White Paper

Neuer Personalausweis – Sicherheitsanforderungen für Diensteanbieter

Version 1.0

März 2011

Herausgeber:
Bundesministerium des Innern
Alt-Moabit 101D
10559 Berlin

Projektleitung:
Fraunhofer-Institut für Offene Kommunikationssysteme (FOKUS)
Kaiserin-Augusta-Allee 31
10589 Berlin

Ansprechpartner:
Jens Fromm (jens.fromm@fokus.fraunhofer.de)
Marian Margraf (marian.margraf@bmi.bund.de)
Andreas Poller (andreas.poller@sit.fraunhofer.de)

Inhaltsverzeichnis

1. ZIELGRUPPE DIESES DOKUMENTS 4

2. BEGRÜNDUNG DER SICHERHEITSANFORDERUNGEN 4

3. DER GEGENSEITIGE IDENTITÄTSNACHWEIS 5

4. ENTSCHEIDUNG FÜR DEN EID-SERVICE ODER DEN EIGENEN EID-SERVER 7

5. SICHERHEITSMAßNAHMEN BEI NUTZUNG EINES EID-SERVICE 8

5.1 Sicherheitskonzept des Diensteanbieters 9

5.2 Maßnahmen für den Web-Server 9

5.3 Maßnahmen für die Kommunikation mit dem Web-Browser des Nutzers 10

5.4 Maßnahmen für die Kommunikation mit der AusweisApp des Nutzers 10

5.5 Maßnahmen für die Kommunikation mit dem eID-Server 10

5.6 Maßnahmen für die Kommunikation mit den Infrastrukturdiensten 11

5.7 Maßnahmen für den eID-Server 11

6. SICHERHEITSMAßNAHMEN BEI NUTZUNG EINES EIGENEN EID-SERVERS 12

6.1 Sicherheitskonzept des Diensteanbieters 12

6.2 Maßnahmen für den Web-Server 12

6.3 Maßnahmen für die Kommunikation mit dem Web-Browser des Nutzers 13

6.4 Maßnahmen für die Kommunikation mit der AusweisApp des Nutzers 13

6.5 Maßnahmen für die Kommunikation mit dem eID-Server 13

6.6 Maßnahmen für die Kommunikation mit den Infrastrukturdiensten 13

6.7 Maßnahmen für den eID-Server 13

7. SICHERHEITSMAßNAHMEN IM ÜBERBLICK 14

8. KONSEQUENZEN FÜR DEN DIENSTEANBIETER BEI NICHTBEACHTUNG 15

9. LINKS 15

10. REFERENZEN 16

11. INFORMATIONEN 17

1. Zielgruppe dieses Dokuments

Zielgruppe dieses White Papers sind IT-Entscheider und Mitarbeiter von Unternehmen, welche die Online-Ausweisfunktion (eID-Funktion) des neuen Personalausweises in Web-Anwendungen und Kundensysteme integrieren möchten. Angesprochen sind insbesondere Personen, die innerhalb der Unternehmen für die technische Ausgestaltung und Anwendungssicherheit der eID-Integration verantwortlich sind. Dieses White Paper betrachtet den häufigsten Anwendungsfall des neuen Ausweises im E-Business und E-Government, nämlich die Online-Authentisierung über das Internet gegenüber der Web-Anwendung eines Diensteanbieters. Hersteller und Betreiber von Automaten (z.B. Verkaufsautomaten, Selbstbedienungsautomaten), welche Interesse an einer Integration des neuen Personalausweises haben, sei ergänzend das White Paper " Automaten-Anwendungen" empfohlen.

2. Begründung der Sicherheitsanforderungen

Auf einen Blick

- Datenschutz und Datensicherheit sind nach dem Stand der Technik zu erfüllen.
- eID-Daten aus dem Personalausweis besitzen das Schutzniveau „hoch“.
- Vorgaben des Datenschutzgesetzes sind zu beachten.
- Verbot der Weitergabe der Daten ohne Einwilligung.

Die Anforderungen zum Schutz der eID-Daten des neuen Personalausweises leiten sich aus dem Personalausweisgesetz (PAuswG) und der Personalausweisverordnung (PAuswV) ab. Darin heißt es, dass der Diensteanbieter den Datenschutz und die Datensicherheit nach dem Stand der Technik zu erfüllen hat, um insbesondere die Vertraulichkeit und Unversehrtheit der eID-Daten zu gewährleisten. Als Stand der Technik gelten die Vorgaben der technischen Richtlinien, welche in einem Anhang der PAuswV genannt werden. Grundlage dieser technischen Richtlinien wiederum ist das Sicherheitsrahmenkonzept des neuen Ausweises, das für alle eID-Daten des neuen Ausweises das Schutzniveau "hoch" vorsieht. Die damit verbundenen Anforderungen und Maßnahmen sind in der IT-Grundschutzsystematik des BSI näher beschrieben. Das hohe Schutzniveau gilt auch dann, wenn ausschließlich datensparsame Funktionen, z.B. die Altersverifikation oder die Pseudonymfunktion des Ausweises genutzt werden. In jedem Fall sind die Vorgaben des Bundesdatenschutzgesetzes (BDSG) zu beachten:

- Einhaltung der Zweckbindung der ausgelesenen Daten
- Recht auf Auskunft über gespeicherte Daten bzw. Löschen gespeicherter Daten
- Verpflichtung zur Absicherung der Verarbeitung personenbezogener Daten
- Verbot der Weitergabe der Daten ohne Einwilligung.

Der Diensteanbieter ist auch dann für die Einhaltung der Datenschutzvorschriften verantwortlich, wenn ein eID-Service genutzt wird, der die persönlichen Daten des Ausweisinhabers im Auftrag des Dienstanbieters erfasst (vgl. §11 BDSG). Die Vergabestelle für Berechtigungszertifikate (VfB) des Bundesverwaltungsamts ist dazu befugt, konkrete technische und organisatorische Anforderungen für Diensteanbieter festzulegen (vgl. §29 Abs.2 PAuswV). In der Regel wird die VfB dabei auf die technischen Richtlinien des BSI verweisen, insbesondere auf die Richtlinie [TR-3130], in der sicherheitstechnische Anforderungen an den Betrieb von eID-Servern beschrieben sind. Weitere Vorgaben werden ggf. unter www.personalausweisportal.de veröffentlicht.

Gemäß den technischen Richtlinien müssen grundsätzlich alle Nachrichten, die über offene Netze laufen, verschlüsselt und digital signiert werden, um im Gesamtsystem den Schutz der eID-Daten auf hohem Niveau zu gewährleisten. Die Einsatzumgebung des Diensteanbieters muss die zugehörigen kryptographischen Schlüssel und Zertifikate vor missbräuchlichem Zugriff schützen. Auch die Verfügbarkeit des eID-Servers und seine Kommunikation mit den Infrastrukturdiensten stehen unter dem Schutzniveau "hoch". Die folgenden Kapitel beschreiben die wichtigsten Sicherheitsmaßnahmen, für die der Diensteanbieter verantwortlich ist.

