Bundesamt
für Sicherheit in der
Informationstechnik

Innovationen für eine eID-Architektur in Deutschland

www.bsi.bund.de

Das **Bundesamt für Sicherheit in der Informationstechnik (BSI)** ist der zentrale IT-Sicherheitsdienstleister Deutschlands: eine unabhängige neutrale Stelle für Fragen zur IT-Sicherheit in der Informationsgesellschaft. Das BSI informiert über Risiken und Gefahren beim Einsatz von Informations- und Kommunikationstechnik, entwickelt Sicherheitsrichtlinien und berät Hersteller, Vertreiber und Anwender. In erster Linie wendet sich das BSI an öffentliche Verwaltungen in Bund, Ländern und Kommunen, sucht aber auch den Informationsaustausch mit Unternehmen und Privatanwendern.

Inhalt

1. Der neue Personalausweis – sicherer Standard-Identitätsnachweis in der Onlinewelt

Der neue Personalausweis wird ab 1. November 2010 in Deutschland als elektronische Multifunktionskarte im Scheckkartenformat eingeführt, die sowohl für den Reiseverkehr und die Personenkontrolle als auch für die elektronische Welt gilt. Dabei wird ein innovatives Konzept realisiert, das auf einer kontaktlosen Schnittstelle basiert, wie sie bereits weltweit für den elektronischen Reisepass verwendet wird.

Der neue Personalausweis wird nicht nur ein modernes hoheitliches Dokument darstellen, das das Identifizieren von Personen, z. B. an Grenzkontrollen, deutlich verbessert. Der Ausweis wird mit zusätzlichen elektronischen Funktionalitäten, insbesondere dem elektronischen Identitätsnachweis (eID) und der zusätzlich aktivierbaren Qualifizierten Elektronischen Signatur (QES) ausgestattet sein, die erhebliche Vorteile für die Nutzer bieten. Diese Funktionalitäten ermöglichen die eindeutige Identifikation im Internet und die Abgabe von rechtsverbindlichen elektronischen Willenserklärungen. Sie sind damit Schlüsselinstrumente für rechtswirksame Transaktionen und Vertragsabschlüsse im Internet und sollen durchgängige E-Government- und E-Business-Dienstleistungen entscheidend fördern.

Die Einführung der Identifikationsfunktion des neuen Personalausweises ist Anlass für die Vorbereitung, Entwicklung und Einführung einer komplexen IT-Infrastruktur und ihre Einbettung in ein komplexes Gesamtsystem mit mehr als 60 Mio. Beteiligten. Dafür mussten zunächst entsprechende organisatorische, gesetzliche und technische Voraussetzungen geschaffen werden. Das Gesetz über Personalausweise

und den elektronischen Identitätsnachweis (Personalausweisgesetz) definiert den allgemeinen Rechtsrahmen [PAuswG 2010] und in der Verordnung über Personalausweise und den elektronischen Identitätsnachweis (Personalausweisverordnung) werden insbesondere auch die Vorgaben für die Sicherheit und den Datenschutz der eID-Infrastruktur definiert [PAuswV 2010]. Dazu kommen fast 20 Technische Richtlinien und Protection Profils des Bundesamtes für Sicherheit in der Informationstechnik (BSI), die verbindlich im Bundesanzeiger veröffentlicht werden. Beispielhaft werden in dieser Broschüre einige dieser Vorgaben erläutert.

Mit der Infrastruktur des neuen Personalausweises soll ein vertrauenswürdiges und effizientes Identity Management realisiert werden. Durch die Kombination eines hoheitlichen Ausweisdokuments mit der eID-Funktionalität für E-Business und E-Government können die Nutzer auch in der elektronischen Welt über eine sichere Identität verfügen und sollen vor vielen Arten der Cyberkriminalität, wie Phishing und Identitätsdiebstahl, besser geschützt werden.

Auf Datenschutz, Datensicherheit und die Wahrung der informationellen Selbstbestimmung wird besonderer Wert gelegt. Alle Informationen und Übertragungen werden mit international anerkannten und etablierten Verschlüsselungsverfahren sicher geschützt. Im Rahmen der eID-Funktion werden die Nutzerdaten ausschließlich zwischen dem Anbieter des Dienstes und dem Ausweisinhaber ausgetauscht.

Biometrisch nutzbare Daten, also Lichtbild, ggf. Fingerabdrücke, Augenfarbe, Körpergröße und die eigenhändige Unterschrift, werden in keinem Falle an Diensteanbieter oder über das Internet übertragen. Nur hoheitliche Stellen verfügen über die Berechtigung und die technische Möglichkeit, diese sensiblen Informationen abzufragen.

