Bereich hoheitlicher Dokumente“ legt Anforderungen an die Kommunikationsbeziehungen nach [TR PDÜ hD] fest. Sie beschreibt Kommunikationsmodelle für alle Nachrichten zwischen Behörden und Dokumentenherstellern.

Das vorliegende Dokument definiert Prüfanforderungen zur Feststellung der Korrektheit der Umsetzung der in BSI TR-03132 festgelegten Anforderungen.

1.1 Referenzierte Spezifikation

Das vorliegende Dokument ist gültig im Zusammenhang mit BSI TR-03132, Version 1.7.

1.2 Aufbau des Dokuments

Die in BSI TR-03132 definierten Kommunikationsmodelle erstrecken sich in der Beziehung zwischen Behörde und Dokumentenhersteller typischerweise über diverse Verarbeitungsschritte, von der initialen Signatur und Verschlüsselung über den Transport über ggf. verschiedene Akteure bis hin zum Lesen und Verarbeiten der Nachricht auf Empfängerseite.

Infolgedessen sind i.A. auch verschiedene Akteure und verschiedene Software-Module zur Umsetzung der relevanten Funktionalitäten im Einsatz. Aus diesem Grund spezifiziert diese Technische Richtlinie verschiedene Prüfmodule mit durchzuführenden Prüfschritten für verschiedene Teilaspekte des gesamten Kommunikationsszenarios.

Die durchzuführenden Prüfmodule ergeben sich aus der Funktionalität der Software-Module im Rahmen der Kommunikationsmodelle und werden in Abstimmung zwischen Hersteller, Prüfstelle und Zertifizierungsstelle festgelegt.

2 Prüfmodule

2.1 Inhaltsdatenebene

2.1.1 Relevante Vorgaben der BSI TR-03132

Dieses Modul dient der Abprüfung der Vorgaben der BSI TR-03132 (Kapitel 4: Kodierung der Inhaltsdatensignatur und -verschlüsselung).

2.1.2 Anwendbarkeit

Diese Prüffälle sind anwendbar auf Softwarekomponenten, welche Signatur- und Verschlüsselungsoperationen auf Inhaltsdatenebene ausführen. Führt ein Modul beide Schritte zusammen aus, muss es das Zwischenergebnis zum Zweck der Prüfung (nur Signatur) separat ausgeben können.

2.1.3 Prüffälle

<table>
<tr><td colspan="2">Prüffall I-001: Inhaltsdatensignatur</td></tr>
<tr><td colspan="2">Umfang</td></tr>
<tr><td colspan="2">► Dieser Prüffall dient zur Überprüfung der korrekten Durchführung der Inhaltsdatensignatur</td></tr>
<tr><td colspan="2">Vorbedingungen</td></tr>
<tr><td colspan="2">► Vorlage einer XhD-konformen Nachricht gemäß [03123] vom Typ <code>BestellungDokument</code>
► Vorlage des zugehörigen kryptographischen Materials (Hardware- oder Software-PSE, zugehörige PIN und Passwort)
► Durchführung einer Signatur der XhD-Nachricht</td></tr>
<tr><td colspan="2">Prüfschritte</td></tr>
<tr><td colspan="2">1 Zugriff auf den privaten Schlüssel</td></tr>
<tr><td>Erwartetes Resultat</td><td>► Das Prüfobjekt muss auf den privaten Schlüssel des Autors Zugriff nehmen können.
Anmerkung für die Prüfung
Für Software-PSE ist die Prüf-Anforderung i.W. trivial (Zugriff auf das Schlüsselmaterial). Im Fall von Hardware-PSE muss geprüft werden, ob es durch das Software-Modul Einschränkungen (z.B. bzgl. der Verwendung bestimmter Kartenleser gibt). Ist nur eine definierte Liste von Kartenlesern für die Verwendung mit der Software freigegeben, so ist jeder Leser dieser Liste zu prüfen; gibt es keine Einschränkung, so ist die Prüfung mit drei marktgängigen Kartenlesern durchzuführen.</td></tr>
<tr><td colspan="2">2 Schema-Konformität der Nachricht</td></tr>
</table>

