Bundesamt
für Sicherheit in der
Informationstechnik

Technische Richtlinie zur Produktionsdatenerfassung, -qualitätsprüfung und -übermittlung für Pässe

BSI TR-03104

Version 2.1.5

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

Inhaltsverzeichnis

Vorwort

Die Einführung von elektronischen Pässen mit biometrischen Merkmalen wird durch eine Reihe nationaler, europäischer und internationaler Gremienbeschlüsse angestoßen.

Am 9. Januar 2002 wurde vom Deutschen Bundestag das Terrorismusbekämpfungsgesetz [TerrGesetz] erlassen. Dadurch wurden Änderungen an Pass-, Personalausweis- und Ausländergesetz motiviert. Es wird u.a. festgelegt, dass Pässe neben dem Lichtbild und der Unterschrift weitere biometrische Merkmale von Gesicht oder Fingern des Passinhabers enthalten.

Auf internationaler Ebene wurde im März 2003 von Gremien der International Civil Aviation Organization (ICAO) die New Orleans Resolution verabschiedet. Davon ausgehend wurden im Mai 2004 normative Technical Reports [ICAO_04] veröffentlicht, die das Gesichtsbild als primäres biometrisches Erkennungsmerkmal festlegen. Zusätzliche biometrische Merkmale sind Fingerabdruck und Iriserkennung. Die biometrischen Merkmale sind als digitale Bilddateien in kontaktlosen IC-Chips zu speichern, um eine globale maschinengestützte Verifikation der Identität anhand der biometrischen Merkmale zu unterstützen.

Auf europäischer Ebene wurde im Dezember 2004 von Gremien der Europäischen Union (EU) die Verordnung No 2252/2004 erlassen [EU_2252/2004]. Die Verordnung legt Anforderungen für Sicherheitsmerkmale und biometrische Daten in von den Mitgliedstaaten ausgestellten Pässen und Reisedokumenten fest. Insbesondere wird die Einführung der Reisepässe mit biometrischen Merkmalen verbindlich in Bezug auf Lichtbilder auf 18 Monate und in Bezug auf Fingerabdrücke auf 36 Monate nach Inkrafttreten der Technischen Spezifikationen zur Verordnung 2252/2004 festgelegt.

Vorbemerkungen

Die Version 2.1 der Technische Richtlinie zur Produktionsdatenerfassung, -qualitätsprüfung und -übermittlung für Pässe (TRPDÜ) entspricht der Version 2.1 der Anlage zur PassDEÜV vom 21.05.2007.

Versionshistorie

Version	Kommentar
1.1	Initiale Version zum Feldtest
2.1	Überarbeitete Version gemäß der Anlage zur PassDEÜV V 2.1
2.1.1	Empfehlungen des BSI gemäß §6 PassDEÜV, umfasst die Änderungsdokumente 1-3
2.1.2	Empfehlungen des BSI gemäß §6 PassDEÜV, umfasst das Änderungsdokument 4, ausschließlich Änderungen für Reiseausweise
2.1.3	Fortschreibung der Technischen Richtlinie
2.1.4	Überarbeitung der Technischen Richtlinie auf Grund von Verordnungsänderungen im Zusammenhang mit der Einführung des neuen Personalausweises
2.1.5	Korrektur hinsichtlich des Ordens- und Künstlernamens im Reiseausweis für Flüchtlinge / für Ausländer / für Staatenlose und weiterer editorischer Fehler in Annex 3 [Annex-XPASS]

Titel

Diese TR trägt den Titel "Technische Richtlinie zur Produktionsdatenerfassung, -qualitätsprüfung und -übermittlung für Pässe".

Kennzeichnung

Diese TR wird gekennzeichnet mit „BSI TR-03104“.

Fachlich zuständige Stelle

Fachlich zuständig für die Formulierung und Betreuung dieser TR ist das Bundesamt für Sicherheit in der Informationstechnik (BSI).

Anschrift: Bundesamt für Sicherheit in der Informationstechnik (BSI)
Abteilung 3
Godesberger Allee 185 - 189
53175 Bonn

E-Mail: tr-pdu@bsi.bund.de

1. Übersicht

Kapitel 1 erläutert den Aufbau und die Inhalte der Richtlinie. Es werden Rollen definiert, die im Rahmen dieses Dokumentes verwendet werden. Zur Übersicht wird eine schematische Darstellung des Prozessablaufs gegeben.

1.1 Aufbau und Inhalte der Anlage

Die Anlage hat die folgenden normativen Inhalte:

- Kapitel 2: Die Erfassung der biometrischen Produktionsdaten, also des Lichtbilds und der Fingerabdrücke. Es gibt weitere Produktionsdaten (Name, Geburtsdatum usw.), deren Erfassung von der Anlage nicht festgelegt wird.
- Kapitel 3: Die Qualitätsüberprüfung der biometrischen Produktionsdaten. Die biometrischen Daten werden einer Qualitätsprüfung unterzogen, die gewährleistet, dass die erfassten biometrischen Daten den ISO-Normen [ISO_FACE, ISO_FINGER] und insbesondere den ICAO-Kriterien [ICAO_04] entsprechen.
- Kapitel 4, 5, 6 und 7: Der Aufbau, die Übermittlung und Absicherung der Produktionsdaten zwischen Passbehörden oder Vermittlungsstellen und Passhersteller. Alle zu übertragenden Daten werden hinsichtlich Art und Umfang definiert. Um die Übermittlung der Daten integer, authentisch und vertraulich zu gestalten, werden die Übertragungprotokolle festgelegt und Vorgaben für die Datensicherheit bei der Übermittlung gemacht.
- Kapitel 8: Verfahren zur Testdatenübermittlung zur Problemanalyse und –behebung bei der Passdatenübermittlung.
- Kapitel 9: Festlegungen zur Konformität und Interoperabilität von Hard- und Softwaremodulen im Zusammenhang mit der Erfassung, Qualitätssicherung und Übermittlung von Passantragsdaten.
- Kapitel 10: Die zentrale Qualitätssicherungs-Statistik.

1.2 Rollen

In der Anlage werden folgende Rollen unter der zugeordneten Bedeutung verwendet:

Passbehörden	sind Stellen, bei denen ein elektronischer Pass beantragt werden kann, diese können u. a. bei einer Kommune oder bei einer Auslandsvertretung lokalisiert sein. Passbehörden fungieren als Erfassungsstellen für Produktionsdaten, an denen auch die biometrischen Daten erhoben werden. Gemäß § 6 Absatz 1 PassG kann die Datenerfassung auch durch andere mit hoheitlichen Befugnissen ausgestattete Stellen erfolgen, die eine Passbehörde oder eine Vermittlungsstelle beauftragen, die Daten zu den Antragsdatensätzen zusammenzufassen und an den Passhersteller zu übermitteln.
Vermittlungsstellen	haben von Passbehörden den Auftrag, Daten zu verarbeiten. In diesem Zusammenhang werden Produktionsdaten, meist von mehreren Passbehörden, zentral gesammelt und gebündelt an den Passhersteller weitergereicht. Die Vermittlungsstellen sind u. a. in Rechenzentren lokalisiert. Es bleibt den Passbehörden freigestellt, keine Vermittlungsstelle zu beauftragen und die Produktionsdaten selbst an den Passhersteller zu übermitteln.

Passhersteller nimmt Produktionsdaten entgegen und produziert elektronische Pässe, übermittelt Rückantworten an Vermittlungsstellen und Passbehörden.

1.3 Übersicht

In diesem Abschnitt wird eine Skizze als Übersicht über das Verfahren angegeben. Die Skizze wird in Abschnitt 1.4 erläutert.