2. Nutzerorientierte Anforderungen an die Identifikationsfunktion des neuen Personalausweises

Als Schutzfunktion für die auf dem Ausweischip gespeicherten personenbezogenen Daten ist vorgeschrieben, dass alle Institutionen, die auf diese Daten vollständig oder teilweise zugreifen wollen, über eine Berechtigung verfügen müssen. Vor der Vergabe einer solchen Berechtigung wird staatlich geprüft, welche Daten der Diensteanbieter (z.B. Online-Shops oder auch Behörden) für seine Zwecke unbedingt benötigt und ob er vertrauenswürdig ist. Die Berechtigung ist immer nur für einen bestimmten Zeitraum gültig und kann auch wieder entzogen werden. Technisch wird die Berechtigung durch so genannte Berechtigungszertifikate umgesetzt, deren Status bei der Terminal Authentication abgefragt wird.

Bevor der neue Personalausweis Daten für einen Diensteanbieter mit Berechtigungszertifikat freigibt, muss der Diensteanbieter sein Zertifikat und damit auch die Daten, die er lesen darf, anzeigen. Der Ausweisinhaber hat immer noch die Möglichkeit, die Leseberechtigung auf weniger Daten einzuschränken.

Anschließend muss der Ausweisinhaber noch die sechsstellige persönliche Geheimnummer (PIN) eingeben. Sofern die elektronische Prüfung des Berechtigungszertifikats positiv verläuft, werden die Daten freigegeben. Alle Daten werden verschlüsselt übertragen.

Die Leseberechtigung kann auch soweit eingeschränkt werden, dass z.B. nur über das Alter Auskunft erlangt werden kann. Des Weiteren gibt es eine Pseudonym-Funktion, über die es möglich ist, sich mit seinem Personalausweis

bei einem Diensteanbieter – z.B. in einem Internet-Forum – anzumelden und wiedererkannt zu werden, ohne dass der Diensteanbieter personenbezogene Daten erhält. Diese Funktion ist karten- und dienstespezifisch, das heißt, dass Diensteanbieter, die ihre Datenbanken abgleichen, nicht feststellen können, ob sich hinter den bei Ihnen gespeicherten Pseudonymen dieselbe Person verbirgt.

Bei Verlust des neuen Personalausweises kann die eID-Anwendung mit einem persönlichen Kennwort gesperrt werden (siehe Kapitel 6). Wird die persönliche Geheimnummer dreimal falsch eingegeben, muss sie durch eine PIN Unblocking Key (PUK) reaktiviert werden.

Auf Wunsch kann die eID-Anwendung auf dem Ausweis durch die Ausweisbehörde abgeschaltet werden.

Zusätzlich kann auf dem neuen Personalausweis auch die Funktion einer Qualifizierten Elektronischen Signatur freigeschaltet werden. Eine solche Signatur ermöglicht auf elektronischem Wege die Erfüllung der Schriftformerfordernis im Vertragsrecht. Die für dieses Verfahren erforderlichen elektronischen Zertifikate können bei Anbietern aus der Wirtschaft erworben werden.

3. Anwendungssoftware für den Nutzer – AusweisApp

Damit die Bürger ihren neuen Personalausweis im Internet nutzen können, benötigen sie eine Software, die als Schnittstelle zwischen Ausweis, Kartenlesegerät und eID-Server des Diensteanbieters fungiert. Eine solche Software – sie trägt den Namen „AusweisApp“ – wird dem Bürger für die Betriebssysteme Windows, Linux und Mac OS über ein Webportal vom Bundesministerium des Innern kostenlos zur Verfügung gestellt. Dieses Webportal ist unter der Internetadresse https://www.ausweisapp.bund.de zu erreichen.

Neben der Nutzung der Identitätsfunktion des neuen Personalausweises ermöglicht die AusweisApp auch das qualifizierte elektronische Signieren mit verschiedenen Signaturkarten sowohl mit herkömmlichen, kontaktbehafteten als auch mit kontaktlosen wie dem neuen Personalausweis. Auch Funktionen der deutschen Gesundheitskarte werden unterstützt.

Die AusweisApp ist eine Implementierung der Technischen Richtlinie eCard-API-Framework, in welchem einfach zu nutzende, einheitliche Schnittstellen für die Kommunikation von Kartenlesern, Karten und Anwendungen (webbasiert oder lokal) definiert sind [TR-03112].

4. Sicherheitsmechanismen für die Identifikationsfunktion des neuen Personalausweises

Mit den Sicherheitsmechanismen und den daraus abgeleiteten IT-Infrastrukturen für den neuen Personalausweis lassen sich sowohl der Schutz personenbezogener Daten, der Nachweis der Authentizität des Ausweises sowie seine Fälschungssicherheit gewährleisten.

