Der neue Personalausweis als Berechtigung zur Zutrittssteuerung

Eine Zusammenfassung der Eigenschaften und der Betriebsweise des ePA bzw. nPA

Der elektronische Personalausweis der Bundesrepublik Deutschland hieß bisher meist ePA (elektronischer Personalausweis), jetzt wird er auch nPA (neuer Personalausweis) genannt[1)]. Er wird ausschließlich an deutsche Staatsbürger ausgegeben. Gleichartig aufgebaut und mit gleichem Equipment auszulesen ist der elektronische Aufenthaltstitel (eAT) für visumpflichtige Nicht-EU-Bürger, die sich längere Zeit in Deutschland aufhalten wollen. Ein in ähnlicher Weise auszulesendes, hoheitliches Dokument gibt es für die Bürger der anderen EU-Staaten und nicht-visumpflichtige Ausländer bisher nicht, sie müssen sich also mit einem anderen ID-Mittel ausweisen.

[1)] Der nPA ersetzt seit 01.11.2010 den bisherigen Ausweis. Mittlerweile wird er meist „Personalausweis mit Online-Ausweisfunktion" genannt.

Der nPA trägt **drei Hauptapplikationen**, nämlich

- den hoheitlichen Identitätsnachweis, ggf. inklusive der biometrischen Erkennung*, der ausschließlich hoheitlichen Zwecken zur Verfügung steht.
- die Signaturanwendung für die gesetzeskonforme elektronische Unterschrift.
  Sie wird nachträglich auf Antrag freigeschaltet und ist kostenpflichtig.
- den elektronischen Identitätsnachweis (eID-Funktion oder Online-Ausweisfunktion), der für den Identitätsnachweis bei Käufen im Internet, aber ggf. auch bei Sicherheitsanwendungen zum Einsatz kommen kann.

*** Hinweis zur biometrischen Erkennung:**

Auf dem Chip im Ausweis werden ein digitales Lichtbild und auf freiwilliger Basis digitale Fingerabdrücke hinterlegt. Diese sogenannten biometrischen Merkmale dienen ausschließlich zur sicheren Feststellung der Identität durch Behörden (bspw. bei Grenz- oder Polizeikontrollen). Mit ihnen kann schnell und zuverlässig festgestellt werden, ob die Person, die den Ausweis vorlegt, auch der berechtigte Inhaber bzw. die berechtigte Inhaberin ist.

Der nPA steht nur Personen ab 16 Jahren zur Verfügung. Die eID-Funktion des nPA kann bei Erstausgabe auf Wunsch kostenlos freigeschaltet werden, eine nachträgliche Freischaltung ist kostenpflichtig.
Hier wird nur der elektronische Identitätsnachweis eID mit Ausweislesern (ohne die hierfür nicht zugängliche biometrische Erkennung) betrachtet, die beiden anderen Funktionen stehen ausschließlich und eng begrenzt nur für die beschriebenen Einsatzfelder zur Verfügung.

Voraussetzung für die Nutzung der Online-Ausweisfunktion (eID-Funktion)

Die Online-Ausweisfunktion macht die sichere gegenseitige Authentisierung zweier Kommunikationspartner (der Dienstanbieter und der Ausweisinhaber) online und an Automaten möglich (siehe vorab: Hauptapplikationen). In diesem Papier wird die eID-Funktion zur Nutzung als Ausweis zur Zutrittsregelung behandelt. Per Definition und in Teilen der Normung wird die gesteuerte Berechtigung des physischen Zutritts zu Arealen, Gebäuden oder Räumen auch als „Zutrittskontrolle" oder „Zutrittssteuerung" bezeichnet, jedoch leider nicht konsequent.

Oft wird auch von einer Zugangskontrolle gesprochen, obwohl dieser Begriff für den gesteuerten Zugang zu Rechnern und Kommunikationsnetzen gilt. Die Zugangskontrolle soll den unberechtigten Zugriff auf Programme, Dateien und Datennetze verhindern. Die Personenidentifikation erfolgt bei beiden Berechtigungsprüfungen über die Online-Ausweisfunktion mit PIN-Eingabe und wird deshalb oft miteinander verwechselt. Bei der gegenseitigen Authen-

tisierung mit der Online-Ausweisfunktion weist sich ein Ausweisinhaber durch den Besitz des nPA und Buchung an einem Lesegerät mit Eingabe einer PIN aus. Der Anbieter eines Dienstes, z.B. einer Zutritts- oder Zugangskontrolle, benötigt ein Berechtigungszertifikat, welches auf dem eID-Server hinterlegt bzw. abgespeichert ist. Beim Buchungsablauf (s. Abb. S. 3) wird durch den Chip des Ausweises überprüft, welche personen- und ausweisbezogenen Daten der Anbieter eines Dienstes aus dem Personalausweis des Nutzers abfragen darf.