3. Der gegenseitige Identitätsnachweis

Auf einen Blick

- Sichere gegenseitige Identitätsprüfung im Internet zwischen Ausweisinhaber und Diensteanbieter.
- Erhöhter Schutz vor Online-Betrug und Identitätsdiebstahl.
- Alle Nachrichten, die über offene Netze laufen müssen verschlüsselt und digital signiert werden.

Der neue Personalausweis bietet mit seiner Online-Ausweisfunktion die Möglichkeit einer sicheren gegenseitigen Identitätsprüfung im Internet zwischen Ausweisinhaber und Diensteanbieter des E-Government / E-Business. Bei dieser so genannten Online-Authentisierung kann sich der Bürger mittels des neuen Ausweises einfach und sicher ausweisen.

Der Diensteanbieter identifiziert sich mit Hilfe des Berechtigungszertifikates gegenüber dem Bürger, das vom Ausweis-Chip überprüft wird. Auf diese Weise erhält der Diensteanbieter gemäß seiner Berechtigung persönliche Daten aus einem hoheitlichen Dokument. Die Online-Authentisierung kann auf diese Weise den Schutz vor fehlerhaften Dateneingaben, Online-Betrug und Identitätsdiebstahl erhöhen. Abb. 1 zeigt den Ablauf der Online-Authentisierung zwischen dem PC des Dienstenutzers, dem Web-Server des Diensteanbieters und dem eID-Server. Die Online-Authentisierung läuft in den folgenden Schritten ab:

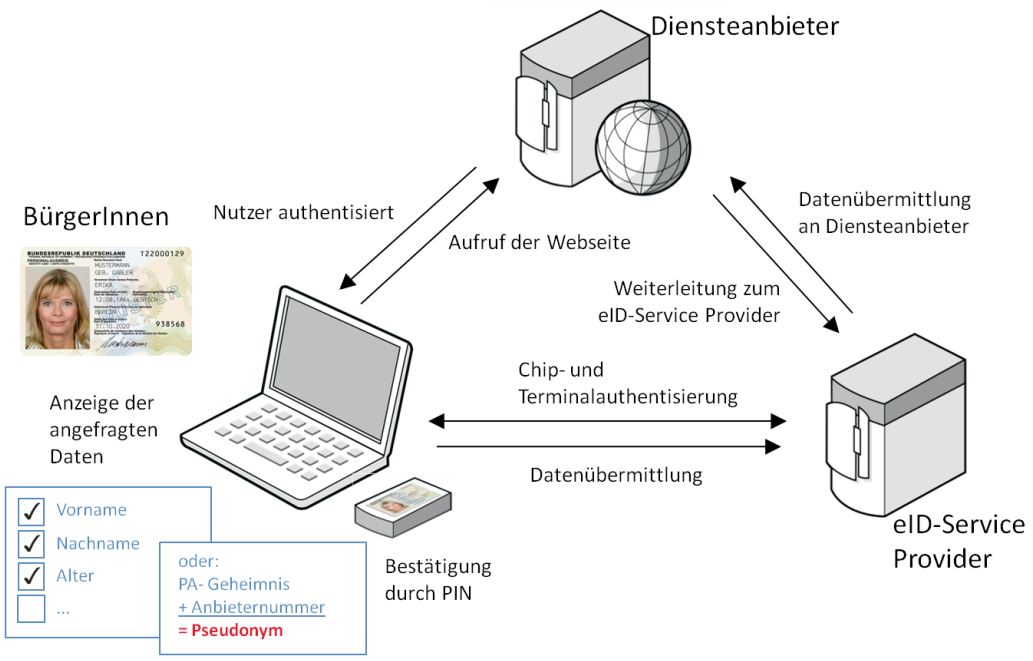

Abb. 1: Ablauf der Online-Authentisierung

Auf einen Blick

- Alle persönlichen Informationen werden durch kryptographische Sicherheitsmechanismen geschützt.
- Der eID-Server darf keine Identitätsdaten vorhalten.
- Der Nutzer authentisiert sich gegenüber dem Diensteanbieter

1. Der Nutzer ruft über den Web-Browser eine Seite in der Web-Anwendung des Diensteanbieters auf, für die ein Identitätsnachweis erforderlich ist.

2. Die Web-Anwendung antwortet mit einer Authentisierungsanfrage an den eID-Server.

3. Der eID-Server sendet Informationen über den Diensteanbieter (Datenschutzerklärung, gewünschte Leserechte, Daten für die Alters- und Wohnortverifikation etc.) an den Nutzer und ruft über den Web-Browser die AusweisApp des Nutzers auf.

4. Nachdem der Nutzer seinen Personalausweis auf den Kartenleser gelegt hat, werden ihm Informationen über den Diensteanbieters angezeigt. Der Nutzer kann die Auswahl der Daten, die der Diensteanbieter vom Ausweis lesen darf, weiter einschränken.

5. Zur Freigabe der Daten gibt der Bürger abschließend seine sechsstellige PIN ein. Mittels PACE-Protokoll wird die Korrektheit der eingegebenen PIN überprüft und eine sichere Verbindung zum kontaktlosen Ausweis-Chip aufgebaut.

6. Der eID-Server führt mittels der kryptographischen Protokolle die Kommunikation mit dem Personalausweis durch. Dies ist der zentrale Vorgang der Online-Authentisierung. Der Ausweis prüft zunächst das Berechtigungszertifikat und die Authentisierungsdaten des Diensteanbieters (Terminal-Authentisierung). Anschließend prüft der eID-Server, ob es sich um einen echten Ausweis handelt (Chip-Authentisierung), ob der Ausweis noch gültig und nicht als gesperrt gemeldet ist. Schließlich werden über den verschlüsselten Kommunikationskanal die vom Nutzer freigegegebenen eID-Daten aus dem Ausweis gelesen.

7. Die ermittelten Ergebnisse und eID-Daten werden vom eID-Server an den Web-Server des Diensteanbieters zu Verfügung gestellt.

8. Die Web-Anwendung des Diensteanbieters entscheidet, ob die Authentisierung des Nutzers als erfolgreich gelten kann und sendet die Antwort an den Web-Browser des Nutzers. Im Erfolgsfall bekommt der Nutzer Zugang zum angefragten Dienst.

Als wichtigste Komponente der Online-Authentisierung bietet der neue Personalausweis hohe Sicherheit für die im Ausweis elektronisch gespeicherten eID-Daten. Alle persönlichen Informationen werden gleichermaßen als sensibel behandelt und durch dieselben kryptographischen Sicherheitsmechanismen geschützt. Dabei ist bereits konzeptionell sichergestellt, dass die Übertragung der eID-Daten vom Ausweis-Chip zum eID-Server mittels der Sicherheitsmechanismen immer gegen Zugriff durch Dritte gesichert ist.