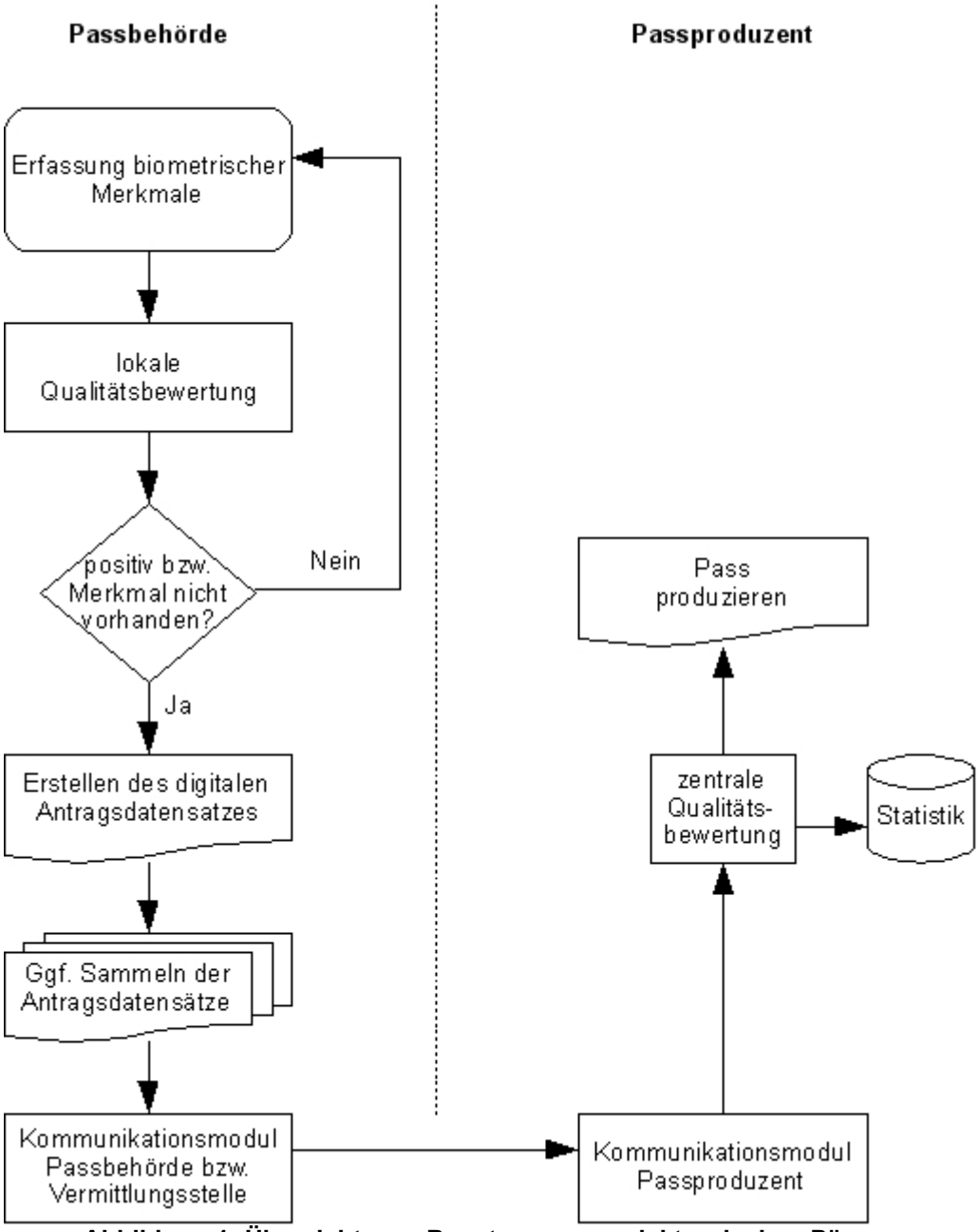


Abbildung 1: Übersicht zum Beantragen von elektronischen Pässen

Bei der Übersicht ist zu beachten, dass die Übermittlung der Antragsdatensätze auch über eine Vermittlungsstelle erfolgen kann. Die Kommunikation erfolgt dann zwischen der Vermittlungsstelle und dem Passhersteller. Der Transport der Antragsdaten zwischen Passbehörde und Vermittlungsstelle wird in der TR nicht behandelt, die entsprechenden Anforderungen für die Qualitätssicherung der zu übertragenden Antragsdaten und die Datensicherheit bei der Übermittlung sind aber auch bei der Kommunikation zwischen Passbehörde und Vermittlungsstelle zu beachten.

1.4 Verfahrensablauf

In diesem Abschnitt werden die Schritte im Ablaufdiagramm in Abschnitt 1.3 erläutert. Es handelt sich um eine grobe Sicht auf den Prozessablauf und dient dem allgemeinen Verständnis, insbesondere sind nicht alle Kommunikationsschritte zwischen Passbehörde oder Vermittlungsstelle und Passhersteller wiedergegeben.

1. An den Arbeitsplätzen der Passbehörden werden die Antragsdaten des Antragstellers aufgenommen. Das vorliegende Dokument behandelt die Erfassung der biometrischen Daten, die Erfassung aller anderen Antragsdaten liegen nicht im Fokus der Verordnung.

2. Die biometrischen Daten sind einer lokalen Qualitätssicherung zu unterziehen. Sind die Daten fehlerhaft, wird möglichst unmittelbar eine entsprechende Rückantwort an den Antragsteller gegeben. Das Datenqualitätsmanagement wird in Kapitel 3 der Anlage behandelt.

3. Die erfassten Antragsdaten werden zu einem digitalen Antragsdatensatz zusammengefasst. Siehe hierzu Kapitel 4 der Anlage.

4. Mehrere Antragsdatensätze können zu einem Bestelldatensatz zusammengefasst werden. Auch hierzu befinden sich detaillierte Informationen in Kapitel 4 der Anlage.

5. Die Passbehörde oder Vermittlungsstelle überträgt integer, authentisch und vertraulich den Bestelldatensatz zum Passhersteller. Kapitel 5 behandelt zulässige Protokolle und Kapitel 7 enthält die Regelungen zur Datensicherheit.

6. Der Passhersteller nimmt den Bestelldatensatz entgegen und sichert eine integere, authentische und vertrauliche Kommunikation mit der Passbehörde oder Vermittlungsstelle zu.

7. Die biometrischen Daten werden einer zentralen Qualitätsüberprüfung und einer Qualitätssicherungs-Statistik (siehe Kapitel 10) zugeführt.

8. Der Pass wird produziert.

2. Datenerfassung

Kapitel 2 spezifiziert, wie die Daten in den Passbehörden erfasst werden und welche Anforderungen an die dabei verwendeten Erfassungsgeräte gestellt werden.

2.1 Anforderungen an den Erfassungsprozess für das Lichtbild

Bei der Beantragung eines elektronischen Passes durch den Antragsteller ist die Erfassung des Lichtbilds erforderlich. Für die Anforderungen an den entsprechenden Erfassungsprozess und die damit verbundenen technischen und organisatorischen Maßnahmen zur Qualitätssicherung siehe Kapitel 3.

2.2 Hardwareanforderungen für die Erfassung von Gesichtsbilddaten

Für die Erfassungsgeräte zur Digitalisierung der durch die Antragsteller bereitgestellten Lichtbilder gelten technische und organisatorische Anforderungen. Für die entsprechenden Vorgaben siehe Kapitel 3.

2.3 Anforderungen an den Erfassungsprozess für Fingerabdrücke

Bei der Beantragung eines elektronischen Passes ist die Erfassung und Digitalisierung der Fingerabdrücke des Antragstellers erforderlich. Für die Anforderungen an den entsprechenden Erfassungsprozess und die damit verbundenen technischen und organisatorischen Maßnahmen zur Qualitätssicherung siehe Kapitel 3.

2.4 Hardwareanforderungen für die Erfassung von Fingerabdrücken

Für die Erfassungsgeräte der Fingerabdrücke der Antragsteller gelten technische und organisatorische Anforderungen. Für die entsprechenden Vorgaben siehe Kapitel 3.

3. Datenqualitätsmanagement

Die Ausführungen in Kapitel 3 zum Datenqualitätsmanagement für das Lichtbild werden im Annex 1 [Annex-QS-Gesicht] zu dieser Anlage geführt.

Der Titel von Annex 1 der Anlage lautet:

> „Qualitätsanforderungen bei der Erfassung und Übertragung der Lichtbilder als biometrische Merkmale für elektronische Pässe“

Die Ausführungen in Kapitel 3 zum Datenqualitätsmanagement für Fingerabdrücke werden im Annex 2 [Annex-QS-Finger] zu dieser Anlage geführt.

Der Titel von Annex 2 der Anlage lautet:

> „Qualitätsanforderungen bei der Erfassung und Übertragung der Fingerabdrücke als biometrische Merkmale für elektronische Pässe“

Inhalte von Annex 1 und 2 der Anlage sind:

- Qualitätsanforderungen und Qualitätssicherungsmaßnahmen jeweils für das Lichtbild und die Fingerabdrücke;
- Anforderungen an eine dezentrale und zentrale Qualitätsbewertung (QS-Statistik);
- Festlegung von Datenformaten zur Kompression, Kodierung der biometrischen Daten und zur Übertragung.

4. Datenmodell

Die Ausführungen in Kapitel 4 zum Datenmodell werden im Annex 3 [Annex-XPASS] zu dieser Anlage geführt.

Der Titel von Annex 3 der Anlage lautet:

> „Datenaustauschformat für die Übermittlung von Daten für elektronische Pässe“.

Inhalt des Annex 3 der Anlage ist:

- XML-basiertes [XML] Datenaustauschformat für Dokumentdaten und dokumentabhängiger Geschäftsprozesse in Nachrichten zwischen den Passbehörden oder Vermittlungsstellen und dem Passhersteller. Er beschreibt damit das Datenmodell. Annex 3 behandelt weiterhin die Authentisierung und Verschlüsselung der Produktionsdaten auf Anwendungsebene durch XML-Signature [XDSIG] und XML-Encryption [XENC].