Erwartetes Resultat	▶ Die Nachricht ist konform zum XhD 1.4-Schema (Namensraum `http://www.bsi.de/trxhd/1.4`). ▶ Das Teilelement `Signature` ist konform zum [XMLDSIG]-Schema.
3 Typus und Platzierung der Signatur	
Erwartetes Resultat	▶ Es handelt sich um eine eingebettete Signatur nach [XMLDSIG]. Der Algorithmus-Kennzeichner ist `http://www.w3.org/2000/09/xmldsig#enveloped-signature` ▶ Das `Signature`-Element ist gekapselt im Element `any` das letzte Element der zu signierenden Daten im XML-Baum. ▶ Die verwendeten `CanonicalizationMethod` entsprechen den Vorgaben von [XMLDSIG]. ▶ Das `Signature/SignedInfo`-Element enthält genau ein `Reference`-Element mit Wert Leerstring (`URI=""`).
4 Korrekte Verwendung der Hash- und Signatur-Algorithmen	
Erwartetes Resultat	▶ Die Signatur benutzt eine `DigestMethod`, welche [XMLDSIG] entspricht und vom BSI zugelassen ist. ▶ Die Signatur benutzt eine `SignatureMethod`, welche [XMLDSIG] entspricht und vom BSI zugelassen ist.[1]
5 Korrektheit von Signatur und Hash-Berechnung	
Erwartetes Resultat	▶ Der Hash-Algorithmus wird korrekt berechnet. ▶ Die Signatur wird korrekt berechnet. **Anmerkung für die Prüfung** Das Nachrechnen der Korrektheit ist unabhängig von der existierenden Software auf einem zweiten Weg (manuell oder durch Verwendung anderer Software-Funktionalitäten) nachzuprüfen. Bietet die Software Konfigurationsmöglichkeiten bzgl. verschiedener Algorithmen an, so ist der Prüffall für alle möglichen Kombinationen durchzuführen.

Tabelle 1: Prüffall I-001 Inhaltsdatensignatur

Prüffall I-002: Inhaltsdatenverschlüsselung
Umfang
▶ Dieser Prüffall dient zur Überprüfung der korrekten Durchführung der Inhaltsdatenverschlüsselung
Vorbedingungen

1 Vgl. https:/www.bsi.bund.de/Algorithmenkatalog

► Vorlage einer XhD-konformen, nach TR-03132 auf Inhaltsdatenebene signierten Nachricht vom Typ `BestellungDokument` ► Vorlage des zugehörigen kryptografischen Materials (Inhaltsdaten-Verschlüsselungszertifikat des Lesers) ► Durchführung der Verschlüsselung der XhD-Nachricht auf Inhaltsdatenebene	
Prüfschritte	
1 Zugriff auf den privaten Schlüssel	
Erwartetes Resultat	► Das Prüfobjekt muss auf den privaten Schlüssel des Lesers Zugriff nehmen können. **Anmerkung für die Prüfung** Für Software-PSE ist die Prüf-Anforderung i.W. trivial (Zugriff auf das Schlüsselmaterial). Im Fall von Hardware-PSE muss geprüft werden, ob es durch das Software-Modul Einschränkungen (z.B. bzgl. der Verwendung bestimmter Kartenleser gibt). Ist nur eine definierte Liste von Kartenlesern für die Verwendung mit der Software freigegeben, so ist jeder Leser dieser Liste zu prüfen; gibt es keine Einschränkung, so ist die Prüfung mit drei marktgängigen Kartenlesern durchzuführen.
2 Schema-Konformität der Nachricht	
Erwartetes Resultat	► Die Nachricht ist konform zum XhD 1.4-Schema (Namensraum `http://www.bsi.de/trxhd/1.4`). ► Das Teilelement `EncryptedData` ist konform zum [XMLENC]-Schema.
3 Typus und Platzierung der Verschlüsselung	
Erwartetes Resultat	► Es handelt sich um eine Element-Verschlüsselung nach [XMLENC]. Der Algorithmus-Kennzeichner ist `http://www.w3.org/2001/04/xmlenc#Element` ► Die Elemente `Nachrichtenkopf` und `Signature` sind unverschlüsselt und gegenüber dem Input unverändert. ► Das Element `Nutzdaten` ist entfernt und das Element `EncryptedData` innerhalb des `any`-Elements eingefügt. ► Es gibt in `EncryptedData` ein Element `EncryptedKey` (hybrides Verschlüsselungsverfahren). ► Es gibt unter `EncryptedKey` eine `KeyInfo`-Struktur, welche mittels `X509SubjectName` auf das verwendete Inhaltsdaten-Verschlüsselungszertifikat zeigt.
4 Korrekte Verwendung der Verschlüsselungsalgorithmen	
Erwartetes Resultat	► Die Verschlüsselung benutzt Algorithmen, welche [XMLENC] entspricht und vom BSI zugelassen sind (vgl. Signaturprüffall).