Ein besonderes Gewicht haben dabei Lösungen, die auf die Absicherung der kontaktlosen Schnittstelle zwischen Ausweis und Terminal gerichtet sind. Denn diese muss u.a. den Anforderungen an Qualifizierte Elektronische Signaturen genügen.

Im Folgenden werden Protokolle und andere Maßnahmen vorgestellt, die unter maßgeblicher Beteiligung des BSI entwickelt wurden, um die oben genannten Sicherheitsziele zu erreichen:

Kurzform	Titel	Zweck
PACE	Password Authenticated Connection Establishment	Zugriffskontrolle, schützt vor Auslesen des RF-Chips auf Entfernung
EAC	Extended Access Control	Erweiterte Zugangskontrolle bestehend aus zwei Subprotokollen
	CA: Chip Authentication	Aufbau einer gesicherten Verbindung und Erkennung „geklonter“ RF-Chips
	TA: Terminal Authentication	Authentisierung des Lesegerätes zum Auslesen sensibler Daten vom RF-Chip
PA	Passive Authentication	Prüfung der Echtheit und Unverfälschtheit der Daten auf dem RF-Chip

RI	Restricted Identification	Erzeugung von chip- und anbieterspezifischen Pseudonymen
PKI	Public Key Infrastructure	Hierarchie von digitalen Zertifikaten
	CSCA: Country Signing Certificate Authority	Hierarchie von digitalen Zertifikaten zur Signierung von Daten in elektronischen Ausweisdokumenten
	CVCA: Country Verifying Certificate Authority	Hierarchie von digitalen Zertifikaten zur Leseberechtigung bei elektronischen Ausweisdokumenten

4.1 Password Authenticated Connection Establishment (PACE)

Password Authenticated Connection Establishment (PACE) sorgt dafür, dass der kontaktlose RF-Chip im neuen Personalausweis nicht ohne direkten Zugriff ausgelesen werden kann und die mit dem Lesegerät ausgetauschten Daten verschlüsselt übertragen werden [Bender 2008].

Welches Passwort für PACE benutzt werden kann, hängt vom Berechtigungszertifikat des verwendeten Lesegerätes ab. Im Allgemeinen ist dies eine sechsstellige Personal Identification Number (PIN), die nur dem Ausweisinhaber bekannt ist.

Bei Lesegeräten mit Berechtigungszertifikaten für den hoheitlichen Einsatz, wie z.B. bei der Grenzkontrolle, ist entweder die auf der Rückseite des neuen Personalausweises aufgedruckte Machine Readable Zone (MRZ) oder die auf der Vorderseite aufgedruckte sechsstellige Card Access Number (CAN) ausreichend.

PACE hat den Vorteil, dass sich die Länge des Passwortes nicht auf das Sicherheitsniveau der Verschlüsselung auswirkt. Das heißt, auch bei der im Gegensatz zur MRZ kurzen CAN oder PIN sind die Daten auf dem RF-Chip des elektronischen Personalausweises und während der Übertragung stark geschützt.

4.2 Extended Access Control (EAC), Lesegeräte und EAC-Box

Extended Access Control (EAC) beinhaltet verschiedene Protokolle, die je nach dem welches elektronische Ausweisdokument gelesen werden soll, in einer bestimmten Reihenfolge durchgeführt werden [TR-03110].

Zu den EAC-Protokollen zählen Chip Authentication (CA) und Terminal Authentication (TA). Die beiden Protokolle werden zusammen mit Password Authenticated Connection Establishment (PACE) und Passive Authentication (PA) ausgeführt.

Die **Chip Authentication** dient zum einen dem Nachweis, dass es sich bei dem Chip um einen echten Chip (und nicht etwa um eine Fälschung oder einen Klon) handelt, zum anderen wird ein sicherer Kanal zwischen Chip und Lesegerät, bzw. Diensteanbieter bei der Online Authentication, aufgebaut.

Die Chip Authentication basiert auf dem Diffie-Hellman-Schlüsselaustausch, wobei das Lesegerät ein flüchtiges (ephemeral) Schlüsselpaar und der Chip ein statisches Paar nutzt. Der öffentliche Schlüssel des Chips wird während des Herstellungsprozesses signiert (Passive Authentication – siehe Kapitel 4.3).

Durch die Verwendung des signierten Schlüssels wird die Echtheit des Chips nachgewiesen, gleichzeitig wird ein stark

verschlüsselter und authentisierter Ende-zu-Ende-Kanal zwischen Chip und – im Falle der Online Authentication – Diensteanbieter aufgebaut.