5. Datenübermittlung

In Kapitel 5 werden einzusetzende Verfahren zur Datenübermittlung behandelt.

Die Passantragsdaten müssen von den Passbehörden bzw. Vermittlungsstellen zum Passhersteller integer, vertraulich und authentisch übertragen werden. Die Rückantworten müssen vom Passhersteller zu den Passbehörden oder Vermittlungsstellen ebenfalls integer und authentisch übertragen werden.

Die Integrität der Passantragsdaten und Rückantworten wird durch elektronische Signaturen und die Vertraulichkeit der Passantragsdaten wird durch Verschlüsselung auf Anwendungsebene sichergestellt. Die authentische Datenübermittlung zwischen Passbehörden bzw. Vermittlungsstellen und Passhersteller wird durch geeignete Transportprotokolle und der Verwendung vertrauenswürdiger Authentisierungszertifikate gewährleistet. Für die authentische Übermittlung der Passantragsdaten und Rückantworten wird OSCI-Transport benutzt. Für Passbehörden, die OSCI bis zur ausschließlich elektronischen Passdatenübermittlung noch nicht vollständig unterstützen können, wird eine ersatzweise Übermittlung der Passantragsdaten und Rückantworten auf der Basis von XML und WSDL/SOAP spezifiziert.

Die folgende Abbildung 2 veranschaulicht diese Möglichkeiten:

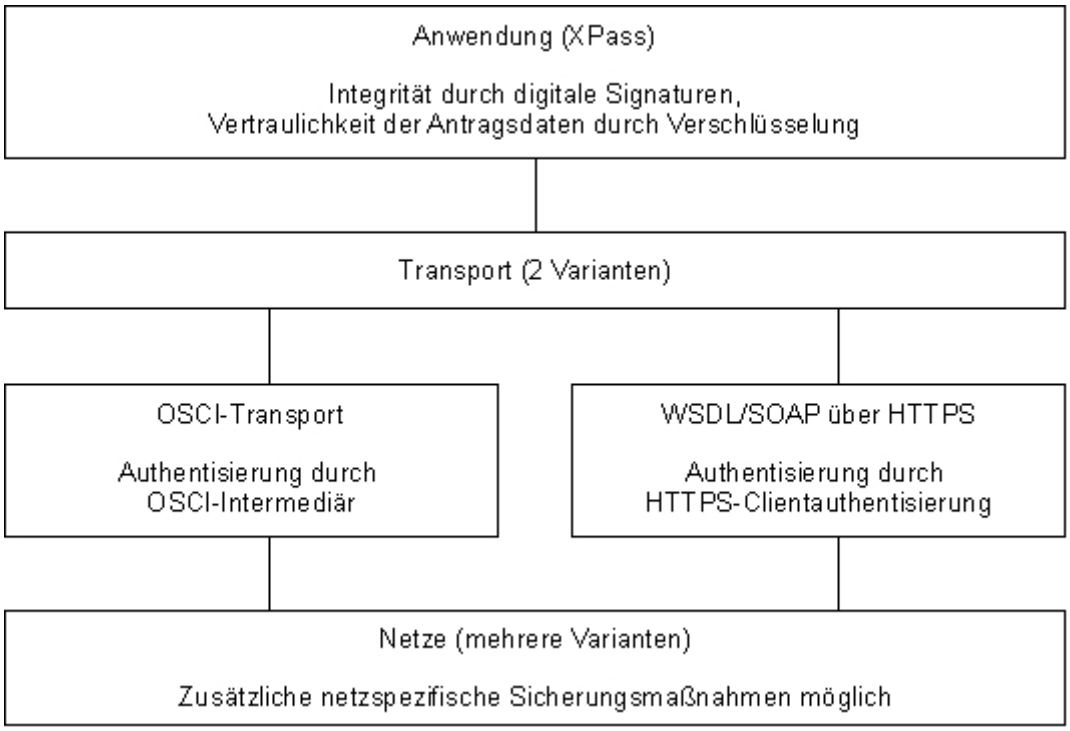


Abbildung 2: Übermittlung der Antragsdaten und Rückantworten

5.1 OSCI-Transport

OSCI-Transport ist zur Übermittlung der Antragsdaten und Rückantworten gemäß [OSCI] einzusetzen.

Zur Authentisierung der kommunizierenden Instanzen durch den notwendigen OSCI-Intermediär, zur Erstellung und Prüfung elektronischer Signaturen und zur Ver- und Entschlüsselung von Daten werden X.509-Zertifikate geeigneter Public Key Infrastukturen (PKIs) eingesetzt. Siehe hierzu Kapitel 7.

5.2 Ersatzverfahren: WSDL/SOAP über HTTPS

Das Ersatzverfahren stützt sich auf die Technologien Web Service Description Language (WSDL) und Simple Object Access Protocol (SOAP), die XML als Grundlage haben. Als Trägerprotokoll wird Hypertext Transfer Protocol Secure (HTTPS) verwendet. Siehe hierzu die Referenzen [WSDL] und [SOAP].

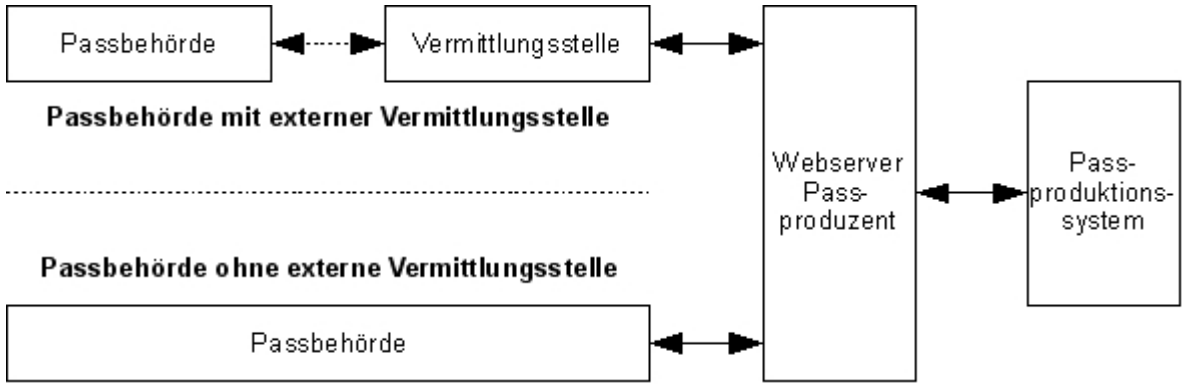
5.2.1 Kommunikationsmodell

Zwischen Passbehörden bzw. Vermittlungsstellen und Passhersteller werden Daten zwecks Produktion der Pässe übermittelt. Passbehörden können direkt mit dem Passhersteller kommunizieren oder Daten von Passbehörden können in Vermittlungsstellen zusammengefasst oder getrennt werden und zwischen Vermittlungsstellen und dem Passhersteller übertragen werden.

Kommuniziert eine Passbehörde direkt mit dem Passhersteller, fallen die Kommunikationsinstanzen Passbehörde und Vermittlungsstelle zusammen. Eine solche Passbehörde kann daher auch als (ihre eigene) Vermittlungsstelle bezeichnet werden.

Es ist nur die Kommunikationsbeziehung zwischen Vermittlungsstellen und Passhersteller relevant, die Datenübermittlung zwischen Passbehörden und Vermittlungsstellen wird nicht betrachtet.

Die folgende Abbildung konkretisiert dieses Kommunikationsmodell noch einmal für den Fall, dass ein Web-Server seitens des Passherstellers eingesetzt wird.



Legende: ◀▶ nicht von der Anlage erfasst.

Abbildung 3: Kommunikationsmodell mit Webserver

In der Abbildung gestrichelt dargestellte Kommunikationswege werden nicht von der Verordnung erfasst.

Es wird in dieser Anlage ein Webservice XPassTransportService zur Kommunikation zwischen Vermittlungsstellen (Clients, Service consumer) und Passhersteller (Server, Serviceprovider) definiert.

Der Webservice XPassTransportService stützt sich auf die Technologien WSDL und SOAP, die XML als Grundlage haben. Als Trägerprotokoll wird HTTPS verwendet.

Die Registrierung des Webservice in der Registry Universal Description, Discovery and Integration (UDDI) ist nicht notwendig und nicht vorgesehen. Die eigentliche Implementierung des Webservice XPassTransportService kann in beliebiger Programmiersprache auf beliebiger Plattform realisiert sein.