Als Identitätsnachweis des Nutzers gilt die geschützte Übermittlung der eID-Daten an den eID-Server und die Weitergabe der Daten an den Web-Server des Diensteanbieters. Der eID-Server darf dabei keine Identitätsdaten vorhalten und gar als Identity Provider gegenüber Dritten auftreten. Der Nutzer authentisiert sich formal gegenüber dem Diensteanbieter, der die Berechtigung besitzt, bestimmte eID-Daten aus dem Personalausweis zu lesen. Der Diensteanbieter ist daher für die Einhaltung sämtlicher Sicherheitsanforderungen an die Ermittlung und den Umgang mit den eID-Daten des Personalausweises verantwortlich. Einen Überblick über die Verfahren und technischen Spezifikationen gibt die Richtlinie [TR-3127].

4. Entscheidung für den eID-Service oder den eigenen eID-Server

Auf einen Blick

- Einsatz eines eigenen eID-Servers oder eines eID-Services eines externen Anbieters.
- eID-Server:
  Diensteanbieter für Einhaltung der organisatorischen, technischen und sicherheitstechnischen Maßnahmen verantwortlich.
- eID-Service:
  Alle wesentlichen Maßnahmen werden vom Betreiber des eID-Service durchgeführt.

Um den elektronischen Identitätsnachweis des neuen Personalausweises nutzen zu können, benötigt der Diensteanbieter die Anbindung seiner Web-Anwendung an einen eID-Server. Dies

erfolgt über die eID-Schnittstelle des eID-Servers wie in der Richtlinie [TR-3130] beschrieben. Als zentrale Infrastrukturkomponente kommuniziert der eID-Server zudem über die so genannte eCard-API gemäß [TR-3112] mit der AusweisApp und dem Personalausweis des Nutzers sowie über die PKI-Schnittstelle [TR-3128] mit den zentral bereitgestellten Infrastrukturdiensten, um Berechtigungszertifikate, Dokumentenprüfschlüssel und Ausweissperrlisten zu laden. Neben den genannten funktionalen Schnittstellen besitzt der eID-Server eine administrative Schnittstelle [TR-3130] zur Konfiguration von Parametern und Schlüsseln. An den Betrieb des eID-Servers werden besondere sicherheitstechnische Anforderungen gestellt.

Dem Diensteanbieter stehen grundsätzlich zwei alternative Integrationsszenarien zur Auswahl: Er kann den eID-Service eines externen Dienstleisters nutzen oder seinen eigenen eID-Server betreiben. Abb. 2 zeigt das erste Szenario mit Nutzung eines eID-Service, das insbesondere für kleine und mittlere Unternehmen attraktiv ist.

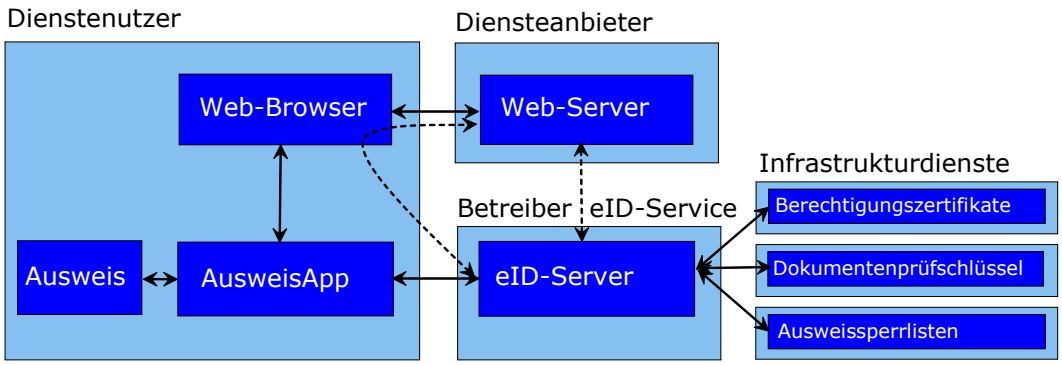

Abb. 2: Szenario mit Nutzung eines eID-Service

Die Vorteile liegen auf der Hand: Alle wesentlichen Maßnahmen zur Durchführung der Online-Authentisierung werden beim Betreiber des eID-Servers durchgeführt. Der Diensteanbieter benötigt für die Anbindung an den eID-Service kein anspruchsvolles technisches Know-How und kann auf zusätzliche Ausstattung weitgehend verzichten. Dennoch bleibt der Diensteanbieter formal für die Einhaltung sämtlicher Sicherheitsanforderungen verantwortlich, auch im Bereich des eID-Service. Führt ein externer Dienstleister im Namen mehrere Diensteanbieter Online-Authentisierungen durch, so liegt ein mandantenfähiger eID-Service vor. Die Kommunikation zwischen eID-Service und Web-Server läuft typischerweise über offene Netze, z.B. das Internet, und muss daher besonders geschützt werden.

In einem zweiten Szenario betreibt der Diensteanbieter seinen eigenen eID-Server, siehe Abb. 3. Folglich muss er selbst für die Einhaltung der organisatorischen, technischen und sicherheitstechnischen Maßnahmen zur Durchführung der Online-Authentisierung sorgen.

Dazu gehört auch, die beiden Kommunikationsverbindungen des Web-Servers und des eID-Servers zum PC des Nutzers eindeutig einander zuzuordnen. Web-Server und eID-Server sind typischerweise in einer geschützten Umgebung des Diensteanbieters aufgestellt und über ein internes Netz verbunden. Die Kommunikation zwischen eID-Server und Web-Server kann dennoch auch in diesem Szenario über den PC des Nutzers und damit über offene Netze verlaufen.

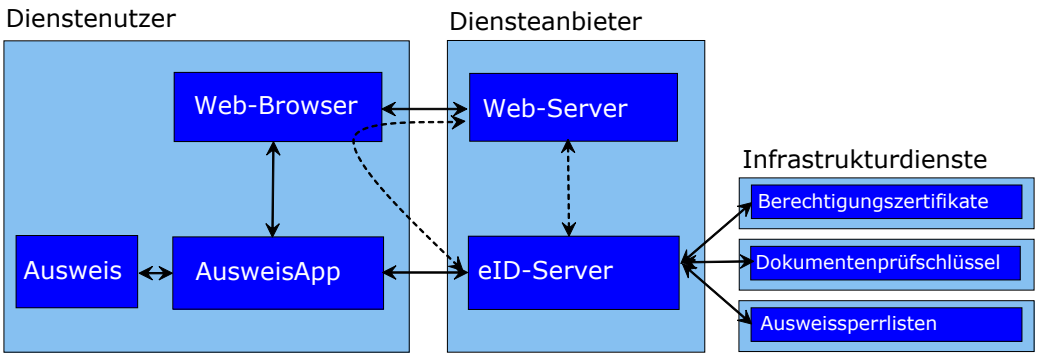

Abb. 3: Szenario mit eigenem eID-Server

Um für beide Szenarien die Integration der eID-Funktion in den Web-Server zu vereinfachen, beschreibt die technische Richtlinie [TR-3130] eine eID-Schnittstelle, die als Web Service für die direkte Kommunikation zwischen Web-Server und eID-Server genutzt werden kann. Die Web-Anwendung ruft dazu wiederholt die eID-Schnittstelle des eID-Servers auf, bis die eID-Daten vom Ausweis ausgelesen wurden und zur Beantwortung der Anfrage vorliegen. Diese direkte eID-Anbindung ist in Abb. 2 und Abb. 3 als gestrichelte Verbindung zwischen Web-Server und eID-Server dargestellt. Als alternative Anbindung ist in [TR-3130] eine Kommunikation mit SAML-Token [SAML] und ein entsprechendes SAML-Profil beschrieben. Dabei kommunizieren der Web-Server und der eID-Server nicht direkt miteinander, sondern mittels POST-Binding ausschließlich über den Web-Browser des Nutzers. Diese Anbindung ist in Abb. 2 und Abb. 3 als gestrichelte Verbindung angedeutet, die über den Web-Browser des Nutzers verläuft. Welche Anbindung konkret genutzt wird, muss der Diensteanbieter mit dem Betreiber des eID-Servers abstimmen.