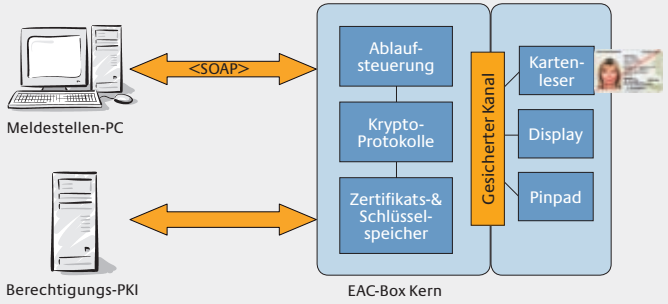
Alle Daten des neuen Personalausweises werden als sensibel behandelt und müssen vor dem Auslesen durch unbefugte Personen geschützt werden. Dafür wurde das Protokoll Terminal Authentication (TA) entwickelt. Die sensiblen Daten können nur gelesen werden, wenn dieses Protokoll erfolgreich am Lesegerät durchgeführt wurde. Der RF-Chip im Ausweisdokument ist so angelegt, dass er bestimmte Daten nur dann zum Lesen freigibt, wenn das Lesegerät eine explizite Leseberechtigung für genau diese Daten (z.B. nur das Geburtsdatum) nachweisen kann. Damit der RF-Chip diese Berechtigung prüfen kann, hat er das Country Verifier Certification Authority Certificate (CVCA-Zertifikat) gespeichert. Dieses Zertifikat bildet die Wurzel der Country Verifier Public Key Infrastructure (CV-PKI), einer Hierarchie für die Berechtigungszertifikate für das Lesen von sensiblen Daten auf Ausweisdokumenten.

Bei der **Terminal Authentication** schickt das Lesegerät seine Leseberechtigung in Form eines Terminal-Zertifikats an den RF-Chip. Zusätzlich schickt das Lesegerät das CVCA-Zertifikat und alle Zertifikate, die in der Zertifikats-Hierarchie zwischen diesen beiden Zertifikaten stehen, mit. Der RF-Chip kann damit die Echtheit und Unverfälschtheit des Terminal-Zertifikats kontrollieren. Für ein positives Ergebnis müssen alle in der Hierarchie nachfolgenden Zertifikate jeweils mit dem geheimen Schlüssel ihres Vorgängers signiert worden sein, beginnend mit dem CVCA-Zertifikat. Dieses ist für den RF-Chip vertrauenswürdig, da es schon bei der Herstellung auf dem RF-Chip gespeichert wird.

Wenn die Echtheit und Unverfälschtheit des vom Lesegerät gesendeten Terminal-Zertifikates feststeht, muss der RF-Chip noch sicherstellen, dass dieses Zertifikat auch wirklich für dieses Lesegerät ausgestellt wurde. Daher schickt der RF-Chip eine Zufallszahl an das Lesegerät, welches diese mit dem geheimen Schlüssel signiert, der zu dem Terminal-Zertifikat gehört. Dann sendet das Lesegerät die signierte Zufallszahl zurück an den RF-Chip. Mit dem öffentlichen Schlüssel des Lesegeräts, welcher im Terminal-Zertifikat enthalten ist, kann der RF-Chip die Signatur der Zufallszahl prüfen und damit feststellen, ob das Lesegerät den zum Zertifikat passenden geheimen Schlüssel besitzt.

Jedes Lesegerät, das auf die Daten des elektronischen Personalausweises zugreifen will, benötigt entsprechende Berechtigungszertifikate mit eigenen privaten und öffentlichen Schlüsseln, die regelmäßig über eine PKI erneuert werden müssen. Die **EAC-Box** stellt diese Funktionen gekapselt in einer evaluierten und zertifizierten Umgebung zur Verfügung und kommuniziert mit externen Komponenten und Diensten über standardisierte Schnittstellen [TR-03131].

EAC-Box
Kernkomponente im Änderungsdienst



Spezifikation: BSI Technische Richtlinie TR-03131 „EAC Box Architecture and Interfaces“
Schutzprofil: „CC Protection Profile for Inspection Systems“

Die EAC-Box wird zur Einführung des elektronischen Personalausweises als Lesegerät zur Änderung der Adressdaten auf dem ePA in den Meldestellen der Kommunen eingesetzt werden. Neben diesem Szenario sind auch weitere Einsatzgebiete denkbar (z. B. Grenzkontrolle).

4.3 Passive Authentication (PA)

Die Passive Authentication (PA) dient dazu, die Echtheit und Unverfälschtheit der Daten auf dem RF-Chip des Ausweisdokuments zu prüfen.