Um Ausweisdaten von einem PC übertragen zu können, wird ein Kartenlesegerät für Ausweise mit kontaktlosem RFID-Chip (Mifare DESFire-Ausweise) nach ISO 14443 benötigt. Empfohlen werden vom BSI zertifizierte Kartenleser. Diese erkennt man am aufgedruckten Personalausweis-Logo (s. Bild rechts).

Man unterscheidet drei Typen von Lesegeräten oder Terminals, die in der technischen Richtlinie BSI TR 03119 spezifiziert sind:

- Bei der Verwendung eines Basis-Kartenlesers (ohne Display und PIN-Tastatur) muss die 6-stellige PIN über die Computertastatur eingegeben werden.
- Standard- und Komfort-Kartenleser verfügen über eine eigene Tastatur zur PIN-Eingabe.
- Komfort-Kartenleser unterstützen darüber hinaus auch die Unterschriftsfunktion des neuen Personalausweises.

Bildquelle:
Broschüre des BMI: Der neue Personalausweis - Informationen zur Online-Ausweisfunktion

Außerdem ist eine zertifizierte Software (AusweisApp 2) erforderlich, die die Kommunikation* zwischen dem Ausweisleser/Terminal und dem PC ermöglicht. Diese wird kostenfrei vom Bundesamt für Sicherheit in der Informationstechnik (BSI) unter https://www.ausweisapp.bund.de/startseite zur Verfügung gestellt. Auf dieser Webseite erhält man ferner eine Liste der verfügbaren Lesegeräte.

** Im Rahmen der sogenannten Terminal Authentication (TA) prüft der Chip des nPA mit Hilfe eines Challenge-Response-Verfahrens die Zugriffsberechtigungen des Lesegeräts (Terminal). Die Protokollspezifikation der Terminal Authentication ist in [BSI-TR-03110], Abschnitt 4.4.1 zu finden.*

Ausweisinhalt, eID-Daten und Funktionen

Für die eID-Funktion stehen folgende Datensätze zur Verfügung, aus denen aber je nach Applikation und Zertifikat des Diensteanbieters nur ein Teilbereich zugänglich ist:

- Vor- und Familienname(n), akademischer Grad; Ordens-, Künstlername
- Geburtstag und -ort; Angabe, ob ein bestimmtes Alter über- oder unterschritten ist
- Anschrift, Wohnort-ID
- Dokumentenart („Personalausweis“) und ausstellendes Land („D“)
- Dienste- und kartenspezifisches Kennzeichen, DKK (siehe „Ausweisgültigkeit“ und „Pseudonymfunktion“)

Applikationsspezifische zusätzliche Daten können nicht hinzugefügt werden, alle Daten können nur gelesen werden, Schreibfunktionen sind unterbunden.