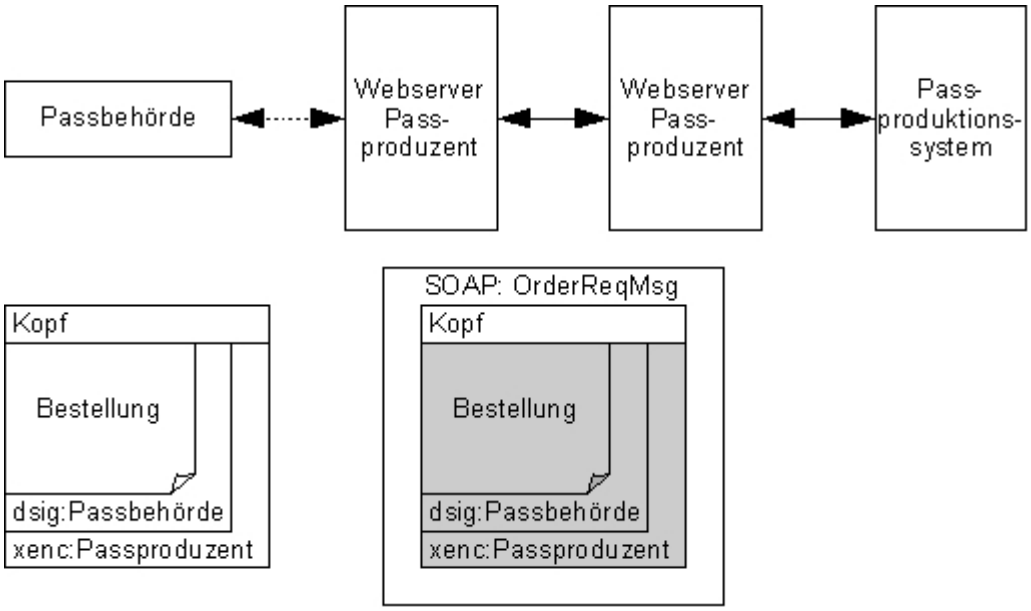
Aufbauend auf die mit dieser Anlage vorliegende XML-Modellierung der Antragsdaten und Rückantworten, kann der Webservice XPassTransportService auf SOAP-Basis weitgehend werkzeuggestützt realisiert werden.

Seitens der Vermittlungsstellen werden HTTPS-Clients eingesetzt, seitens des Passherstellers ein SOAP-fähiger HTTPS-Server [1].

5.2.2 Datenfluss

Der Webservice XPassTransportService stellt seine verfügbaren Dienste (Methodenaufrufe) als SOAP-Nachrichten zur Verfügung. Zum Transport der SOAP-Nachrichten wird HTTPS mit Client-Auth-Verfahren (also HTTP mit TLS/SSL und einem zusätzlichen SSL-Client-Auth-Verfahren mit einem Benutzerzertifikat) benutzt.

Die folgende Abbildung gibt ein Beispiel für den zu realisierenden WSDL/SOAP-Datenfluss zwischen Passbehörde, Vermittlungsstelle und Passhersteller.



Legende: ◀▶ nicht von der Anlage erfasst.

Abbildung 4: Beispiel zum Datenfluss und Nachrichtenstruktur

In der Abbildung gestrichelt dargestellte Kommunikationswege werden nicht von der Verordnung erfasst.

Die Passbehörde erstellt ihre Bestellungen/Aufträge, authentisiert (signiert) sie elektronisch und verschlüsselt sie anschließend. Dann werden die Daten an die Vermittlungsstelle übergeben.

Die Vermittlungsstelle benutzt den Webservice XPassTransportService zum Übertragen der angelieferten Daten.

Der Passhersteller entschlüsselt die angelieferten Daten, prüft die angehängte Signatur und speichert Bestellungen/Aufträge zur weiteren Prüfung und Bearbeitung durch das Passproduktionssystem. Daraus resultierende Rückantworten werden zum Abruf durch die Vermittlungsstellen bereitgestellt.

---

1 Z. B. Webserver Apache mit Software-Bibliothek Axis, einer Open-Source-Implementierung des Webservice-Standards SOAP

5.2.3 Unterstützung durch Zertifikate und PKIs

Zur Authentisierung der kommunizierenden Instanzen, zur Erstellung und Prüfung elektronischer Signaturen und zur Ver- und Entschlüsselung von Daten werden X.509-Zertifikate aus geeigneten PKIs eingesetzt. Siehe hierzu Kapitel 7.

5.2.4 Webservice XPassTransportService

Die Beschreibung des Webservice XPassTransportService erfolgt in WSDL (Definitionen siehe Kapitel 6).

Der Webservice XPassTransportService definiert jeweils einen eigenen Methodenaufruf (SOAP-Operation) für jedes der XPass-Elemente (Antragsdaten und Rückantworten), welche im XML-Schema xpass.xsd [Annex-XPASS] definiert sind.

Eine SOAP-Nachricht ist eine XML-Nachricht zur Kapselung eines Methodenaufrufs. Die Kapselung bewirkt Unabhängigkeit von Betriebssystem, Programmiersprache und Anwendung, mit der der Webservice realisiert wurde. Die SOAP-Nachricht besteht aus SOAP-Envelope, optionalem SOAP-Header und SOAP-Body.

Es gibt die folgenden Methodenaufrufe:

#	Methode	Typ	Logische Gruppierung
1	Bestellung	Antragsdaten	Bestellung
2	Bestellinformation	Rückantwort	Bestellung

Die Methodenaufrufe gehören entweder zum Typ Antragsdaten (zum Passhersteller) oder zum Typ Rückantwort (zur Vermittlungsstelle bzw. Passbehörde). Eine Bestellung kann auch eine Reklamationsbestellung beinhalten; die Bestellinformation eine Information zu einer Reklamationsbestellung.

Damit eine einfache Fehlerhandhabung möglich ist, wird für jede dieser Methodentypen eine eigene Request-/Response-Nachrichtenstruktur definiert. Diese Nachrichtenstrukturen sind immer ähnlich im Aufbau und bilden immer die Kommunikationsgrundlage zur Abbildung der XPass-Prozessabläufe.

Die Vermittlungsstellen bzw. Passbehörden werden als Client in allen Fällen der Kommunikation (Methodenaufrufe) zum Passhersteller aktiv, der Passhersteller (Server) übernimmt keine aktive Rolle.

Für Methoden vom Typ Antragsdaten ist die Modellierung immer:

Request:

```
<?xml version="1.0" encoding="UTF-8"?>

<soapenv:Envelope xmlns:soapenv="...Namensräume...">

<soapenv:Body>

<header><...xpass:type.Verfahrenskennzeichen...>

</header>
      <XEnc><...verschlüsselt für Passhersteller...>

            <DSig><...signiert durch Passbehörde...>
```

```
                    <...XPass-Modellierung: Antragsdaten...>
                </DSig>
            </XEnc>
        </soapenv:Body>
        </soapenv:Envelope>
```

Response:

```
        <?xml version="1.0" encoding="UTF-8"?>
        <soapenv:Envelope xmlns:soapenv="...Namensräume...">
        <soapenv:Body>
                <status><...WebService OK / Error...>
        </status>
        </soapenv:Body>
        </soapenv:Envelope>
```

Ein Methodenaufruf vom Typ Antragsdaten wird vom SOAP-Client einer Vermittlungsstelle zusammen mit den Antragsdaten an den SOAP-Server des Passherstellers gesandt. Als Rückantwort wird vom SOAP-Server nur eine allgemeine Status-Antwort erwartet. Diese Antwort sagt aber nichts über die tatsächliche Weiterverarbeitung der Antragsdaten beim Passhersteller aus, sondern bestätigt nur den korrekten Ablauf beim SOAP-Server.

Für Methoden vom Typ Rückantwort ist die Modellierung immer:

Request:

```
        <?xml version="1.0" encoding="UTF-8"?>
        <soapenv:Envelope xmlns:soapenv="...Namensräume...">
        <soapenv:Body>
                <header><...Kennung der Vermittlungsstelle...>
        </header>
        </soapenv:Body>
        </soapenv:Envelope>
```

Response:

```
        <?xml version="1.0" encoding="UTF-8"?>
        <soapenv:Envelope xmlns:soapenv="...Namensräume...">
        <soapenv:Body>
        <header><...xpass:type.Verfahrenskennzeichen...>
```

```
</header>
<DSig><...signiert durch Passhersteller...>

          <...XPass-Modellierung: Rückantwortdaten...>

</DSig>

</soapenv:Body>

</soapenv:Envelope>
```

Bei Methodenaufrufen vom Typ Rückantwort ist der Request-Header rein informativ. Die eigentliche Authentisierung/Identifikation wird durch das Vermittlungsstellen-Client-Auth-Zertifikat gebildet. Da der Header nicht verschlüsselt ist, kann dieser bei den Zuordnungen zwischen Passbehörden und Vermittlungsstellen herangezogen werden. Auch kann der Header benutzt werden, um seitens des Webservice die jeweilige Passbehörde zu benachrichtigen, falls beim späteren Entschlüsseln irgendwelche Probleme auftreten.