5 Korrektheit der Verschlüsselung	
Erwartetes Resultat	► Die Verschlüsselung durch den symmetrischen Schlüssel ist mathematisch korrekt. ► Die Verschlüsselung des symmetrischen Schlüssels durch das Inhaltsdaten-Verschlüsselungszertifikat ist mathematisch korrekt. **Anmerkung für die Prüfung** Das Nachrechnen der Korrektheit ist unabhängig von der existierenden Software auf einem zweiten Weg (manuell oder durch Verwendung anderer Software-Funktionalitäten) nachzuprüfen. Bietet die Software Konfigurationsmöglichkeiten bzgl. verschiedener Algorithmen an, so ist der Prüffall für alle möglichen Kombinationen durchzuführen.

Tabelle 2: Prüffall I-002 Inhaltsdatenverschlüsselung

Prüffall I-003: Bezug des Inhaltsdaten-Verschlüsselungszertifikats	
Umfang	
► Dieser Prüffall dient zur Überprüfung des korrekten Bezugs des Inhaltsdaten-Verschlüsselungszertifikats.	
Vorbedingungen	
► DVDV-Anbindung technisch vorhanden. ► Bezug der vollständigen Dienstbeschreibung gemäß [03132] aus dem DVDV. **Anmerkung für die Prüfung** Für Nutzungsszenarien, in denen keine DVDV-Anbindung möglich ist, kann das Prüfobjekt auch eine alternative Zuführung des Inhaltsdaten-Verschlüsselungszertifikats vorsehen.	
Prüfschritte	
1 Abruf aus dem DVDV	
Erwartetes Resultat	► Das Prüfobjekt ruft die korrekte WSDL-Beschreibung aus dem DVDV ab.
2 Korrektes Auslesen des Inhaltsdaten-Verschlüsselungszertifikats aus der WSDL-Beschreibung.	
Erwartetes Resultat	► Das Prüfobjekt nutzt das korrekte Zertifikat für die Durchführung der Inhaltsdatenverschlüsselung. **Anmerkung für die Prüfung** Dies ist durch Betrachtung erzeugten Chiffrats zu prüfen.

Tabelle 3: Prüffall I-003: Bezug des Inhaltsdaten-Verschlüsselungszertifikats

2.2 Prüfmodul OSCI-Client

2.2.1 Relevante Vorgaben der BSI TR-03132

Dieses Modul dient der Abprüfung der Vorgaben der BSI TR-03132 zur Erstellung der OSCI-Nachrichten im OSCI 1.2-Kommunikationsmodell.

2.2.2 Anwendbarkeit

Diese Prüffälle sind anwendbar auf Softwarekomponenten, welche OSCI 1.2-Nachrichten erstellen. Dies umfasst alle in der BSI TR-03132 geregelten Aspekte einschließlich der Kommunikation mit dem OSCI-Intermediär.