Bei der Herstellung eines elektronischen Ausweisdokuments werden die im RF-Chip gespeicherten Daten digital signiert. Dazu wird ein so genanntes Document Signing-Zertifikat verwendet, welches wiederum mit dem Country Signing Certificate Authority Certificate (CSCA-Zertifikat) der ausstellenden Nation signiert ist und nur dem offiziell beauftragten Ausweishersteller zur Verfügung steht. Dieses Zertifikat bildet die Wurzel der Country Signing Certificate Authority Public Key Infrastructure (CSCA-PKI), einer Hierarchie für die Zertifikate zum Nachweis der Unverfälschtheit von Daten auf Ausweisdokumenten.

Beim Lesen eines Ausweisdokumentes wird mittels der Passive Authentication die Signatur der im RF-Chip gespeicherten Daten geprüft und bis zum CSCA-Zertifikat zurückverfolgt. So kann festgestellt werden, ob die Daten im Ausweisdokument vom offiziell beauftragten Passhersteller im RF-Chip gespeichert wurden und ob diese unverfälscht sind.

4.4 Public Key Infrastructures (PKI) für elektronische Ausweisdokumente

Für den neuen Personalausweis werden zwei Public Key Infrastructures (PKI) benötigt: eine PKI für die Echtheitsprüfung von elektronischen Ausweisdokumenten (Passive Authentication), die Country Signing Certificate Authority (CSCA), und eine PKI für den Schutz der Fingerabdrücke auf den elektronischen Ausweisdokumenten (Terminal Authentication), die Country Verifying Certificate Authority (CVCA). Die Technische Richtlinie TR-03128 beschreibt die grundlegenden Funktionalitäten und Anforderungen an diese Infrastrukturen.

4.4.1 Country Signing Certificate Authority (CSCA)

Die Country Signing Certificate Authority (CSCA) wird vom BSI betrieben. Hier werden regelmäßig die deutschen Wurzelzertifikate (CSCA-Zertifikate) erstellt, mit deren privaten Schlüsseln die Document Signing-Zertifikate des Pass- bzw. Ausweisherstellers signiert werden. Der Pass- bzw. Ausweishersteller nutzt die privaten Schlüssel der Document Signing-Zertifikate, um damit Dateien im elektronischen Ausweisdokument zu signieren, welche die Daten des Ausweisdokuments repräsentieren. Das Document Signing-Zertifikat wird ebenfalls elektronisch im Ausweisdokument gespeichert.

Mit Hilfe des Wurzelzertifikats kann nun überprüft werden, ob ein elektronisches Ausweisdokument wirklich im Auftrag der ausstellenden Nation hergestellt wurde, und ob die Daten seit der Produktion in irgendeiner Weise verändert wurden. Dies geschieht mit Hilfe der Passive Authentication.

Damit bei den Grenzkontrollen in anderen Ländern die Echtheit und Unverfälschtheit der deutschen elektronischen Ausweisdokumente festgestellt werden kann, bzw. an deutschen

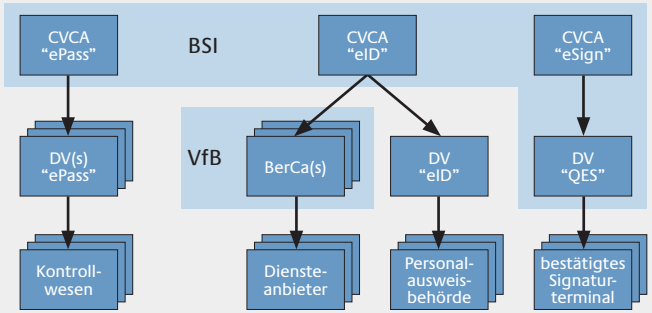
Grenzen auch die elektronischen Pässe anderer Nationen auf ihre Echtheit und Unverfälschtheit geprüft werden können, müssen die verschieden Nationen ihre Wurzelzertifikate auf sichere Art und Weise austauschen. Dies geschieht entweder über den diplomatischen Austausch oder über das ICAO Public Key Directory (ICAO-PKD).

4.4.2 Country Verifying Certificate Authority (CVCA)

Die Country Verifying Certificate Authority (CVCA) wird ebenfalls vom BSI betrieben. Hier werden regelmäßig die deutschen Wurzelzertifikate erstellt, mit deren privaten Schlüsseln die Document Verifier-Zertifikate der Document Verifier Instances (DV-Instanzen) signiert werden.