5.2.5 Einbettung der SOAP-Nachrichten in HTTPS

Die oben definierten SOAP-Nachrichten werden zwischen Vermittlungsstellen (SOAP-Clients) und Passhersteller (SOAP-Server) über das Protokoll HTTPS übertragen. Die Einbettung der SOAP-Nachrichten in HTTP-Strukturen wird vollständig vom automatisch erzeugten Code des SOAP-Servers übernommen und bedarf keiner expliziten Programmierung.

5.2.6 Definitionen zum Webservice XPassTransportService

Die vollständige Definition des Webservice XPassTransportService ist im Kapitel 6 dieses Dokuments enthalten.

6. Definition Webservice XPassTransportService

Dieses Kapitel 6 enthält die vollständige Definition des Webservice XPassTransportService. Es ist in folgende Abschnitte aufgeteilt:

- Hierarchie der verwendeten XML-Schemata und Bezug zu OSCI,
- Definition XPassTransportService.wsdl,
- Definition XPassTS.xsd,
- Definition XPassTSSub.xsd.

Der erste Abschnitt "Hierarchie der verwendeten XML-Schemata und Bezug zu OSCI" zeigt den Zusammenhang und die Anordnung der im Webservice XPassTransportService verwendeten XML-Definitionen, die restlichen Abschnitte enthalten die Definitionen selbst.

6.1 Hierarchie der verwendeten XML-Schemata und Bezug zu OSCI

Die folgende Abbildung zeigt den Zusammenhang und die Anordnung der im Webservice XPassTransportService verwendeten XML-Definitionen.

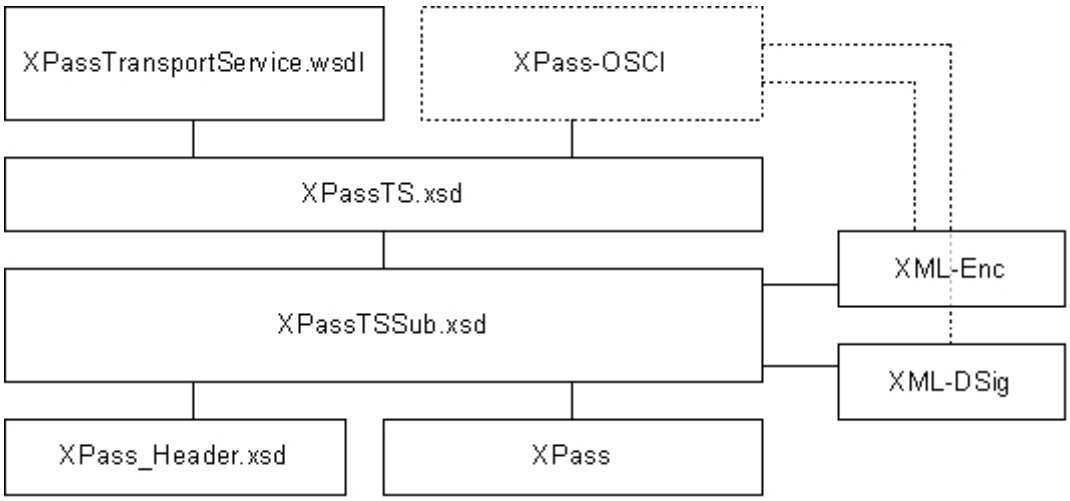


Abbildung 5: Hierarchie der verwendeten XML-Schemata und Bezug zu OSCI

Die Definition "XPassTransportService.wsdl" enthält die Webservice-Definition in WSDL-Notation. Sie stützt sich auf die darunter liegende Definition "XPassTS.xsd".

Das in der Abbildung gestrichelt eingezeichnete Modul "XPass-OSCI" wird von der Webservice-Definition NICHT benutzt. Wird anstelle des Verfahrens WSDL/SOAP über HTTPS (siehe Kapitel 5.2) das Verfahren OSCI-Transport (siehe Kapitel 5.2) eingesetzt, so muss das Modul "XPass-OSCI" (anstelle der Definition "XPassTransportService.wsdl") die darunter liegende Definition "XPassTS.xsd" verwenden.

Die Definition "XPassTS.xsd" beschreibt die XML-Datenblöcke, der per Protokoll HTTPS (oder per OSCI-Transport) zu übertragen sind. Diese XML-Datenblöcke sind zusammengesetzt aus einzelnen Elementen gemäß der darunter liegenden Definition "XPassTSSub.xsd".

Die Definition "XPassTSSub.xsd" beschreibt einzelne XML-Datenelemente und die signierten oder verschlüsselt/signierten XML-Daten. Dazu werden die Definition "XPass_Header.xsd" und die Module XML-DSig und XML-Enc des W3C-Consortiums benutzt.

Die Definition "XPass_Header.xsd" beschreibt gemeinsame XML-Datentypen für die Definition "XPassTSSub.xsd" und das Modul "XPass". Sie wird in [Annex-XPASS] wiedergegeben.

Das Modul "XPass" enthält die XML-Definitionen aus Annex 3 [Annex-XPASS].

6.2 Definition XPassTransportService.wsdl

Die Definition "XPassTransportService.wsdl" enthält die Webservice-Definition in WSDL-Notation.

Die Definition "XPassTransportService.wsdl" benutzt die Definition "XPassTS.xsd" (siehe weiter unten).

6.3 Definition XPassTS.xsd

Die Definition "XPassTS.xsd" kapselt im Webservice verwendete XML-Typdefinitionen.

Die Definition "XPassTS.xsd" benutzt die Definition "XPassTSSub.xsd" (siehe weiter unten).

6.4 Definition XPassTSSub.xsd

Die Definition "XPassTSSub.xsd" kapselt im Webservice verwendete XML-Typdefinitionen.

Die Definition "XPassTSSub.xsd" benutzt die Definition "XPass_Header.xsd" (Definition siehe [Annex-XPASS]) und die XML-Module XML Signature und XML Encryption des W3C-Consortium [XDSIG], [XENC].

7. Datensicherheit bei der Übermittlung

Kapitel 7 enthält Regelungen zur Datensicherheit bei der Übermittlung der Produktionsdaten und der Rückantworten.

In Abschnitt 7.1 werden allgemeine Sicherheitskriterien zur Datensicherheit bei der Übermittlung formuliert.

Die zur Realisierung der Sicherheitskriterien notwendigen PKIs werden in Abschnitt 7.2 behandelt.

7.1 Allgemeine Anforderungen an die Datensicherheit

Es sind die einschlägigen Anforderungen der Sicherheit im Umgang mit digitalen Daten zu berücksichtigen. Insbesondere zur Gewährleistung der Schutzziele Integrität, Vertraulichkeit und Authentisierung.

Als Signatur- und Verschlüsselungskomponenten, einschließlich zugehöriger Smartcards und Smartcardleser, sind nach mindestens EAL 3+ zertifizierte Komponenten einzusetzen. In Fällen, wo dies nicht gewährleistet werden kann, müssen besondere organisatorische Sicherheitsmaßnahmen getroffen werden, die einen unerlaubten Zugriff auf die Signatur- und Verschlüsselungskomponenten verhindern.

7.1.1 Integrität

Die übermittelten Inhaltsdaten während einer Kommunikationsbeziehung müssen auf mögliche Veränderungen geprüft werden. Dies ist durch Anwendung und Prüfung elektronischer Signaturen mittels gültiger X.509-Zertifikate mit ausreichender kryptographischer Stärke sicherzustellen.

7.1.2 Vertraulichkeit

Die übermittelten Passantragsdaten während einer Kommunikationsbeziehung dürfen nicht von nicht-autorisierten Stellen einsehbar sein. Dies ist durch Anwendung von digitaler Verschlüsselung mittels gültiger X.509-Zertifikate mit ausreichender kryptographischer Stärke sicherzustellen.

7.1.3 Authentisierung

Sender und Empfänger in Kommunikationsbeziehungen müssen identifiziert und authentisiert werden. Dies ist durch Verwendung von gültigen X.509-Zertifikaten mit ausreichender kryptographischer Stärke sicherzustellen.

7.2 Public Key Infrastrukturen (PKIs)

Um die Anforderungen zur Datensicherheit im Rahmen dieser Anlage zu erfüllen, müssen die erforderlichen X.509-Zertifikate von Public Key Infrastrukturen (PKIs) generiert, verwaltet und geprüft werden. Zum Generieren gehören das Beantragen, Genehmigen und Herstellen der Zertifikate. Zum Verwalten gehören das Verteilen, Sperren und Erneuern der Zertifikate. Zum Prüfen gehören das Bereitstellen von validen

Zertifikatsketten der Zertifikatshierarchie und aktuellen Sperrinformationen von Zertifikaten in Sperrlisten (Certificate Revocation Lists, CRLs), die über Statusabfragen eine Verifizierung von Zertifikaten erlauben.