5. Sicherheitsmaßnahmen bei Nutzung eines eID-Service

Nutzt der Diensteanbieter einen eID-Service, so verlässt er sich in der Regel darauf, dass der Betreiber des eID-Service alle technischen Anforderungen beachtet und die notwendigen Sicherheitsmaßnahmen implementiert hat. Der Diensteanbieter ist aber formal auch für die Sicherheit des eID-Services verantwortlich und muss den eID-Service in seinem Sicherheitskonzept mitbetrachten. Abb. 4 zeigt die Kommunikationskanäle zwischen Diensteanbieter, Nutzer und Betreiber des eID-Service.

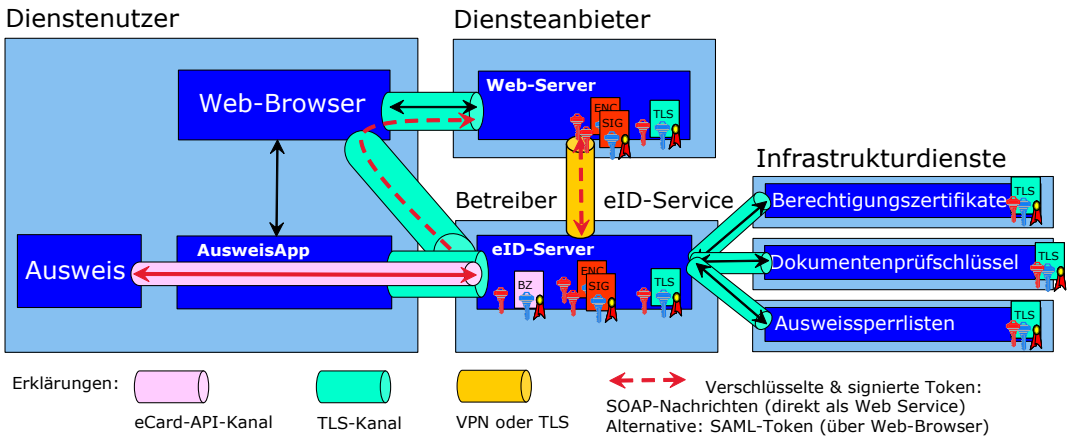

Abb. 4: Kommunikationsverbindungen bei Nutzung eines eID-Service

Die Kommunikation über offene Netze erfolgt über abgesicherte TLS-Verbindungen. In Abb. 4 angedeutet sind die notwendigen Zertifikate und zugehörigen Schlüsselpaare auf Seiten des Diensteanbieters. Da der PC des Nutzers in den TLS-Verbindungen immer die Rolle des Aufrufers (TLS-Clients) innehat, wird dort kein eigenes TLS-Zertifikat benötigt. Die eID-Schnittstelle zwischen Web-Server und eID-Service kann anstelle von TLS auch durch ein anderes Verfahren geschützt werden, z.B. durch ein virtuelles privates Netz (VPN).

5.1 Sicherheitskonzept des Diensteanbieters

Auf einen Blick

- Die Kommunikation erfolgt über abgesicherte TLS-Verbindungen.
- Der Diensteanbieter muss ein Sicherheitskonzept erstellen, welches die Einhaltung der technischen und organisatorischen Sicherheitsanforderungen darstellt.
- Der Webserver muss in einer sicheren Betriebsumgebung aufgestellt sein.

Auf Basis der technischen Richtlinien muss der Diensteanbieter ein Sicherheitskonzept erstellen, das die Maßnahmen zur Einhaltung der technischen und organisatorischen Sichereitsanforderungen nachvollziehbar darstellt. Dazu gehören insbesondere die Verhinderung unberechtigten Zugriffs auf das Schlüsselmaterial und die Schutzmaßnahmen gegen den Missbrauch der übertragenen eID-Daten durch Dritte. Neben der Organisation und Technik im eigenen Hause muss das Konzept auch den Betreiber des eID-Service sowie die Kommunikation zwischen Web-Server und eID-Service betrachten. Leitlinien für das Sicherheitskonzept sind im Anhang C der Richtlinie [TR-3130] zu finden.

Der Diensteanbieter ist dazu verpflichtet, auf dieser Grundlage sein Sicherheitskonzept laufend zu aktualisieren und bei Aufforderung der VfB vorzulegen.

5.2 Maßnahmen für den Web-Server

Als vordringliche Maßnahme muss der Diensteanbieter den Web-Server gegen webbasierte Angriffe absichern. Der Web-Server muss in einer sicheren Betriebsumgebung aufgestellt sein, da die vom eID-Server sicher empfangenen eID-Daten geschützt werden müssen. Geht z.B. der Diensteanbieter mit den privaten Schlüsseln sorglos um, können diese Schlüssel Angreifern in die Hände fallen. Diese könnten dann, z.B. im Falle der eID-Anbindung mit SAML-Token, Nachrichten abfangen und eID-Daten entschlüsseln. Zum Schutz der kryptographischen Schlüssel und Zertifikate stehen Software-Lösungen zur Verfügung, dessen Zugriffsschutz in der Regel per Passwort gewährleistet ist. Derartig geschützte Schlüssel und Zertifikate werden als Soft-

token oder auch als Software-Zertifikate bezeichnet. Im Falle eines erfolgreichen Angriffs auf den Web-Server können jedoch Offline-Angriffe auf das Passwort verübt werden, wobei je nach Passwortgüte eine Kompromittierung der Schlüssel möglich ist. Deshalb wird für die sichere Aufbewahrung der Schlüssel und Zertifikate der Einsatz eines kryptographischen Hardwaremoduls empfohlen, beispielsweise eines zertifizierten High Security Modules (HSM). Anstelle eines HSM können auch zertifizierte Signaturkarten eingesetzt werden, die kostengünstiger, aber auch weniger leistungsstark sind.