Die DV-Instanzen sind dafür zuständig, die Berechtigungszertifikate für das Lesen von elektronischen Ausweisdokumenten auszugeben. Dabei werden auch die individuellen Leserechte, d.h. welche Informationen aus den Ausweisdokumenten gelesen werden dürfen, festgelegt. Diese Berechtigung wird beim Leseprozess vom RF-Chip

CVCA Public Key Infrastructure
für Bürgeranwendungen des neuen Personalausweises



CVCA - Country Verifying Certification Authority
DV - Document Verifier
BerCA - Berechtigungs Certification Authority
VfB - Vergabestelle für Berechtigungszertifikate
QES - Qualifizierte elektronische Signatur

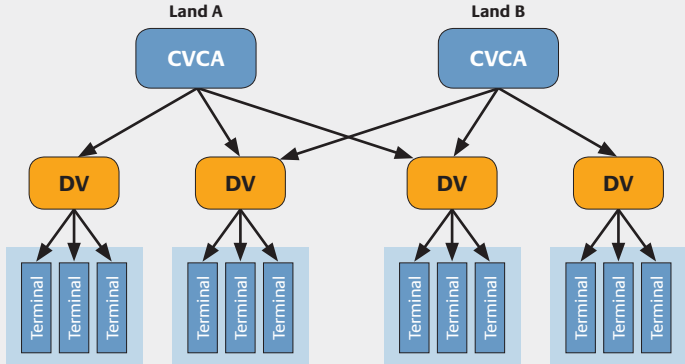
des elektronischen Ausweisdokuments bei der Terminal Authentication geprüft.

Für den neuen Personalausweis erhalten nur Kontrollbehörden (z.B. Bundespolizei) und Meldebehörden (für die Kontrolle der Richtigkeit der Daten durch den Bürger) Berechtigungszertifikate. Diese werden auch für das Auslesen von Fingerabdrücken benötigt.

Das Spektrum der Varianten von nationalen Berechtigungszertifikaten für den neuen Personalausweis zeigt die Graphik „CVCA Public Key Infrastructure für Bürgeranwendungen des neuen Personalausweises“. Neben den Anwendungen für hoheitliche Zwecke und für die elektronische Identifikation wird auch die Qualifizierte Elektronische Signatur von der CVCA unterstützt.

Des Weiteren müssen beim neuen Personalausweis Berechtigungszertifikate für die Kontrollbehörden anderer Nationen ausgestellt werden, welche berechtigt sind auf die hoheitliche Funktion im neuen Personalausweis zuzugreifen. Diese Berechtigung wird für jede Nation separat erteilt.

CVCA Public Key Infrastructure
im internationalen Kontext



Zusammenfassend wird durch die beschriebenen kryptografischen Protokolle Schutz vor verschiedenen Angriffen erreicht:

- PACE hat den Vorteil, dass sich die Länge des Passwortes nicht auf das Sicherheitsniveau der Verschlüsselung auswirkt. Das heißt, auch bei der im Gegensatz zur MRZ kurzen CAN oder PIN sind die Daten auf dem RF-Chip des neuen Personalausweises und während der Übertragung stark geschützt.
- PACE schützt vor Zugriff „im Vorbeigehen“ und baut einen verschlüsselten integritätsgesicherten Kanal zwischen Karte und Lesegerät auf.
- PACE ermöglicht zusätzlich die Eingabe/Verifikation einer PIN, dadurch Bindung der Authentisierung an die Person und Schutz vor unbefugter Nutzung des neuen Personalausweises.
- Die Terminal Authentication stellt sicher, dass das Lesegerät/der Diensteanbieter nur berechtigte Zugriffe durchführen kann. Die Leserechte können für die verschiedenen Datenfelder separat vergeben werden.
- Die Chip Authentication baut einen sicheren Ende-zu-Ende-Kanal zwischen Chip und Diensteanbieter auf. Weiter wird durch die Chip Authentication in Verbindung mit der Passive Authentication die Echtheit des Chips nachgewiesen.
- Die Integrität und Authentizität der ausgelesenen Daten wird implizit über den Echtheitsnachweis des Chips gesichert.

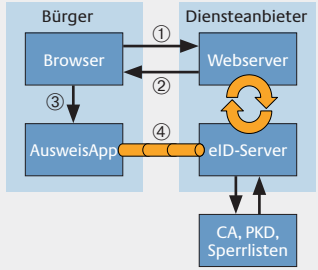
5. Schnittstelle für Web-Anwendungen – eID-Server

Um die Nutzung der elektronischen Identitätsfunktion in Web-Anwendungen zu vereinfachen, ist ein eID-Server erforderlich. Der eID-Server stellt eine einfache Schnittstelle für Web-Anwendungen bereit, um die Komplexität der elektronischen Identitätsfunktion zu kapseln. Die Richtlinie [TR-03130] spezifiziert die Schnittstelle, die durch Web-Anwendungen genutzt wird, und die entsprechenden Datenformate für den Austausch der Informationen.