7.2.1 Erforderliche X.509-Zertifikate

Gemäß Abbildung 2 in Kapitel 5 werden Zertifikate auf folgenden Ebenen benötigt:

- Auf der Anwendungsebene (XPass),
- auf der Transportebene in der Variante OSCI-Transport ,
- auf der Transportebene in der Variante WSDL/SOAP über HTTPS.

Zertifikate auf der Anwendungsebene (XPass) werden zur Sicherstellung von Integrität, Authentizität und Vertraulichkeit der Daten benutzt.

Um die Integrität der Daten zu gewährleisten, werden Signaturzertifikate bei den Passbehörden und beim Passhersteller benutzt. Jede Passbehörde sowie der Passhersteller besitzen ein eigenes, eindeutiges Signaturzertifikat. Das Signaturzertifikat jeder Passbehörde ist auf einer SmartCard abgelegt, die in der Passbehörde sicher zu verwahren ist. Die Signaturzertifikate des Auswärtigen Amtes und des Passherstellers können auch als Softwarezertifikate ausgeführt sein, da sie in einer sicheren Umgebung verwendet werden. Der jeweilige Erzeuger der Daten (Passbehörde oder Passhersteller) bildet mit dem privaten Schlüssel seines Signaturzertifikats über die zu übertragenden Daten eine XML-Signatur. Der jeweilige Konsument der Daten (Passhersteller oder Passbehörde) überprüft mit dem öffentlichen Schlüssel des Signaturzertifikats des Erzeugers die erhaltenen signierten Daten.

Um die Vertraulichkeit der Daten zu gewährleisten, wird ein Verschlüsselungszertifikat beim Passhersteller benutzt. Das Verschlüsselungszertifikat des Passherstellers kann als Softwarezertifikat ausgeführt sein, da es in einer sicheren Umgebung beim Passhersteller verwendet wird. Der jeweilige Erzeuger der Daten (Passbehörde) verschlüsselt mit dem öffentlichen Schlüssel des Verschlüsselungszertifikats die zu übertragenden (signierten) Daten mit einer XML-Verschlüsselung. Der Konsument der Daten (Passhersteller) entschlüsselt mit dem privaten Schlüssel seines Verschlüsselungszertifikats die erhaltenen verschlüsselten (und signierten) Daten. Nur die Antragsdaten von den Passbehörden zum Passhersteller werden verschlüsselt. Die Rückantworten vom Passhersteller zu den Passbehörden enthalten keine personenbezogenen Daten und werden daher nur signiert aber nicht verschlüsselt.

Jede Passbehörde benötigt ihr eigenes Signaturzertifikat, das Signaturzertifikat (öffentlicher Schlüssel) des Passherstellers und das Verschlüsselungszertifikat (öffentlicher Schlüssel) des Passherstellers.

Der Passhersteller braucht sein eigenes Signaturzertifikat, die Signaturzertifikate (öffentliche Schlüssel) aller Passbehörden und sein eigenes Verschlüsselungszertifikat.

Die folgende Abbildung veranschaulicht die notwendigen kryptographischen Schritte auf der Anwendungsebene (XPass) am Beispiel der Übermittlung von Antragsdaten. Der Ablauf bei der Übermittlung von Rückantworten verläuft mit vertauschten Rollen analog, aber ohne die Schritte der Ver- und Entschlüsselung der signierten XML-Daten.

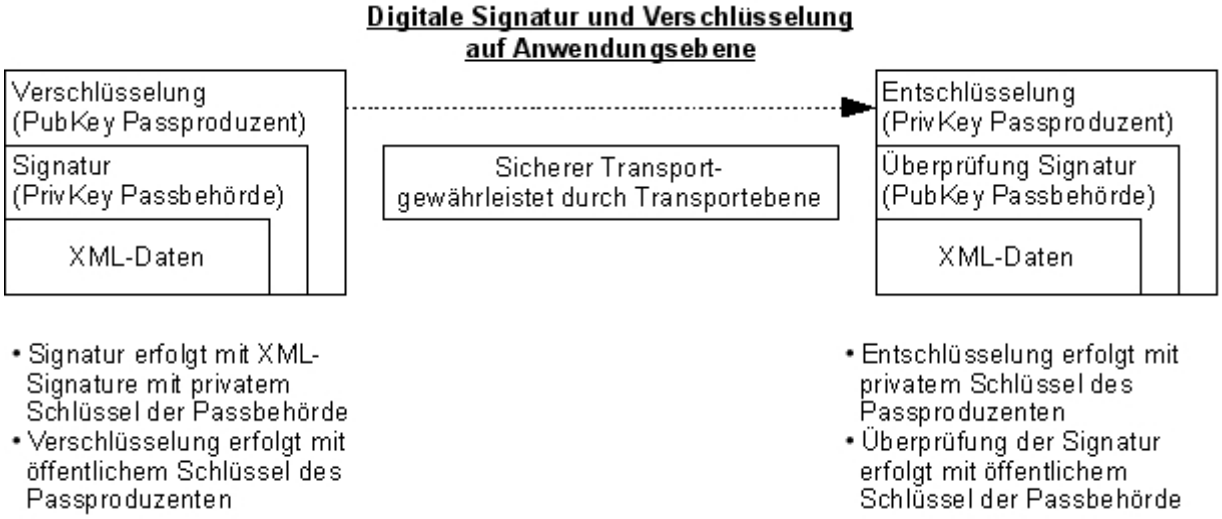


Abbildung 6: Datensicherheit auf Anwendungsebene (XPass)

Zertifikate auf der Transportebene in der Variante OSCI-Transport werden zur Authentisierung der Kommunikationspartner und bei Passbehörden und beim Passhersteller zusätzlich zu den Zertifikaten auf der Anwendungsebene (XPass) benutzt.

Zur Authentisierung werden Authentisierungszertifikate bei den OSCI-Clients und beim OSCI-Intermediär benutzt. Jeder OSCI-Client sowie der OSCI-Intermediär besitzen ein eigenes, eindeutiges Authentisierungszertifikat. Ein OSCI-Client (Passbehörde, Vermittlungsstelle oder Passhersteller) weist mit dem privaten Schlüssel seines Authentisierungszertifikats seine Identität gegenüber dem OSCI-Intermediär nach. Der OSCI-Intermediär (Passhersteller) überprüft mit dem öffentlichen Schlüssel des Authentisierungszertifikats des OSCI-Clients dessen Identität. Darüber hinaus können die Nutzdaten im OSCI-Container zwischen OSCI-Client und OSCI-Intermediär verschlüsselt werden.

Jeder OSCI-Client braucht sein eigenes Authentisierungszertifikat und das Authentisierungszertifikat (öffentlicher Schlüssel) des OSCI-Intermediärs. Eventuell können weitere Verschlüsselungszertifikate zur Ver- und Entschlüsselung für die Nutzdaten im OSCI-Container verwendet werden.

Der OSCI-Intermediär braucht sein eigenes Authentisierungszertifikat und die Authentisierungszertifikate (öffentliche Schlüssel) aller OSCI-Clients.

Die folgende Abbildung veranschaulicht die notwendigen kryptographischen Schritte auf der Transportebene in der Variante OSCI-Transport am Beispiel der Übermittlung von Antragsdaten. Der Ablauf bei der Übermittlung von Rückantworten verläuft mit vertauschten Rollen analog, aber ohne die Schritte der Ver- und Entschlüsselung der signierten XML-Daten.