Ausweisgültigkeit

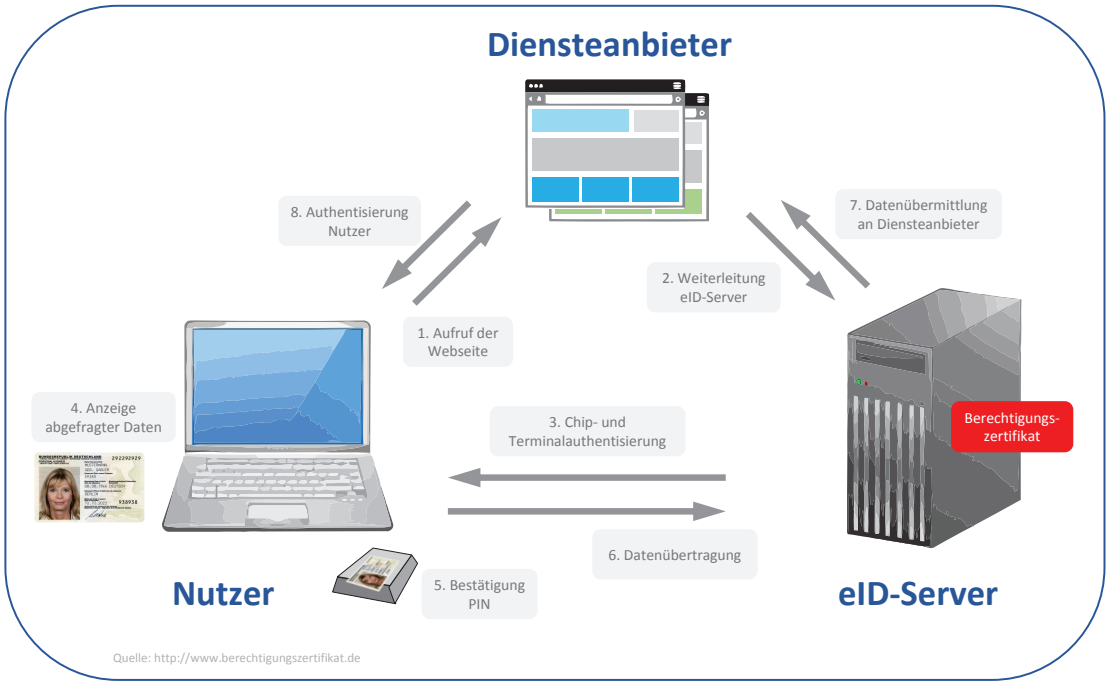
Das Sperrmerkmal und die Angabe, ob der Personalausweis gültig oder abgelaufen ist, werden zur Überprüfung immer übermittelt. Die Abfrage von Datenfeldern durch einen Diensteanbieter kann jedoch nur erfolgen, wenn dieser ein entsprechendes Berechtigungszertifikat besitzt.

Pseudonymfunktion

Die im nPA integrierte Pseudonymfunktion dient der Identifikation* des Ausweisinhabers, ohne dass personenbezogene Daten über das Internet übertragen werden müssen.

** Hierzu wird dem nPA im Berechtigungszertifikat des Diensteanbieters eine eindeutige Kennung des Dienstes übermittelt. Aus dieser Kennung und einem chip-individuell gespeicherten (privaten) Schlüssel (für Restricted Identification = RI) erzeugt bzw. berechnet der nPA-Chip ein Pseudonym („Cookie") als eindeutiges Identifikationsmerkmal. Das Pseudonym ändert sich mit der Ausstellung eines neuen Ausweises und muss über einen neuen Registrierungsprozess dem Diensteanbieter mitgeteilt werden (siehe Berechtigungszertifikat). Das Pseudonym bzw. DKK ermöglicht außerdem eine Wiedererkennungsfunktion, ohne dass jedes Mal Namen und Geburtsdatum ausgelesen werden müssen (Datenreduzierung).*

Buchungsablauf/Identifikationsnachweis



http://www.berechtigungszertifikat.de/

- Jede ZK-Buchung bzw. Transaktion kann nur mit einem (technischen) Berechtigungszertifikat, welches dem Dienstanbieter durch eine Berechtigungs-CA (BerCA) ausgestellt wird, durchgeführt werden. Zuvor muss der Dienstanbieter einen entsprechenden Antrag bei der Vergabestelle für Berechtigungszertifikate stellen. Erst mit dem positiven Bescheid darf die BerCA für einen Dienstanbieter tätig werden. Ausführliche Informationen zu Berechtigungszertifikate und -Anbieter finden Sie unter:
  http://www.personalausweisportal.de; in Suchfeld „Berechtigungszertifikate" eingeben
- Jede Transaktionsfreigabe bzw. ZK-Buchung/Identifikation erfordert eine 6-stellige PIN-Eingabe.
- Der zum Berechtigungszertifikat gehörende private Schlüssel kann entweder von einem eID Service Provider treuhändisch verwaltet oder in einem geeigneten Schlüsselspeicher im System des Dienstanbieters erzeugt und gespeichert werden (z.B. einer SmartCard).
- (Technische) Berechtigungszertifikate sind 2 Tage gültig und müssen täglich erneuert werden. Diese automatische Funktion übernimmt entweder der eID Service Provider oder das System des Dienstanbieters selbst.
- Das Identitätszertifikat muss realtime eingeholt werden, eine Speicherung mit regelmäßigem Update der Zertifikate ist nicht möglich.
- Nach Hochrechnung benötigt das Übermitteln von Ausweisdaten heute ca. 10-15 Sekunden je Identitätsprüfung, die eigentliche Transaktion ca. 5 Sekunden, zuzüglich der Dauer für die Eingabe der PIN ohne Berücksichtigung zusätzlicher Softwarefunktionen, z.B. für die Zutrittskontrolle. Bei Einschaltung eines eID Service Provider kommt die Dauer für die online Kommunikation mit dem eID Server hinzu.