2.2.3 Prüffälle

Prüffall O-001: OSCI-Nachrichtenerstellung
Umfang
► Dieser Prüffall dient zur Überprüfung der korrekten Erstellung der OSCI-Nachricht **Anmerkung für die Prüfung** Je nach Kommunikationsrichtung kommen verschiedene Nachrichten als Payload in Frage. Ebenso finden verschiedene OSCI-Nachrichten, je nach OSCI-Szenario Anwendung. Im Rahmen des Prüffalls sind bei den verschiedenen Optionen jeweils die für das Szenario relevanten auszuwählen.
Vorbedingungen
► Vorlage einer XhD-konformen, nach TR-03132 auf Inhaltsdatenebene signierten und verschlüsselten Nachricht vom Typ `BestellungDokument` oder `Auftragsinformation`. ► Vollständige DVDV-Dienstbeschreibung gemäß TR-03132 im DVDV oder einem gültigen DVDV-Cache gemäß Kapitel 3.4.2 der TR-03132 vorhanden. ► OSCI-Sender-Zertifikat ► Durchführung der Kommunikation mit einem OSCI-Intermediär, Protokollierung der On-The-Wire-Durchführung der Kommunikation **Anmerkung für die Prüfung** In der Kommunikation zum Dokumentenhersteller ist die Nutzung eines Test-Intermediärs und eines zugehörigen Backendsystems notwendig. Hierzu kann das Testsystem des Dokumentenherstellers nach [03104] herangezogen werden. Bei auftretenden Fehlern ist hierbei allerdings auch auf ein mögliches Fehlverhalten des Intermediärs bzw. Backendsystems zu achten und deren Spezifikationskonformität zu untersuchen. In der Kommunikation zur Behörde und beim Abholen von Nachrichten durch die Behörde ist ein geeigneter Test-Intermediär zu nutzen. Das korrekte Verhalten des Intermediärs ist analog zu beachten.
Prüfschritte
1 Bezug der DVDV-Dienstbeschreibung

Erwartetes Resultat	▶ Der Client bezieht die Dienstbeschreibung aus dem DVDV oder aus einem gültigen DVDV-Cache gemäß Kapitel 3.4.2 der TR-03132.
2 Korrektheit der OSCI-Kommunikation	
Erwartetes Resultat	▶ Alle im Rahmen der OSCI-Kommunikation mit dem Intermediär ausgetauschten Nachrichten sind konform zum [OSCI]. ▶ Die jeweils korrekten OSCI-Nachrichtentypen (insbesondere die eigentlichen Transportnachrichten `StoreDelivery` und `ForwardDelivery`) werden verwendet. **Anmerkung für die Prüfung** Hierzu sind alle im Rahmen des OSCI-Dialogs erzeugten Nachrichten zu untersuchen. Die jeweiligen Abschnitte der OSCI-Spezifikation definieren Schemata für jede Nachricht und ggf. darüber hinausgehende Anforderungen, welche abzuprüfen sind.
3 Korrektheit der ContentContainer	
Erwartetes Resultat	▶ Es gibt genau einen ContentContainer mit der Ref-ID `XHD_DATA`. ▶ Der ContentContainer ist signiert durch den OSCI-Sender. ▶ Die Anforderungen von [OSCI] an die Signatur werden eingehalten.
4 Einbindung des Autoren-Zertifikats auf OSCI-Ebene	
Erwartetes Resultat	▶ Das im Input auf Inhaltsdatenebene verwendete Autoren-Signatur-Zertifikat wird auf der Transportebene zusätzlich abgelegt.
5 Korrekte Übernahme der Zertifikate	
	▶ Der Client nutzt das korrekte Zertifikat aus der WSDL-Beschreibung als OSCI-Empfänger-Zertifikat.