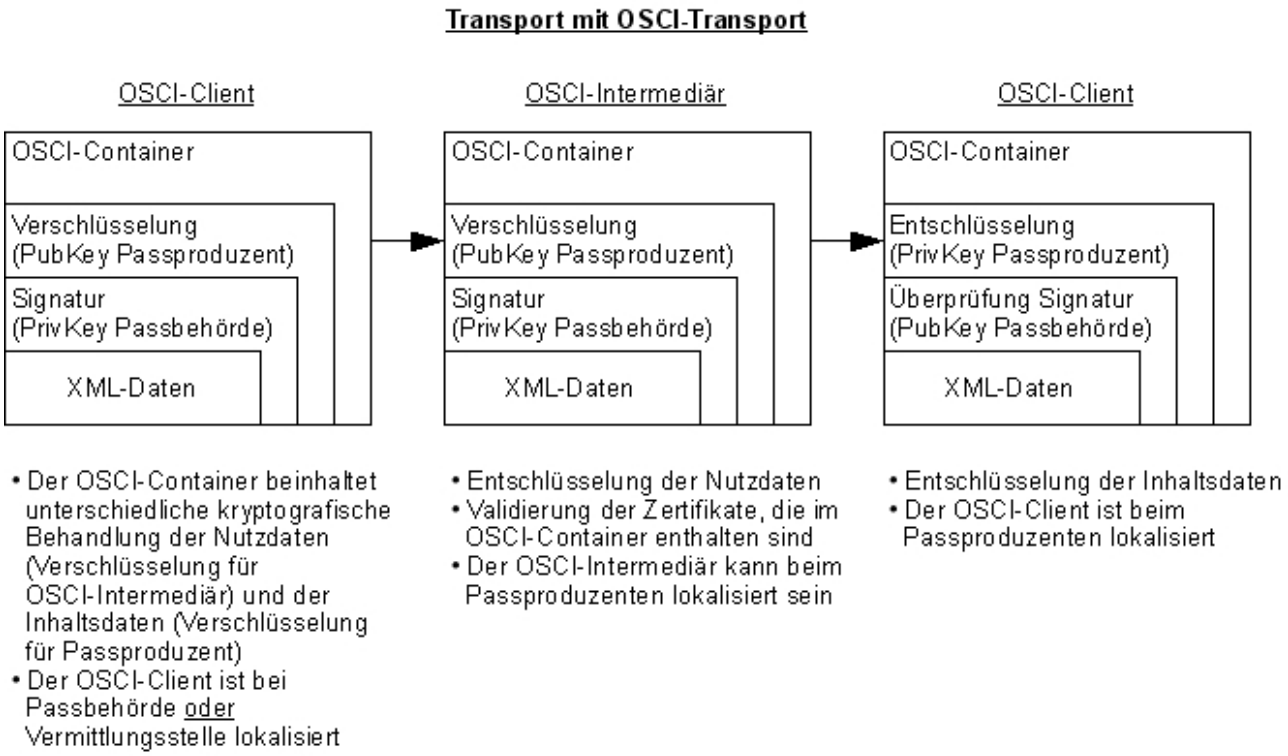


Abbildung 7: Datensicherheit auf Transportebene: OSCI-Transport

Zertifikate auf der Transportebene in der Variante WSDL/SOAP über HTTPS werden zur Authentisierung der Kommunikationspartner und bei Passbehörden und beim Passhersteller zusätzlich zu den Zertifikaten auf der Anwendungsebene (XPass) benutzt.

Zur Authentisierung werden Authentisierungszertifikate bei den HTTPS-Clients und beim Web-Server benutzt. Jeder HTTPS-Client besitzt ein eigenes, eindeutiges Authentisierungszertifikat (Client-Zertifikat). Ein HTTPS-Client (Passbehörde oder Vermittlungsstelle) weist mit dem privaten Schlüssel seines Client-Zertifikats seine Identität gegenüber dem Web-Server nach. Der Web-Server besitzt ein eigenes, eindeutiges Authentisierungszertifikat (Server-Zertifikat). Der Web-Server (Passhersteller) weist mit dem privaten Schlüssel seines Server-Zertifikats seine Identität gegenüber den HTTPS-Clients nach. Jeder HTTPS-Client muss die Gültigkeit des Server-Zertifikats prüfen können. Dies kann mittels Statusabfragen von Sperrlisten (CRL)geschehen. Es ist gewährleistet, dass nur HTTPS-Clients mit Client-Zertifikaten den Webservice XPassTransportService benutzen können.

Jeder HTTPS-Client braucht sein eigenes Client-Zertifikat (privater Schlüssel).

Der Web-Server braucht sein eigenes Server-Zertifikat. Der Web-Server des Passherstellers hat außerdem eine Liste der zulässigen (als "trusted" gesetzten) Client-Zertifikate und kann deren Gültigkeit mittels Statusabfragen verifizieren.

Die folgende Abbildung veranschaulicht die notwendigen kryptographischen Schritte auf der Transportebene in der Variante WSDL/SOAP über HTTPS am Beispiel der Übermittlung von Antragsdaten. Der Ablauf bei der Übermittlung von Rückantworten verläuft analog, aber ohne die Schritte der Ver- und Entschlüsselung der signierten XML-Daten.

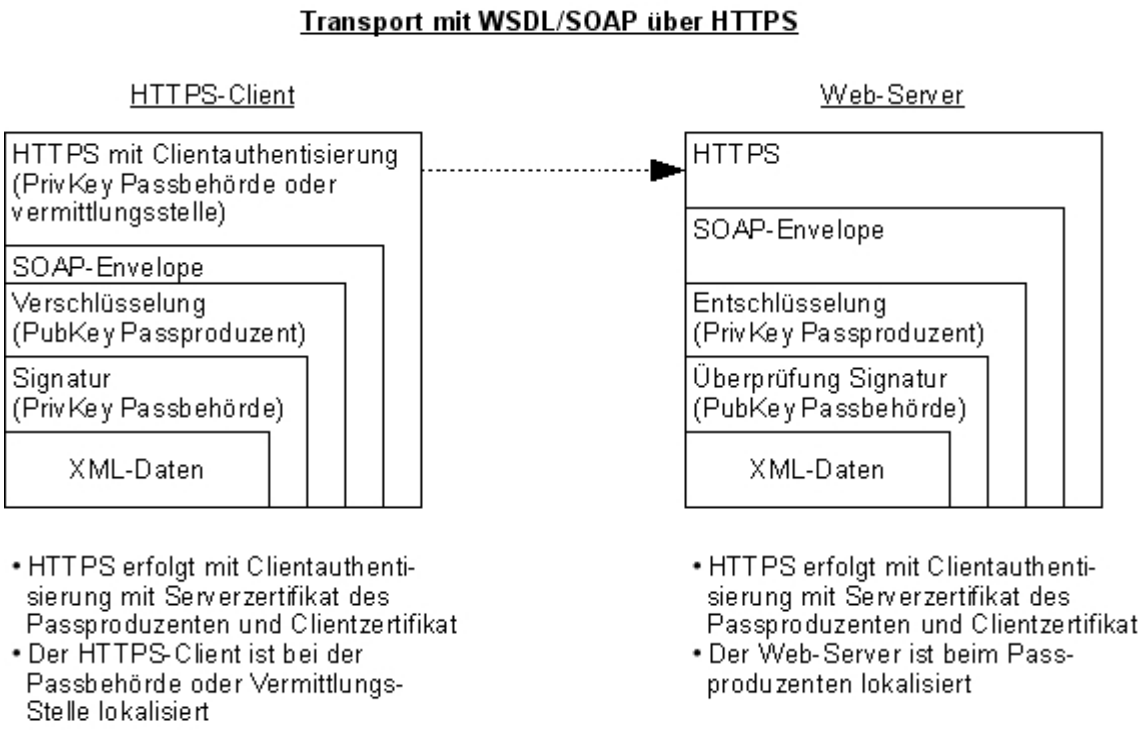


Abbildung 8: Datensicherheit auf Transportebene: WSDL/SOAP über HTTPS

7.2.2 Vorgaben für eine Pass-PKI

Für Passhersteller, Vermittlungsstellen und Passbehörden wird eine Pass-PKI innerhalb der Verwaltungs-PKI [V-PKI] betrieben.

Die von der Pass-PKI herausgegebenen Zertifikate müssen dem Standard X.509 in Version 3 [X.509] entsprechen, die Zertifikate müssen konform zu ISIS-MTT [ISIS-MTT] sein.

Bei den verwendeten Schlüssellängen und Algorithmen sind die jährlichen Empfehlungen der Bundesnetzagentur zur Eignung von Signaturalgorithmen gemäß § 17(1) SigG [BNetzA] zu beachten.

Der Aufbau der Pass-PKI und ihre Zertifikatsprofile sind in der Zertifizierungsrichtlinie (Certificate Policy, CP) der Pass-PKI festgelegt [PKI-CP].

Eine Schlüsseltrennung für Signatur-/Authentisierungszertifikate einerseits und Verschlüsselungszertifikate andererseits ist vorzunehmen, um Verschlüsselungszertifikate zum Zugriff auf verschlüsselt gespeicherte Daten archivieren zu können. Vermittlungsstellen brauchen keine Signaturzertifikate. Details hierzu sind in der CP geregelt.

Als Authentisierungszertifikate für die Transportebene in der Variante OSCI-Transport (Zertifikate für OSCI-Clients und OSCI-Intermediär) können auch Zertifikate der V-PKI beliebiger CAs benutzt werden.

Als Authentisierungszertifikate für die Transportebene in der Variante WSDL/SOAP über HTTPS (Client-Zertifikate in den HTTPS-Clients und Server-Zertifikate im Web-Server) können auch ebenfalls Zertifikate der V-PKI beliebiger CAs benutzt werden.

Die Realisierung der Pass-PKI mit ihren technischen Komponenten und organisatorischen Regelungen sind in der Erklärung zum Zertifizierungsbetrieb (Certification Practice Statement, CPS) der Pass-PKI festgelegt [PKI-CPS] und für alle beteiligten Instanzen innerhalb der Pass-PKI bindend.