- Das Berechtigungszertifikat ist kostenpflichtig (nach Angaben im Test ca. 6.000 € /100.000 Buchungen)*, bei Einschaltung eines eID Service Provider kommen weitere Kosten für die einzelnen Buchungen hinzu.

  ** Hinweis: Dies sind Transaktionskosten, die der eID Service Provider in Rechnung stellt. Hinzu kommt (je nach Anbieter) noch eine Setup-Gebühr und jährliche Gebühren für das Hosten der Zertifikate.*
- Verifikation nur mit Ausweis und 6-stelligem PIN (so genannte Zwei-Faktor Authenifizierung: Besitz und Wissen), hinterlegte biometrische Daten stehen dazu nicht zur Verfügung.
- RFID-Ausweisleser, wie sie in mechatronischen Zutrittssystemen (Offline-Türterminals, Schließzylinder) genutzt werden, können nicht eingesetzt werden. Diese verfügen über keine Zertifizierung (bzw. erfüllen nicht die Anforderungen der BSI TR 03119) und benötigen zusätzliche Zutrittsparameter, die nicht auf den nPA geschrieben werden können (siehe Ausweisinhalt).
- Der Ausweisleser bzw. seine Software muss zertifiziert sein. Der PC bzw. Server mit seinem Ausweisleser für die Abwicklung der Identitätsprüfung muss einen direkten Internetanschluss besitzen. Offline-Lösungen (d.h. Verzicht auf dauernden Internetzugang) werden derzeit spezifiert und können deshalb vom BHE in dieser Ausarbeitung und bezüglich ihrer Eignung für die ZK nicht bewertet werden.

Hinweis: Will der Betreiber eines Zutrittssystems nur die Pseudonymfunktion nutzen, muss er sich als Dienstanbieter bei der Vergabestelle für Berechtigungszertifikate (VfB) akkreditieren. Damit kann er das Zertifikat - in dem das RI-Zugriffsrecht nachgewiesen wird - und die darin freigegebenen, eingeschränkten Datenfelder des Ausweises lesen.

Nutzung des nPA zur Zutrittssteuerung

Nach Aussagen des BSI stellt die Nutzung des nPA zur Zutrittssteuerung eine spezielle Offline-Anwendung des nPA dar. Für diese wurden bisher noch keine expliziten rechtlichen und technischen Anforderungen definiert. Es gilt aber der im Personalausweisgesetz festgelegte allgemeine Rechtsrahmen. Ferner gibt es seitens des BSI keine Erfahrungswerte, da für diese Anwendung noch keine Berechtigungszertifikate vergeben wurden. Es gelten daher nur die grundsätzlichen Anforderungen*, die von allen Teilnehmern der eID-Infrastruktur umgesetzt werden müssen.

** Hinsichtlich der technischen Anforderungen zur Realisierung eines Zutrittkontrollsystems mit dem nPA müssen die folgenden grundsätzlichen Anforderungen erfüllt werden:*

- *Kern der Zutrittskontrollanlage bildet der Authentisierungsserver in der Zutrittszentrale. Dieser muss über ein Kryptografiemodul gemäß CVCA-eID Certificate Policy (Abschnitt 6.2) zur Speicherung des privaten Terminal-Schlüssels verfügen.*
- *Die Zutrittszentrale muss organisatorisch und technisch so gesichert sein, dass das gleiche Sicherheitsniveau, wie es von anderen Diensteanbietern erwartet wird, erreicht wird (siehe TR-03130, Anhang C Kapitel 4 „Schutzbedarf") .*
- *An den Zutrittspunkten sollten nur zertifizierte Ausweisleser eingesetzt werden.*
- *Sofern eine BerCA eine Schnittstelle nach TR-03129 anbietet, kann der Authentisierungsserver hierüber automatisiert Berechtigungszertifikate beziehen.*

Ob ein Anbieter für die Zutrittssteuerung eine Berechtigung bzw. ein Berechtigungszertifikat erhält, entscheidet die Vergabestelle für Berechtigungszertifikate (VfB, www.bva.bund.de/vfb). An diese muss man sich wenden und erklären, dass ein Zutrittskontrollsystem realisiert werden soll, welches die „Pseudonyme Kennung" aus dem nPA benötigt. Vorteilhaft ist, wenn zu dieser Anfrage ein Sicherheitskonzept für das geplante Zutrittskontrollsystem beigefügt werden kann. Hierüber könnte dann parallel die sicherheitstechnische Eignung geprüft werden.