Tabelle 4: Prüffall O-001: OSCI-Nachrichtenerstellung

2.3 Prüfmodul OSCI-Intermediär

2.3.1 Relevante Vorgaben der BSI TR-03132

Dieses Modul dient der Abprüfung der Vorgaben der BSI TR-03132, welche an den eingesetzten OSCI-Intermediär gemacht werden.

2.3.2 Anwendbarkeit

Diese Prüffälle sind anwendbar auf die jeweilige OSCI-Intermediärskomponente.

2.3.3 Prüffälle

Prüffall IM-001: OSCI-Intermediärsfunktionalität
Umfang

► Dieser Prüffall dient zur Überprüfung der korrekten Funktionalität des OSCI-Intermediärs im OSCI 1.2-Kommunikationsmodell.	
Vorbedingungen	
► Durchführung der Kommunikation mit einem OSCI-Client, Protokollierung der On-The-Wire-Durchführung des Protokolls ► Ggf. Durchführung der Kommunikation mit einem Backendsystem (bei passivem OSCI-Szenario), Protokollierung der On-The-Wire-Durchführung des Protokolls **Anmerkung für die Prüfung** Fokus der Prüfung sind insbesondere die Aspekte des Intermediär-Betriebs, welche spezielle Anforderungen der BSI TR-03132 darstellen. Die Nutzung eines OSCI-Clients, welcher entsprechend der BSITR-03132 arbeitet, wird vorausgesetzt.	
Prüfschritte	
1 Korrektheit der OSCI-Kommunikation	
Erwartetes Resultat	► Alle im Rahmen der OSCI-Kommunikation mit dem Client ausgetauschten Nachrichten sind konform zum [OSCI]. **Anmerkung für die Prüfung** Hierzu sind alle im Rahmen des OSCI-Dialogs erzeugten Nachrichten zu untersuchen. Die jeweiligen Abschnitte der OSCI-Spezifikation definieren Schemata für jede Nachricht und ggf. darüber hinausgehende Anforderungen, welche abzuprüfen sind.
2 Korrektheit der Prüfung der Zertifikate und des Laufzettels.	
Erwartetes Resultat	► Der Intermediär prüft alle Zertifikate auf Gültigkeit (bis zur Root des Zertifikatsausstellers innerhalb der PKI-1-Verwaltung). ► Der Intermediär protokolliert das Ergebnis der Prüfungen auf dem Laufzettel. **Anmerkung für die Prüfung** Zur Sicherstellung der korrekten Arbeitsweise des Intermediärs sollte dieser Prüfschritt jeweils mit einem gültigen und einem gesperrten Zertifikat durchgeführt werden.

Tabelle 5: Prüffall IM-001: OSCI-Intermediärsfunktionalität

2.4 Prüfmodul Empfangssystem des Dokumentenherstellers

2.4.1 Relevante Vorgaben der BSI TR-03132

Dieses Modul dient der Abprüfung der Vorgaben der BSI TR-03132, welche an den Prüfprozess zur Eingangsprüfung beim Dokumentenhersteller gemacht werden.

2.4.2 Anwendbarkeit

Diese Prüffälle sind anwendbar auf Softwarekomponenten im Empfangs- (Backend-)System des Dokumentenherstellers.