5.3 Maßnahmen für die Kommunikation mit dem Web-Browser des Nutzers

Auf einen Blick

- Einsatz eines zertifizierten High Security Modules (HSM) wird empfohlen.
- Kommunikation zwischen eID-Service und Web-Server des Diensteanbieters durch gegenseitige Authentisierung und Verschlüsselung der Daten.
- Alternative Übermittlung mittels signiertem SAML-Token

Die Kommunikation zwischen Web-Server des Diensteanbieters und Web-Browser des Nutzers muss auf Basis von HTTPS erfolgen. Das entsprechende TLS-Zertifikat sollte der Diensteanbieter möglichst von einer Zertifizierungsstelle beziehen, deren öffentlicher Schlüssel sich bereits in den gängigsten Web-Browsern, wie z.B. Mozilla Firefox, Apple Safari, Opera und Microsoft Internet Explorer befindet, da in diesem Fall der Nutzer keine manuelle Zertifikatsprüfung vorzunehmen braucht.

Nach erfolgreichem Identitätsnachweis können je nach Geschäftsfall weitere Anfragen durch den Nutzer über den Web-Browser ausgelöst werden. Alle auf die Online-Authentisierung bezogenen Daten, die zwischen dem Web-Browser des Nutzers und der Web-Anwendung des Diensteanbieters ausgetauscht werden, müssen in derselben TLS-Session übertragen werden. Der Web-Server muss die notwendigen Sicherheitsvorkehrungen umsetzen, z.B. im Umgang mit der HTTPS-Session. Ebenso sollten alle weiteren Anwendungsdaten des Dienstangebots über dieselbe TLS-Verbindung übermittelt werden, solange der Nutzer als angemeldet gilt.

5.4 Maßnahmen für die Kommunikation mit der AusweisApp des Nutzers

Der Betreiber des eID-Service führt im Auftrag des Diensteanbieters die Kommunikation zwischen dem eID-Server und der AusweisApp bzw. dem Web-Browser des Nutzers durch. Hierfür ist ebenfalls das TLS-Verfahren vorgeschrieben. Zusätzlich wird auf Anwendungsebene durch die Sicherheitsprotokolle des Ausweises (PACE, Terminal- und Chip-Authentisierung) ein verschlüsselter Kommunikationskanal (eCard-API) zwischen dem Ausweis-Chip und dem eID-Server aufgebaut, um die eID-Daten der Online-Authentisierung zu übertragen, siehe Abb. 4. Dabei ist automatisch sichergestellt, dass die eID-Daten ausschließlich vom beteiligten eID-Server, welcher das Berechtigungszertifikat des Diensteanbieters verwendet hat, entschlüsselt werden können.

5.5 Maßnahmen für die Kommunikation mit dem eID-Server

Für die Kommunikation zwischen eID-Service und Web-Server des Diensteanbieters müssen sich beide Seiten auf Transportebene gegenseitig authentisieren und alle Daten verschlüsseln. Das kann auf Basis von TLS geschehen. TLS kann aber auch gegen eine beliebige andere Verschlüsselungstechnik wie z.B. ein VPN auf Layer 3 oder Layer 2 ausgetauscht werden. Der Web-Server muss das entsprechende Serverzertifikat prüfen, um die Echtheit des eID-Servers sicherzustellen. Auf Anwendungsebene werden signierte SOAP-Nachrichten zwischen eID-Server und Web-Server ausgetauscht, wobei beide Seiten die Echtheit und Integrität der Nachrich-

teninhalte mit einer digitalen Signatur absichern. Alternativ können die eID-Daten per signierten SAML-Token über den Web-Browser des Nutzers vom eID-Server an den Web-Server übermittelt werden. In jedem Fall benötigen beide Server also zusätzliche Zertifikate zum Schutz dieser Nachrichten-Token. Auf Seiten des Diensteanbieters werden die Zertifikate und Sicherheitsmechanismen bevorzugt in der eID-Anbindung des Web-Servers konfiguriert, so dass hierfür keine zusätzlichen Implementierungsarbeiten in der Web-Anwendung anfallen.

5.6 Maßnahmen für die Kommunikation mit den Infrastrukturdiensten

Der Betreiber des eID-Service unterhält die Kommunikation mit den Infrastrukturdiensten, um die Berechtigungszertifikate, Dokumentenprüfschlüssel und Ausweissperrlisten auf den eID-Server zu laden. Hierfür ist ebenfalls das TLS-Verfahren mit einer gegenseitigen Authentisierung vorgeschrieben. Grundlage hierfür ist das Registrierungsverfahren, das der Diensteanbieter gemeinsam mit dem Betreiber des eID-Service bei der VfB durchlaufen muss. Darin einbezogen sind auch die Anbieter der Infrastrukturdienste, die vom Betreiber des eID-Service beauftragt werden.

5.7 Maßnahmen für den eID-Server

Auf einen Blick

- Eindeutige Informationen („Hash-Werte“) der beiden TLS-Zertifikate sind im Berechtigungszertifikat enthalten, diese werden durch AusweisApp und Ausweis geprüft.
- eID-Daten verschiedener Diensteanbieter müssen im eID-Server strikt voneinander getrennt werden.
- eID-Server sollte eine revisionssichere Protokollierung der verwendeten Berechtigungszertifikate übernehmen.

Auch die folgenden Maßnahmen werden vom Betreiber des eID-Service übernommen. So muss der eID-Service die Kommunikationsverbindungen des Web-Servers und des eID-Servers zum PC des Nutzers klar einander zuordnen ("Kanalbindung"). Dazu sind eindeutige Informationen ("Hash-Werte") der beiden TLS-Zertifikate im Berechtigungszertifikat des Diensteanbieters enthalten und werden im Rahmen der Sicherheitsprotokolle auf Seiten des Nutzers von der AusweisApp und dem Personalausweis überprüft. Außerdem wird der TLS-basierte Kommunikationskanal zwischen eID-Server und AusweisApp auf Basis eines Pre-Shared-Keys (PSK) aufgebaut, um die ursprüngliche Verbindung des Diensteanbieters zum Nutzer an die Kommunikation der Online-Authentisierung (eCard-API plus TLS) von AusweisApp und eID-Server zu binden.

Auf Seiten des eID-Service müssen sichere Hardwaremodule (HSM, Signaturkarten) zum Einsatz kommen, um die Speicherung der eID-Daten, Zertifikate und Sperrlisten physikalisch abzusichern und rollenbasierte Zugriffsmechanismen und logische Zugriffe auf das Schlüsselmaterial zuverlässig zu kontrollieren. Keinesfalls darf der eID-Service die ausgelesenen Daten dauerhaft speichern, sondern muss sie unmittelbar nach der Übermittlung an den Diensteanbieter löschen.

Betreut der Betreiber des eID-Service mehrere Diensteanbieter, dann sind die Sicherheitsinformationen verschiedener Diensteanbieter und für verschiedene Diensteanbieter ausgelesenen eID-Daten strikt voneinander zu trennen (Mandantentrennung).

Der mandantenfähige eID-Service muss die eindeutige Zuordnung von Diensteanbieter bzw. Dienst zu einem Berechtigungszertifikat als Funktionalität des eID-Servers realisieren. Da der Web-Server des Diensteanbieters jede Anfrage an den eID-Server mit seinem Tokenschlüssel signiert, kann der eID-Server nach Überprüfung der Signatur den Mandanten anhand seines Tokenzertifikats identifizieren. Die Anfrage wird dann im Auftrag des Mandanten und mit dessen Berechtigungszertifikat bearbeitet.

