Der neue Personalausweis
Meine wichtigste Karte.

Die Technik des neuen Personalausweises

Auf einen Blick

- Kontaktloser Chip
- International etablierte Sicherheitsstandards
- Datensicherheit, Zugriffsschutz und Authentizität durch PACE, EAC und sichere Verschlüsselungsverfahren
- Datenschutzfreundliches Sperrmanagement

Neue technische Möglichkeiten

Drei neue Funktionen unterstützt der am 1. November 2010 eingeführte neue Personalausweis. Der integrierte kontaktlose Chip schafft die Grundlage für die Nutzung des Identitätsdokuments auch in der digitalen Welt:

Die hoheitliche Funktion erlaubt ausschließlich Behörden wie Polizei und Zoll das auf dem Chip abgelegte digitale Gesichtsbild und die nur dort optional abgelegten Fingerabdrücke auszulesen.

Die Online-Ausweisfunktion macht die sichere gegenseitige Authentisierung zweier Kommunikationspartner online und an Automaten möglich.

Die Unterschriftsfunktion ermöglicht das elektronische Unterschreiben von Dokumenten mit einer qualifizierten elektronischen Signatur (QES), die nachträglich erworben und auf den Chip geladen werden kann.

Komponenten für die Online-Ausweisfunktion

Bei der gegenseitigen Authentisierung mit der Online-Ausweisfunktion weist ein Ausweisinhaber sich durch den Besitz des Ausweisdokuments und die Kenntnis einer PIN aus. Der Anbieter eines Dienstes benötigt ein Berechtigungszertifikat, das durch den Chip des Ausweises überprüft wird.

Wesentliche Komponenten zur Verwendung der Online-Ausweisfunktion sind auf Seiten der Bürger eine Client-Software, z.B. die vom Bund kostenfrei zur Verfügung gestellte **AusweisApp**, sowie ein geeignetes Kartenlesegerät. Diensteanbieter benötigen einen eID-Server. Beide Komponenten implementieren das eCard-API Framework.

eCard-API:
Das Ziel des eCard-API Frameworks ist das Bereitstellen einer einfachen und homogenen Schnittstelle, um in verschiedenen Anwendungen eine einheitliche Nutzung von unterschiedlichen Chipkarten zu ermöglichen. Eine dieser Chipkarten ist der neue Personalausweis.

Kartenlesegeräte:
Für die Nutzung des neuen Personalausweises ist ein Kartenlesegerät für Karten mit kontaktlosem Chip nach **ISO 14443** erforderlich. Empfohlen werden Kartenlesegeräte, die vom Bundesamt für Sicherheit in der Informationstechnik (BSI) zertifiziert wurden. Drei Arten von Kartenlesegeräten werden unterschieden: Basis-, Standard- und Komfortleser. Sie werden in der technischen Richtlinie **BSI TR-03119** spezifiziert. Im Gegensatz zu den einfachen Basislesern verfügen Standardleser und Komfortleser über eine eigene Eingabetastatur und die Fähigkeit, das PACE-

Die Beauftragte der Bundesregierung für Informationstechnik

Bundesministerium des Innern
Alt-Moabit 101D, 10559 Berlin

Tel. 030 / 18 681 – 0
info@bmi.bund.de

Der neue Personalausweis
Meine wichtigste Karte.

Protokoll durchzuführen. Während für die Online-Ausweisfunktion Basisleser oder Standardleser genügen, ist für die Nutzung der Unterschriftsfunktion ein Komfortleser erforderlich, der neben der Eingabetastatur auch noch über ein Display und ein Kryptographie-Modul verfügt.

Clientsoftware:
Eine clientseitige Middleware gemäß eCard-API unterstützt die Kommunikation zwischen Kartenlesegerät, Ausweis-Chip und einem entfernten eID-Server, um eine sichere Verbindung zwischen diesen Komponenten herzustellen. Mit der AusweisApp wird den Nutzern eine solche Clientsoftware kostenfrei bereitgestellt.

eID-Server:
Die Hard- und Softwarekomponente zur Nutzung des elektronischen Identitätsnachweises auf Seiten des Diensteanbieters ist der eID-Server. Dieser ermöglicht es Diensteanbietern, die Nutzung der eID-Funktion einfach in ihre bereits existierenden IT-Systeme zu integrieren. Der eID-Server ist mit einer eCard-API-konformen Serversoftware ausgestattet. Diese Software übernimmt im Rahmen des Identitätsnachweises die Kommunikation mit der Client-Software und dem Personalausweis-Chip, übermittelt dem Nutzer die Berechtigungsdaten des Diensteanbieters und gibt die aus dem Chip ausgelesenen Personendaten an den jeweiligen Dienst weiter.