Der eID-Server als Hardware- und Softwarekomponente stellt die Kommunikation zur AusweisApp her und übernimmt die Kommunikation zum Abruf von Terminal-Berechtigungszertifikaten (DVCA-Zertifikate), Sperrlisten und CSCA-Zertifikaten.

Der eID-Server wird als logisch eigenständiger Server realisiert, so dass er von mehreren Web-Anwendungen (Mandanten) genutzt und auch z.B. bei einem Dritten entfernt betrieben werden kann. Zur Wahrung der Vertraulichkeit und

eID-Server
Ablauf des elektronischen Identitätsnachweises



① Der Bürger wählt beim Dienstanbieter die Authentisierung mit Hilfe des elektronischen Identitätnachweises (eID).

② Der Webserver des Diensteanbieters übermittelt die für den Aufbau der Verbindung notwendigen Parameter.

③ Der Browser ruft die lokale AusweisApp auf.

④ Die AusweisApp baut einen sicheren Kanal zum eID-Server des Diensteanbieters auf und die Authentisierung beginnt.

CA - Certification Authority
PKD - Public Key Directory

Integrität der verarbeiteten Daten müssen die Daten bei der Übertragung zwischen eID-Server und Anwendungsserver verschlüsselt und signiert werden, wenn sie über ein offenes Netz übertragen werden.

6. Das Sperrmanagement im neuen deutschen Personalausweis

Um die missbräuchliche Nutzung gestohlener oder verloren gegangener Personalausweise zu verhindern, müssen diese vom Ausweisinhaber über ein Sperrmanagement gesperrt werden können [Bender 2010].

Üblicherweise werden heutige Chipkarten, wie z.B. Karten für die Qualifizierte Elektronische Signatur, über einen chip-individuellen öffentlichen Schlüssel gesperrt, der über eine Sperrliste abgeglichen werden kann, also über ein globales chipindividuelles Merkmal. Ein chipindividuelles Merkmal ist aber immer personenbezogen, da es den Chip und damit auch den Inhaber eindeutig identifiziert.

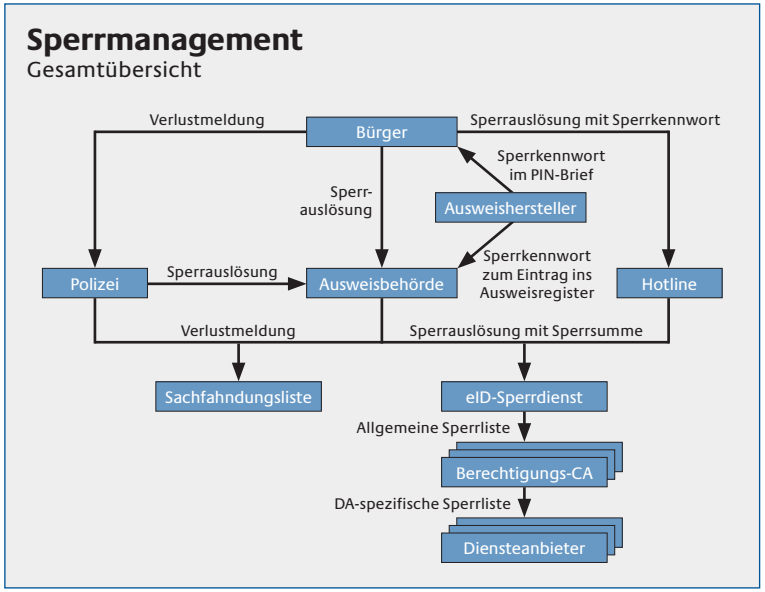
Solch ein Mechanismus stünde damit im Widerspruch zu der datenschutzfreundlichen Ausgestaltung der eID-Funktion, bei der nur diejenigen Daten aus dem Chip übermittelt werden, die für den Dienst benötigt werden. Beispielsweise darf ein Online-Dienst, der lediglich eine Altersverifikation für altersbeschränkte Dienstleistungen benötigt, seine aus dem Ausweis ausgelesenen Daten nicht über ein eindeutiges Sperrmerkmal mit einem Dienst abgleichen können, der Name, Adresse u.ä. Daten aus dem Ausweis erhält (dies gilt im besonderen Maße auch für das Pseudonym).

Eine Lösung dieses Widerspruchs ist die Verwendung von dienstespezifischen Sperrlisten, d.h. jeder Ausweis über-

sendet während des elektronischen Identitätsnachweises ein dienste- und kartenspezifisches Sperrmerkmal an den Diensteanbieter, den dieser gegen seine individuelle, d.h. dienstespezifische Sperrliste abgleicht.