Die Vorgaben in der CP sind die Grundlage für die CPS. Das BSI prüft und überwacht, ob eine realisierte Pass-PKI ihre Spezifikationen CP und CPS erfüllt.

8. Testdatenübermittlung

Kapitel 8 beschreibt ein Verfahren zur Testdatenübermittlung von der Passbehörde bzw. der Vermittlungsstelle zum Passhersteller zur Problemanalyse und Problembehebung bei der Passdatenübermittlung.

Um eventuell auftretende Störungen während der Betriebsphase der Passdatenübermittlung analysieren und beheben zu können, ist es sinnvoll, eine Möglichkeit einzurichten, um fiktive Antragsdaten zu Testzwecken (Testdaten) vom Antragsteller (Passbehörde, Vermittlungsstelle, Verfahrensentwickler) zum Passhersteller zu übertragen.

Diese Testdaten müssen geeignet gekennzeichnet sein (Testflag, Testbehördenkennung, usw.), müssen vom Passhersteller als Testdaten erkannt werden und dürfen nicht in den Produktionsprozess des Passherstellers eingehen. Die Initiierung des Testablaufs ist zwischen Antragsteller und Passhersteller zu koordinieren.

Gegenstand der Tests können der Übertragungsweg, aber auch die benutzten Inhaltsdaten sein.

9. Konformität und Interoperabilität

Kapitel 9 enthält Festlegungen zur Konformität und Interoperabilität.

Eine Komponente ist konform zu dieser Anlage, wenn sie die Konformitätsprüfung bestanden hat. Eine bestandene Konformitätsprüfung wird vom BSI durch einen Konformitätsbescheid bestätigt. Konformität ist die Voraussetzung für Interoperabilität.

Das Verfahren zur Konformitätsprüfung und Festlegungen zur Interoperabilität werden im Annex 4 [Annex-Konformität] zu dieser Anlage geführt.

10. Zentrale Qualitätssicherungs-Statistik (QS-Statistik)

Kapitel 10 erläutert die Notwendigkeit einer zentralen QS-Statistik und legt die Vorgaben zur Durchführung fest.

Der Prozess der dezentralen Qualitätsbewertung biometrischer Merkmale in den Passbehörden (Lichtbild: bewertet durch QS-Software in der Passbehörde; Fingerabdruck: QS-Software) erfordert eine genaue Kenntnis der tatsächlichen Qualität der erhobenen Merkmale. Daher ist eine zentrale Qualitätssicherungs-Statistik aus den folgenden Gründen notwendig:

- Um die Konformität der übertragenen Merkmale gemäß den Anforderungen aus Annex 1 und 2 zu überwachen.
- Um eine breite statistische Basis für die Definition von (neuen) Grenzwerten für die Qualitätskriterien zu gewinnen.
- Um eine Einschätzung über die Gesamtleistung des biometrischen Systems zu erhalten.
- Um notwendige Verbesserungen am Prozess der Erhebung biometrischer Merkmale festzulegen.
- Um Abweichungen von den Vorgaben zur Erfassung und Qualitätssicherung der biometrischen Daten in den Passbehörden zu identifizieren.
- Um ggf. fehlerhafte Hardware in den Passbehörden zu erkennen.

Es müssen Versionsinformationen der verwendeten Module und Parameterdateien, die bei der dezentralen Qualitätsbewertung (siehe Annex 1 und 2) anfallen, zum Passhersteller übermittelt werden. Hier findet eine erneute (zentrale) Bewertung der gelieferten Bilddaten statt.

Eine Abweisung des Antrags bei Abweichungen im Vergleich zur QS-Bewertung in der Passbehörde findet nicht statt.

Der Passhersteller stellt die in der QS-Statistik erfassten Daten dem BMI bzw. den nachgeordneten Behörden (BKA, BSI) zu weiteren Auswertungen zur Verfügung. Die Statistik enthält generell keine personenbezogenen Daten.

Die mit dem Passantrag zusätzlich zu übermittelnden Daten, Vorgaben für die zu erfolgende Speicherung und Auswertung beim Passhersteller und Bereitstellung der Daten zur weiteren Auswertung wird in Annex [Annex-QS-Finger], [Annex-QS-Gesicht] und [Annex-XPASS] geregelt.

11. Abkürzungen

Abkürzung	Erklärung
BKA	Bundeskriminalamt
BNetzA	Bundesnetzagentur
BSI	Bundesamt für Sicherheit in der Informationstechnik
CP	Certificate Policy, Zertifizierungsrichtlinie
CPS	Certification Practice Statement, Erklärung zum Zertifizierungsbetrieb
CRL	Certificate Revocation List, Sperrliste
HTTP	Hypertext Transfer Protocol
HTTPS	HTTP Secure
ICAO	International Civil Aviation Organization
ISIS-MTT	Industrial Signature Interoperability Specification-MailTrusT
ISO	International Organization for Standardization
LDAP	Lightweight Directory Access Protocol
OCSP	Online Certificate Status Protocol
OSCI	Online Service Computer Interface
PassG	Passgesetz
PassDEÜV	Passdatenerfassungs- und -übermittlungsverordnung
PKI	Public Key Infrastructure
QS	Qualitätssicherung
SigG	Signaturgesetz
SOAP	Simple Object Access Protocol
SSL	Secure Socket Layer
TLS	Transport Layer Security
UCS	Universal Character Set (ISO 10646, Unicode)
UDDI	Registry Universal Description, Discovery and Integration
UTF-8	UCS Transformation Format, 8 Bit
WSDL	Web Services Description Language
X.509	ITU-T Recommendation X.509, Authentication Framework

Abkürzung	Erklärung
XML	Extensible Markup Language

12. Referenzen

[Annex-Konformität] Konformitätsprüfung zur Technischen Richtlinie zur Produktionsdatenerfassung, -qualitätsprüfung und -übermittlung für Pässe, Annex 4: Konformität

[Annex-QS-Finger] Qualitätsanforderungen bei der Erfassung und Übertragung der Fingerabdrücke als biometrische Merkmale für elektronische Pässe, Annex 2: Fingerabdrücke

[Annex-QS-Gesicht] Qualitätsanforderungen bei der Erfassung und Übertragung des Lichtbilds als biometrisches Merkmal für elektronische Pässe, Annex 1: Lichtbild

[Annex-XPASS] Datenaustauschformat für die Übermittlung von Daten für elektronische Pässe, Annex 3: XPass - Datenmodell

[BNetzA] Auflistung geeigneter 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: http://www.bundesnetzagentur.de/enid/eaebfc8c88eb553443713ca1ae98cefd,0/Veroeffentlichungen/Algorithmen_sw.html

[ICAO_04] International Civil Aviation Organization, Technical Advisory Group on Machine Readable Travel Documents / New Technologies Working Group (2004):

[ISIS-MTT] Common ISIS-MailTrusT Specifications für interoperable PKI Applications, V1.1 (März 2004)

[ISO_FACE] ISO/IEC 19794-5:2005, Information technology -- Biometric data interchange formats -- Part 5: Face image data

[ISO_FINGER] ISO/IEC 19794-4:2005, Information technology -- Biometric data interchange formats -- Part 4: Finger image data

[OSCI] OSCI-Transport 1.2, Spezifikation, OSCI Leitstelle, 06. Juni 2002, http://www.osci.de/materialien/osci_spezifikation_1_2_deutsch.pdf

[PKI-CP] Zertifizierungsrichtlinie (Certificate Policy, CP) der PassPKI, BSI

[PKI-CPS] Erklärung zum Zertifizierungsbetrieb (Certification Practice Statement, CPS) der PassPKI, BSI

[SOAP] http://www.w3.org/TR/2003/REC-soap12-part1-20030624/

[V-PKI] http://www.bsi.de/fachthem/verwpki/index.htm

[WSDL] Erik Christensen, Curbera, Mredith, Weerawarana, Services Description Language (WSDL) 1.1, W3C Note 15 March 2001, http://www.w3.org/TR/wsdl

[X.509] ITU-T X.509: Information Technology - Open Systems Interconnection – The Directory: Authentication Framework, 1997

[XDSIG] Bartel, Boyer, Fox, LaMacchia, Simon: XML-Signature Syntax and Processing, W3C Recommendation, 12 February 2002, http://www.w3.org/TR/2002/REC-xmldsig-core-20020212/

[XENC] Imamura, Dillaway, Simon: XML Encryption Syntax and Processing, W3C Recommendation, 10 December 2002, http://www.w3.org/TR/2002/REC-xmlenc-core-20021210/

[XML] Extensible Markup Language (XML) 1.0 (Second Edition). W3C Recommendation 6 October, http://www.w3.org/TR/2000/REC-xml-20001006/