Fazit

Der nPA kann z. B. zum sicheren Identitätsnachweis für Besucher in Sicherheitsbereichen eingesetzt werden, jedoch eingeschränkt auf den genannten Personenkreis. Für den Einsatz in Sicherheitsbereichen mit marktgängigen Zutrittsanlagen wären folgende Bedingungen bzw. Einschränkungen auf ihre Verträglichkeit mit dem geplanten Einsatzzweck zu prüfen:

- Die Nutzung des nPA zur Zutrittssteuerung ist, wie auch die Einführung einer Zutrittssteuerung selbst, mitbestimmungspflichtig.

- Nur Deutsche können den nPA besitzen, die relativ wenigen visumpflichtigen Nicht-EU-Bürger, deren Visa ebenfalls gelesen werden könnten, sind in diesem Zusammenhang zu vernachlässigen.
- Jede Buchung ist für den Betreiber des Zutrittskontrollsystems kostenpflichtig. Die Gesamtkosten ergeben sich u.a. aus den Kosten für das Berechtigungszertifikat sowie den Betriebs- und Servicekosten des jeweiligen eID-Services-Providers, bzw. den eigenen Betriebskosten für das Betreiben eines eID-Servers. Bei Nutzung der Pseudonymfunktion und eigener Akkreditierung sind die Zertifikate ebenfalls kostenpflichtig.
- Der Nutzer muss mindestens 16 Jahre alt sein.
- Jeder Identifikationsnachweis dauert ca. 5 – 15 Sekunden.
- Jeder Identifikationsnachweis benötigt die Eingabe eines 6-stelligen PINs, deshalb muss der Ausweisleser über eine numerische Tastatur verfügen.
- Das Zutrittssystem mit dem Ausweisleser benötigt eine direkte Internet-Anbindung.

Der nPA kann nicht als multifunktionaler Mitarbeiterausweis für andere kartengesteuerte Anwendungen, z.B. Betriebs- oder Kantinendatenerfassung, genutzt werden. Da keine zusätzlichen Informationen auf dem Ausweis gespeichert bzw. geschrieben werden können, z.B. Guthaben oder zeitlich begrenzte Berechtigungen, ist der Einsatz für entsprechende Anwendungen nicht möglich.

Abkürzungen und Begriffe

Nachfolgende Tabelle gibt einen Überblick über die in diesem Dokument verwendeten Abkürzungen.

BerCA	Berechtigungszertifikate-Anbieter
BSI	Bundesamt für Sicherheit in der Informationstechnik
CA	Chip Authentication: Authentifizierung der Karte und Aufbau eines sicheren Kanals (Analog authentifizierter Server bei SSL / Homebanking)
CVCA-eID	Country Verifying Certificate Authority - electronic Identity Die CVCA-eID stellt für Berechtigte Document Verifier (DV) Zertifikate aus. Die Kontaktadresse lautet: CVCA-eID@bsi.bund.de
DKK	Dienste- und kartenspezifisches Kennzeichen
eID	elektronischer Identitätsnachweis (Anwendung im ePA)
eAT	elektronische Aufenthaltstitel
ePA	elektronischer Personalausweis
ID	Idendifikation
nPA	neuer Personalausweis
PACE	Password Authenticated Connection Establishment
PC	Personal Computer
PIN	Persönliche Identifikationsnummer
RFID	Radio Frequency Identification
RI	Restricted Identification (sektorspezifisches, eindeutiges Merkmal zur Wiedererkennung)
TA	Terminal Authentication (Identifizierung und Authentifizierung des berechtigten Terminals)
TR-xxxxx	Technische Richtlinie

Quellen:
http://www.bmi.bund.de
http://www.bsi.bund.de
http://www.personalausweisportal.de
https://www.ausweisapp.bund.de

BHE Bundesverband Sicherheitstechnik e.V., Feldstraße 28, 66904 Brücken, Tel.: 06386 9214-0, Fax: 06386 9214-99, info@bhe.de, www.bhe.de