Der Betreiber des eID-Service muss technisch und organisatorisch sicherstellen, dass Ausweisdaten ausschließlich an den Diensteanbieter übermittelt werden, in dessen Auftrag sie ausgelesen wurden. Schließlich muss der eID-Server eine revisionssichere Protokollierung der verwendeten Berechtigungszertifikate vornehmen, damit der Betrieb jederzeit nachvollziehbar ist.

6. Sicherheitsmaßnahmen bei Nutzung eines eigenen eID-Servers

Unterhält der Diensteanbieter seinen eigenen eID-Server, so ist er direkt für die Komponenten und Kommunikationsverbindungen des Web-Servers und eID-Servers verantwortlich. Abb. 5 zeigt die Kommunikation zwischen Web-Server und eID-Server des Diensteanbieters und den Komponenten des Dienstenutzers und der Infrastrukturdienste. Grundsätzlich gelten die im vorigen Kapitel genannten Sicherheitsmaßnahmen, d.h. die Kommunikation über offene Netze muss über TLS-Verbindungen abgesichert werden. Allerdings muss der Diensteanbieter direkt auch für die Sicherheitsmaßnahmen des eID-Servers und seiner Kommunikationsverbindungen sorgen. Daher gelten strengere Vorgaben an die Betriebsumgebung des Diensteanbieters.

6.1 Sicherheitskonzept des Diensteanbieters

Für das Sicherheitskonzept des Diensteanbieters bestehen grundsätzlich strengere Anforderungen als die in Kapitel 5.1 genannten. Auf Basis der technischen Richtlinien ist der Diensteanbieter verpflichtet, ein Sicherheitskonzept gemäß den Standards [BSI-100-2], [BSI-100-3] und [BSI-100-4] zu erstellen, in dem die grundsätzlichen Gefährdungen der IT-Grundschutz-Kataloge und die entsprechenden Sicherheitsmaßnahmen dargestellt werden. Zur Überprüfung und Bestätigung der IT-Grundschutz-Vorgehensweise wird dem Diensteanbieter mit eigenem eID-Server schließlich eine Grundschutz-Zertifizierung nach [ISO-27001] empfohlen.

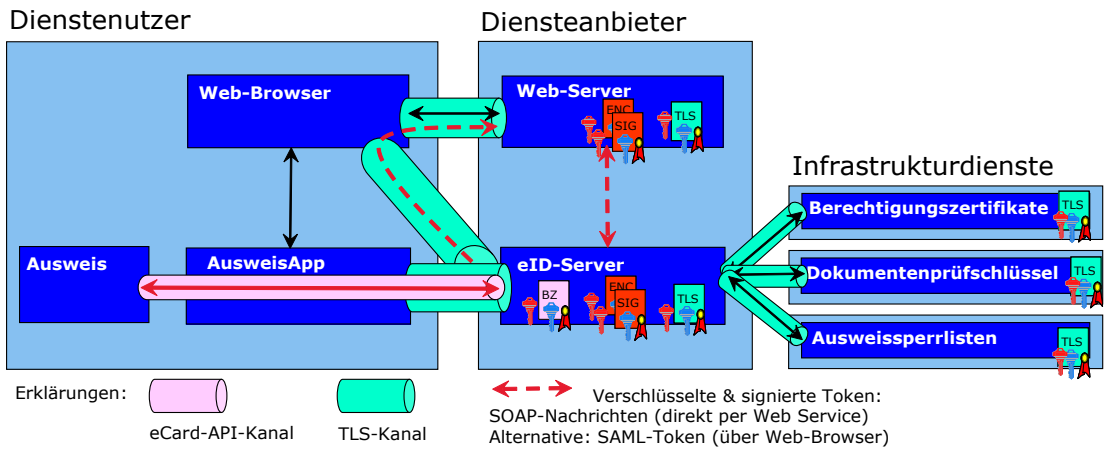

Abb. 5: Kommunikationsverbindungen bei Nutzung eines eigenen eID-Servers

6.2 Maßnahmen für den Web-Server

Für den Web-Server des Diensteanbieters sind mindestens die in Kapitel 5.2 genannten Sicherheitsmaßnahmen erforderlich. Der Web-Server sollte möglichst in der gleichen sicheren Betriebsumgebung wie der eID-Server aufgestellt sein, um in beiden Servern das gleiche hohe Niveau zum Schutz der eID-Daten zu realisieren.

6.3 Maßnahmen für die Kommunikation mit dem Web-Browser des Nutzers

Da für die Kommunikation mit dem Web-Browser prinzipiell die gleichen Anforderungen gelten bezogen auf die Nutzung eines eigenen eID-Servers oder eines eID-Service, gelten die in Kapitel 5.3 genannten Sicherheitsmaßnahmen.

6.4 Maßnahmen für die Kommunikation mit der AusweisApp des Nutzers

Der Diensteanbieter muss nun selbst sicherstellen, dass sich die Online-Authentisierung des Nutzers gegenüber dem eID-Server mittels der offiziellen AusweisApp durchführen lässt. Auf diese Weise kann jeder Nutzer, auch ohne im Web-Browser aktive Inhalte zuzulassen, die eID-Funktion des neuen Ausweises nutzen. Grundsätzlich kann natürlich auf dem PC des Nutzers eine andere Implementierung der AusweisApp zum Einsatz kommen. Der eID-Server des Diensteanbieters darf entsprechend andere Formen der Authentisierung mit dem neuen Personalausweis unterstützen. Bietet der Diensteanbieter dem Nutzer eine alternative Software zum Download an, muss diese jedoch vom BSI nach [PP-AA] zertifiziert sein. In jedem Fall muss der Nutzer den Hinweis erhalten, dass für die Online-Authentisierung auch die offizielle AusweisApp verwenden werden kann und dass diese kostenlos über das Downloadportal des BMI (www.ausweisapp.bund.de) erhältlich ist. Aus Gründen der Sicherheit darf der Diensteanbieter die AusweisApp nicht selbst zum Download anbieten.

6.5 Maßnahmen für die Kommunikation mit dem eID-Server

Der eID-Server und Web-Server des Diensteanbieters müssen sich innerhalb der Netzstruktur eindeutig identifizieren und authentisieren, wobei eine Transportverschlüsselung entfallen darf, wenn der eID-Server im selben Sicherheitsbereich wie der Web-Server betrieben wird. Die Nachrichten müssen aber immer auf Anwendungsebene verschlüsselt und signiert sein.

6.6 Maßnahmen für die Kommunikation mit den Infrastrukturdiensten

Der Diensteanbieter muss nun mit dem eigenen eID-Server die Kommunikation mit den Infrastrukturdiensten unterhalten. Hierfür ist ebenfalls das TLS-Verfahren mit einer gegenseitigen Authentisierung vorgeschrieben. Grundlage ist ein Registrierungsverfahren, das der Diensteanbieter bei der VfB durchlaufen muss. Hierfür müssen auch die Anbieter der Infrastrukturdienste genannt werden, die der Diensteanbieter nach Erhalt der Berechtigung beauftragen möchte.