Sicherheitsmechanismen

Datenschutz und Datensicherheit sowie Zugriffsschutz und Authentizität im Zusammenhang mit den neuen Funktionen werden technisch durch geprüfte Protokolle und Verfahren gewährleistet. Persönliche Identitätsdaten können nur nach vorheriger Eingabe der 6-stelligen Geheimnummer (PIN) und mittels eines Berechtigungszertifikates des Diensteanbieters übermittelt werden.

PACE (Password Authenticated Connection Establishment):
Das zur Eingabe der PIN verwendete Protokoll dient auch dem Aufbau eines verschlüsselten und integritätsgesicherten Kanals zwischen dem lokalen Kartenlesegerät und dem kontaktlosen Chip.

Terminalauthentisierung:
Ist der sichere Kanal aufgebaut, kann der Ausweis-Chip mit Hilfe der Terminalauthentisierung verifizieren, ob der Diensteanbieter berechtigt ist, auf Daten im Personalausweis zuzugreifen. Diese Verifizierung erfolgt anhand eines Berechtigungszertifikates, das jeder Diensteanbieter beantragen muss.

Chipauthentisierung:
Ist die Zugriffsberechtigung nachgewiesen, folgt die Prüfung des Ausweis-Chips auf Echtheit. Des Weiteren dient die Chipauthentisierung dem Aufbau eines stark gesicherten Ende-zu-Ende-Kanals zwischen Ausweis und Diensteanbieter. Erst wenn dieser Kanal aufgebaut ist, kann auf die Daten im Chip zugegriffen werden.

Infrastruktur

Die Nutzung der Online-Ausweisfunktion im E-Government und E-Business wird durch eine umfangreiche Infrastruktur ermöglicht. An der Public Key Infrastruktur (PKI), die z. B. für die Berechtigungszertifikate und das Sperrmanagement verantwortlich ist, sind eine Reihe von Behörden und Institutionen beteiligt. Dazu gehören: das Bundesamt für Sicherheit in der Informationstechnik (BSI) als Betreiber der Root-CA, das Bundesverwaltungsamt (BVA) mit der Vergabestelle für Berechtigungszertifikate (VfB) und dem Sperrdienst, die Trustcenter, die die eigentliche technische Ausstellung der Berechtigungszertifikate übernehmen, die Bundesdruckerei als Hersteller der neuen Ausweise und die Trustcenter, die qualifizierte Signaturzertifikate zum Download auf den neuen Ausweis bereitstellen. Die Berechtigungszertifikate der Berechtigungs-PKI sind CV-Zertifikate (Card Verifiable Certificates) nach **ISO 7816**. Die Zertifikate für die qualifizierte elektronische Signatur sind **X.509**-Zertifikate.

Sperrmanagement

Um die missbräuchliche Nutzung gestohlener oder verloren gegangener Personalausweise zu verhindern, können diese gesperrt werden. Ein mögliches Tracking von einzelnen Ausweisen wird durch die Verwendung von spezifischen Sperrlisten für jeden Diensteanbieter verhindert. Die Ausweise übersenden demnach ein dienste- und kartenspezifisches Sperrmerkmal, das auf der Seite der Diensteanbieter gegen die individuelle Sperrliste abgeglichen wird. Die zentrale Sperrliste, aus der die für Diensteanbieter spezifischen Listen erzeugt werden, wird beim Bundesverwaltungsamt betrieben.

Informationen und Kontakte

Weitere Informationen zu den Sperrlisten und relevanten technischen Richtlinien des BSI finden Sie unter www.bsi.bund.de.

Relevante Technische Richtlinien

- **BSI TR-03110** EAC und PACE
- **BSI TR-03112** eCard-API
- **BSI TR-03127** Architektur
- **BSI TR-03130** eID-Server