Für jeden Dienst, der die eID-Funktion des neuen Personalausweises nutzt, wird aus einer globalen Sperrliste eine dienstespezifische Sperrliste erzeugt. Ein dienste- und kartenspezifisches Merkmal, das während der Nutzung der eID-Funktion vom Chip des Ausweises an den Diensteanbieter gesendet wird, kann dann mit den Merkmalen aus dieser spezifischen Sperrliste abgeglichen werden, um gesperrte Ausweise als solche erkennen zu können.

Durch die Benutzung von dienste- und kartenspezifischen Sperrmerkmalen ist es Diensteanbietern nicht möglich, aus den von Personalausweisen übermittelten Sperrmerkmalen diensteübergreifend Personalausweise wiederzuerkennen. Ähnliches gilt für den Sperrdienst, auch diese zentrale Stelle



kann ohne Mithilfe der Diensteanbieter und Berechtigungs-CAs nicht vom Sperrschlüssel auf die dienste- und kartenspezifischen Sperrmerkmale eines Personalausweises schließen – ein Nachverfolgen von Personalausweisen über den Sperrmechanismus ist somit nicht möglich.

Ebenfalls positiv im Sinne des Datenschutzes ist die Verwendung von Sperrkennwort und Sperrsumme.

Für die Erzeugung der dienstespezifischen Sperrlisten wird ein Sperrschlüssel benötigt. Um die oben beschriebene Sicherheit des Verfahrens gewährleisten zu können, hat dieser Schlüssel eine Länge von 256 Bit und kann damit sicherlich vom Personalausweisinhaber nicht auswendig behalten werden.

Eine Sperrung von abhanden gekommenen Personalausweisen muss jederzeit, d.h. sieben Tage die Woche, 24 Stunden täglich und vor allem auch unterwegs möglich sein. Eine Lösung wäre, beim Sperrdienst neben dem Sperrschlüssel auch die für die Identifizierung notwendigen personengebundenen Daten des Inhabers zu speichern, was de facto einem zentralen Bundesmelderegister entspräche.

Das im Personalausweis zum Einsatz kommende Verfahren geht einen anderen Weg, es wird lediglich der Hashwert (die Sperrsumme) über Name, Vorname, Geburtsdatum und dem Sperrkennwort zusammen mit dem Sperrschlüssel gespeichert.

Diese Umsetzung erlaubt eine effektive Sperrung von Personalausweisen ohne ein zentrales Register, in dem personengebundene Daten gespeichert werden müssten.

7. Referenzen

[PAuswG 2010] *Gesetz über Personalausweise und den elektronischen Identitätsnachweis* (Personalausweisgesetz – PAuswG), 17. August 2010, Bundesgesetzblatt I, S. 1346

[PAuswV 2010] *Verordnung über Personalausweise und den elektronischen Identitätsnachweis* (Personalausweisverordnung – PAuswV), 2010, Bundesgesetzblatt I

[Bender 2008] Jens Bender, Dennis Kügler, Marian Margraf, Ingo Naumann, *Sicherheitsmechanismen für kontaktlose Chips im deutschen elektronischen Personalausweis*, DuD • Datenschutz und Datensicherheit 3 | 2008, S. 173-177

[Bender 2010] Jens Bender, Dennis Kügler, Marian Margraf, Ingo Naumann, *Das Sperrmanagement im neuen deutschen Personalausweis*, DuD • Datenschutz und Datensicherheit 5 | 2010, S. 295-298

[TR-03110] Technische Richtlinie des BSI, *Advanced Security Mechanisms for Machine Readable Travel Documents* (BSI TR-03110)

[TR-03112] Technische Richtlinie des BSI, *eCard-API-Framework* (BSI TR-03112)

[TR-03128] Technische Richtlinie des BSI, *EAC-PKI'n für den elektronischen Personalausweis, Rahmenkonzept für den Aufbau und den Betrieb von Document Verifiern* (BSI TR-03128)

[TR-03130] Technische Richtlinie des BSI, *eID-Server* (BSI TR-03130)

[TR-03131] Technische Richtlinie des BSI, *EAC-Box Architektur und Schnittstellen* (BSI TR-03131)

Herausgeber
Bundesamt für Sicherheit
in der Informationstechnik (BSI)
Godesberger Allee 185 - 189
53175 Bonn

Stand
September 2010

Redaktion
TeleTrusT Deutschland e.V.,
Berlin

Gestaltung / Produktion
Kesberg Consulting,
Bonn

Druck
Buersche Druckerei Neufang KG,
Gelsenkirchen

Foto / Bildnachweis
Bundesministerium des Innern
(Titelbilder), Bundesamt für Sicherheit
in der Informationstechnik (Grafiken)