6.7 Maßnahmen für den eID-Server

Als eID-Server darf der Diensteanbieter nur zertifizierte Software-Module einsetzen, die eine Konformitätsprüfung der eCard-API mit der TestSuite des BSI erfolgreich durchlaufen haben. Damit soll sichergestellt werden, dass der eID-Server mit der offiziellen AusweisApp kommunizieren kann. Der eID-Server und der Web-Server müssen in einer sicheren Betriebsumgebung aufgestellt sein, um in beiden Servern das gleiche hohe Niveau zum Schutz der eID-Daten zu realisieren. Die ausschließlich berechtigte Verwendung aller kryptographischen Schlüssel muss durch technische und organisatorische Maßnahmen sichergestellt werden, die durchaus mit denen vergleichbar sind, die in Trustcentern getroffen werden. Dies umfasst insbesondere den Schutz der IT-Systeme vor Angreifern über öffentliche Netze sowie gegenüber Innentätern, z.B. Absicherung durch Einrichtung aufgabenorientierter Nutzerrechte und protokollierbare Nutzeraktivitäten.

Alle Schlüssel und Zertifikate des eID-Servers sind in kryptographischen Hardwaremodulen einzusetzen, die eine physikalisch gesicherte Speicherung und sichere Zugriffsmechanismen reali-

sieren können. Zu beachten ist, dass sich die Schlüssel der Terminal-Authentisierung mit jedem neuen Berechtigungszertifikat ändern, im Regelfall also beinahe täglich im Kryptographiemodul aktualisiert werden müssen. Der Zertifikats-Request für das nächste Berechtigungszertifikat muss im Kryptographiemodul mit dem privaten Schlüssel des aktuellen Zertifikats signiert werden. Als Kryptographiemodul ist der Einsatz von Signaturkarten oder High Security Modules (HSM) zulässig, die gemäß der Schutzprofile [PP-Sig] bzw. [PP-CM] nach den Common Criteria mit Prüftiefe EAL4+ zertifiziert sind. Im Einzelfall kann aber auf Antrag des Diensteanbieters das BSI einer Ausnahme von dieser Regelung zustimmen.

7. Sicherheitsmaßnahmen im Überblick

Die folgende Tabelle fasst die wichtigsten Anforderungen und Sicherheitsmaßnahmen zusammen. In der Spalte "Sicherheitsmaßnahmen bei Nutzung eID-Service" sind die Maßnahmen, welche direkt vom Betreiber des eID-Service übernommen werden, mit einem Stern (*) gekennzeichnet.

Sicherheitsfokus	Sicherheitsanforderung	Maßnahmen bei Nutzung eines eID-Service	Maßnahmen bei Nutzung eines eigenen eID-Servers
1. Sicherheitskonzept des Diensteanbieters (Kap. 5.1 und 6.1)	Nachweisbarkeit von Sicherheitsmaßnahmen gegenüber VfB	- Laufend aktualisiertes Sicherheitskonzept unter Einbezug des eID-Service	- Laufend aktualisiertes Sicherheitskonzept gemäß [BSI-100-2, -3, -4] - Grundschutz-Zertifizierung nach [ISO-27001] empfohlen
2. Komponente Web-Server (Kap. 5.2 und 6.2)	Schutz der Schlüssel und Zertifikate	- Sichere Betriebsumgebung gemäß Sicherheitskonzept - Einsatz von Kryptographie-modulen (HSM, Signaturkarten) empfohlen	- Sichere Betriebsumgebung gemäß Sicherheitskonzept - Einsatz von Kryptographie-modulen (HSM, Signaturkarten) empfohlen
3. Kommunikation zwischen Web-Server und Web-Browser (Kap. 5.3 und 6.3)	Aufbau einer autorisierten Kommunikationsverbindung	- TLS-Server-Authentisierung - Auf Anwendungsebene: Datenschutzerklärung + Berechtigungszertifikat	- TLS-Server-Authentisierung - Auf Anwendungsebene: Datenschutzerklärung + Berechtigungszertifikat
	Geschützte Kommunikation	- Halten der TLS-Verbindung solange Nutzer authentisiert ist - Auf Anwendungsebene: HTTPS	- Halten der TLS-Verbindung solange Nutzer authentisiert ist - Auf Anwendungsebene: HTTPS
4. Kommunikation zwischen Web-Server und eID-Server (Kap. 5.4 und 6.4)	Aufbau einer autorisierten Kommunikationsverbindung	- TLS oder VPN mit gegenseitiger Authentisierung auf Basis einer Registrierung - Auf Anwendungsebene: Vorab gesicherter Austausch der Tokenzertifikate	- Eindeutige Identifizierung/ Authentisierung von Sender und Empfänger in der internen Netzstruktur - Auf Anwendungsebene: Vorab gesicherter Austausch der Tokenzertifikate
	Geschützte Kommunikation	- TLS oder VPN mit Verschlüsselung - Auf Anwendungsebene: Signierte SOAP-Nachrichten oder signierte SAML-Token mit Verschlüsselung	- Verschlüsselung optional - Auf Anwendungsebene: Signierte SOAP-Nachrichten oder signierte SAML-Token mit Verschlüsselung
5. Kommunikation zwischen eID-Server und AusweisApp bzw. Web-Browser (Kap. 5.5 und 6.5)	Aufbau einer autorisierten Kommunikationsverbindung	- *) TLS-Server-Authentisierung	- TLS-Server-Authentisierung
	Geschützte Kommunikation	- *) TLS mit Verschlüsselung - *) Auf Anwendungsebene: nPA-Sicherheitsprotokolle, HTTPS bzw. HTTPS-Redirect	- TLS mit Verschlüsselung - Auf Anwendungsebene: nPA-Sicherheitsprotokolle, HTTPS bzw. HTTPS-Redirect
6. Kommunikation zwischen eID-Server und Infrastruktur-diensten (Kap. 5.6 und 6.6)	Aufbau einer autorisierten Kommunikationsverbindung	- *) TLS mit gegenseitiger Authentisierung auf Basis einer Registrierung	- TLS mit gegenseitiger Authentisierung auf Basis einer Registrierung
	Geschützte Kommunikation	- *) TLS mit Verschlüsselung	- TLS mit Verschlüsselung
7. Komponente eID-Server (Kap. 5.7 und 6.7)	Einsatz zertifizierter Produkte	- *) Konformitätsprüfung des BSI	- Konformitätsprüfung des BSI
	Schutz der Schlüssel und Zertifikate	- *) Sichere Betriebsumgebung gemäß Sicherheitskonzept - *) Einsatz von Kryptographie-modulen (HSM, Chipkarten), zertifiziert nach [PP-Sig] bzw.	- Sichere Betriebsumgebung gemäß Sicherheitskonzept - Einsatz von Kryptographie-modulen (HSM, Chipkarten), zertifiziert nach [PP-Sig] bzw.