2.4.3 Prüffälle

<table>
<tr><td colspan="2">Prüffall E-001: OSCI-Eingangsprüfung</td></tr>
<tr><td colspan="2">Umfang</td></tr>
<tr><td colspan="2">▶ Dieser Prüffall dient der Prüfung der korrekten Umsetzung der spezifizierten Prüfmaßnahmen beim Eingangssystem des Dokumentenherstellers.</td></tr>
<tr><td colspan="2">Vorbedingungen</td></tr>
<tr><td colspan="2">▶ Durchführung der Kommunikation mit einem OSCI-Client und dem Intermediär des Dokumentenherstellers inkl. Beantwortung durch das passive Backendsystem des Dokumentenherstellers
▶ Vollständige DVDV-Dienstbeschreibung gemäß TR-03132 im DVDV oder einem gültigen DVDV-Cache gemäß Kapitel 3.4.2 der TR-03132 vorhanden.
Anmerkung für die Prüfung
Die Nutzung eines OSCI-Clients und Intermediärs, welcher konform zu BSI TR-03132 arbeitet, wird vorausgesetzt.</td></tr>
<tr><td colspan="2">Prüfschritte</td></tr>
<tr><td colspan="2">Korrektheit der OSCI-Sender-Signatur und VerifyCategory</td></tr>
<tr><td>Erwartetes Resultat</td><td>▶ Der Dokumentenhersteller weist Nachrichten ab, welche eine ungültige Sender-Signatur haben.
▶ Der Dokumentenhersteller weist Nachrichten ab, welche mit ungültigen Zertifikaten signiert sind.
▶ Der Dokumentenhersteller weist Nachrichten ab, bei denen das verifyCategory nicht erfolgreich war.
▶ Der Dokumentenhersteller akzeptiert Nachrichten, bei denen alle o.g. Prüfungen erfolgreich sind, sofern keine weiteren fachlichen Fehler außerhalb des Anwendungsgebiets der BSI TR-03132 vorliegen.
Anmerkung für die Prüfung
Um das korrekte Verhalten abzuprüfen, sind drei fehlerhafte Nachrichten (Signatur ungültig, Zertifikat ungültig, VerifyCategory nicht erfolgreich) und eine valide Nachricht zu generieren und in das Empfangssystem einzuspeisen.</td></tr>
</table>

Tabelle 6: Prüffall E-001: OSCI-Eingangsprüfung

Prüffall E-002: Eingangsprüfung der Inhaltsdatensignatur	
Umfang	
► Dieser Prüffall dient der Prüfung der korrekten Umsetzung der spezifizierten Prüfmaßnahmen beim Eingangssystem des Dokumentenherstellers.	
Vorbedingungen	
► Durchführung der Kommunikation mit einem OSCI-Client und dem Intermediär des Dokumentenherstellers inkl. Beantwortung durch das passive Backendsystem des Dokumentenherstellers **Anmerkung für die Prüfung** Die Nutzung eines OSCI-Clients und Intermediärs, welcher konform zu BSI TR-03132 arbeitet, wird vorausgesetzt.	
Prüfschritte	
Korrektheit der Inhaltsdatensignatur	
Erwartetes Resultat	► Der Dokumentenhersteller prüft, ob die Inhaltsdatensignatur korrekt ist. ► Der Dokumentenhersteller prüft, ob das verwendete Zertifikat gültig ist. ► Der Dokumentenhersteller prüft, ob das verwendete Zertifikat aus der korrekten Sub-CA gemäß BSI TR-03132 stammt.

Tabelle 7: Prüffall E-002: Eingangsprüfung der Inhaltsdatensignatur

3 Literaturverzeichnis

[03104] BSI TR-03104 Technische Richtlinie Produktionsdatenerfassung, -qualitätsprüfung und -übertragung für hoheitliche Dokumente

[03123] BSI TR-03123, Technische Richtlinie XML-Datenaustauschformat für die Beantragung hoheitlicher Dokumente

[03132] BSI TR-03132 Technische Richtlinie Sichere Szenarien für Kommunikationsprozesse im Bereich hoheitlicher Dokumente

[OSCI] OSCI-Leitstelle, OSCI-Transport 1.2 – Spezifikation

[XMLDSIG] W3C, http://www.w3.org/TR/xmldsig-core/

[XMLENC] W3C, http://www.w3.org/TR/xmlenc-core/

4 Abkürzungsverzeichnis

Abkürzung	Beschreibung
DVDV	Deutsches Verwaltungsdiensteverzeichnis
OSCI	Online Services Computer Interface
PIN	Personal Identification Number
PSE	Personal security environment, Smartcard
WSDL	Web Services Description Language
XhD	XML-Datenaustauschformat für hoheitliche Dokumente
XML	Extensible Markup Language
XMLDSIG	XML Signature
XMLENC	XML Encryption