Sicherheitsfokus	Sicherheitsanforderung	Maßnahmen bei Nutzung eines eID-Service	Maßnahmen bei Nutzung eines eigenen eID-Servers
		[PP-CM] auf EAL4+	[PP-CM] auf EAL4+
	Eindeutige Zuordnung gültiger Berechtigungszertifikate zu Diensteanbietern	- *) TLS-Server-Authentisierung - *) Auf Anwendungsebene: Berechtigungszertifikat mit TLS-Hashes + PSK - *) Mandantenfähigkeit des eID-Servers	- TLS-Server-Authentisierung - Auf Anwendungsebene: Berechtigungszertifikat mit TLS-Hashes + PSK
	Zuverlässige Zuordnung der Teilprozesse	- *) Mechanismen für Kanalbindung z.B. über PSK	- Mechanismen für Kanalbindung z.B. über PSK
	Nachvollziehbarkeit d. Verwendung von Zertifikaten	- *) Revisionssichere Protokollierung	- Revisionssichere Protokollierung
	Sicherer Umgang mit den eID-Ergebnisdaten	- *) Mandantenfähigkeit - *) Erheben, Speichern, Weitergeben und Löschen der eID-Daten gemäß Zweckbindung	- Erheben, Speichern, Weitergeben und Löschen der eID-Daten gemäß Zweckbindung

8. Konsequenzen für den Diensteanbieter bei Nichtbeachtung

Auf einen Blick

- Das Berechtigungszertifikat kann durch die VfB entzogen werden.
- Technische Berechtigungszertifikate habe nur eine Laufzeit von zwei Tagen.
- Verstoß gegen die Verpflichtungen der Diensteanbieter kann zu einem Bußgeldverfahren führen.

Die VfB kann die Berechtigung des Dienstanbieters, eID-Daten aus dem Personalausweis zu lesen, wieder entziehen, wenn sich z.B. herausstellt, dass die im Personalausweisgesetz genannten Voraussetzungen (vgl. §21 PAuswG) tatsächlich gar nicht erfüllt sind oder die Angaben des Diensteanbieters bei der Beantragung unrichtig oder unvollständig waren.

Die VfB wird aufgrund einer Beanstandung der datenschutzrechtlichen Aufsichtsbehörde die erteilte Berechtigung zurücknehmen, wenn der Diensteanbieter sich nicht an die Vorgaben hält und beispielsweise:

- eID-Daten geschäftsmäßig oder unberechtigt an Dritte übermittelt,
- seine Berechtigung z.B. durch eine unzulässige Verarbeitung oder Nutzung von eID-Daten missbräuchlich verwendet, oder
- notwendige Maßnahmen zu Datenschutz und Datensicherheit nicht erfüllt.

Bei Entzug der Berechtigung ist der Diensteanbieter dazu verpflichtet, vorhandene Berechtigungszertifikate nicht mehr zu verwenden und muss bei einem Verstoß gegen diese und andere Verpflichtungen zudem mit einem Bußgeldverfahren rechnen (vgl. §32 und §33 PAuswG). Die Aufhebung der Berechtigung hat auch bei einem Rechtsstreit keine aufschiebende Wirkung (vgl. §30 PAuswG) und kann, da die Zertifikate in der Regel eine kurze Laufzeit von 2 Tagen besitzen, technisch sehr schnell durch Nicht-Ausstellen der Folgezertifikate erreicht werden.

9. Links

Die Technischen Richtlinien zum neuen Personalausweis stehen auf der Webseite des BSI unter: www.bsi.bund.de -> Publikationen -> Technische Richtlinien.

Die Dokumente zum IT-Grundschutz sind erhältlich unter www.bsi.bund.de -> IT-Grundschutz.

10. Referenzen

[BSI-100-2]	BSI: Standard 100-2: IT-Grundschutz-Vorgehensweise
[BSI-100-3]	BSI: Standard 100-3: Risikoanalyse auf der Basis von IT-Grundschutz
[BSI-100-4]	BSI: Standard 100-4: Notfallmanagement
[CP-eID]	Certificate Policy für die eID-Anwendung des ePA
[ISO-27001]	ISO/IEC 27001: Information technology – Security techniques – Information security management systems – Requirements
[PP-AA]	BSI: Common Criteria Protection Profile ...
[PP-CM]	BSI: Common Criteria Protection Profile Cryptographic Modules, Security Level “Moderate”, Version 1.01, 2008, BSI-PP-0042
[PP-eID]	BSI: Common Criteria Protection Profile Electronic Identity Card, Version 1.03, 2009, BSI-PP-0061
[PP-Sig]	CEN/TC 224: prEN 14169-1, Protection Profiles for Secure Signature Creation Device – Part 2: Device with Key Generation, Version 1.03, 2009, BSI-PP-0059
[SAML]	OASIS: Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0
[TR-3112]	BSI: Technische Richtlinie TR-03112, eCard-API-Framework
[TR-3127]	BSI: Technische Richtlinie TR-03127: Architektur Elektronischer Personalausweis
[TR-3128]	BSI: Technische Richtlinie TR-03128: EAC-PKI'n für den elektronischen Personalausweis
[TR-3129]	BSI: Technische Richtlinie TR-03129 PKIs for Machine Readable Travel Documents
[TR-3130]	BSI: Technische Richtlinie TR-03130 Technische Richtlinie eID-Server

11. Informationen

Das Bundesministerium des Innern hat unter www.personalausweisportal.de ein Informations- und Serviceportal zum neuen Personalausweis eingerichtet. Hier können sich Bürgerinnen und Bürger, Firmen und Verwaltungen umfassend über den neuen Ausweis informieren. Das Portal gibt Auskünfte zu den neuen Funktionen, zur Handhabung und zum Schutz der persönlichen Daten.

Die AusweisApp wird vom Bundesministerium des Innern kostenlos bereitgestellt und kann von der Webseite der AusweisApp www.ausweisapp.bund.de heruntergeladen werden. Ebenfalls findet man hier geeignete Kartenleser.

Das Bundesministerium des Innern hat ein „Kompetenzzentrum neuer Personalausweis“ eingerichtet, siehe auch www.ccepa.de. Hier finden Bürger weitere Informationen über den Personalausweis, verfügbare Kartenleser und Erläuterungen zum Thema Sicherheit. Das Test- und Demonstrationszentrum (TDZ) im Fraunhofer FOKUS stellt dabei den Kernbereich des Kompetenzzentrums neuer Personalausweis dar.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) stellt auf seinen Webseiten „BSI für Bürger“ unter www.bsi-fuer-buerger.de vielfältige Informationen rund um die Sicherheit für Heim-PCs, das Internet und den neuen Personalausweis zur Verfügung. Die technischen Richtlinien werden unter www.bsi.de zur Verfügung gestellt.

Bei allen Fragen zum Personalausweis steht auch der Bürgerservice zur Verfügung:

Bürgerservice (Servicezeiten Mo – Fr, 7.00 – 20.00 Uhr)
Telefon: 0180-1-33 33 33
(3,9 ct/Min dt. Festnetz, max. 42 ct/Min Mobilnetz)