

Der neue Personalausweis als Ausweis für Zutrittsregelung Eine kurze Zusammenfassung der Eigenschaften und der Betriebsweise des ePA bzw. nPA

Der neue elektronische Personalausweis der Bundesrepublik Deutschland hieß bisher meist ePA (elektronischer Personalausweis), jetzt wird er auch nPA (neuer Personalausweis) genannt. Er wird naturgemäß ausschließlich an deutsche Staatsbürger ausgegeben. Gleichartig aufgebaut und mit gleichem Equipment auszulesen ist die elektronische Aufenthaltsbestätigung 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.

Der nPA trägt drei **Hauptapplikationen**, nämlich

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

Er steht nur Personen ab 16 Jahren zur Verfügung. Er kann bei Erstausgabe des nPA auf Wunsch kostenlos freigeschaltet werden, eine nachträgliche Freischaltung ist kostenpflichtig.

*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. Mit ihnen kann schnell und zuverlässig festgestellt werden, ob die Person, die den Ausweis vorlegt, auch der berechnigte Inhaber bzw. die berechnigte Inhaberin ist.

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

Die Online-Ausweisfunktion macht die sichere gegenseitige Authentisierung zweier Kommunikationspartner online und an Automaten möglich (siehe vorab: Hauptapplikationen). In dieser Beschreibung wird die eID-Funktion zur Nutzung als Ausweis zur Zutrittsregelung behandelt. Per Definition und in Teilen der Normung wird die gesteuerte Berechtigung des physikalischen 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 Authentisierung mit der Online-Ausweisfunktion weist ein Ausweisinhaber sich 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, das durch den Chip des Ausweises überprüft wird.

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



Man unterscheidet drei Typen von Lesegeräten, 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 erforderlich, die die Kommunikation zwischen dem Ausweisleser und dem PC ermöglicht.

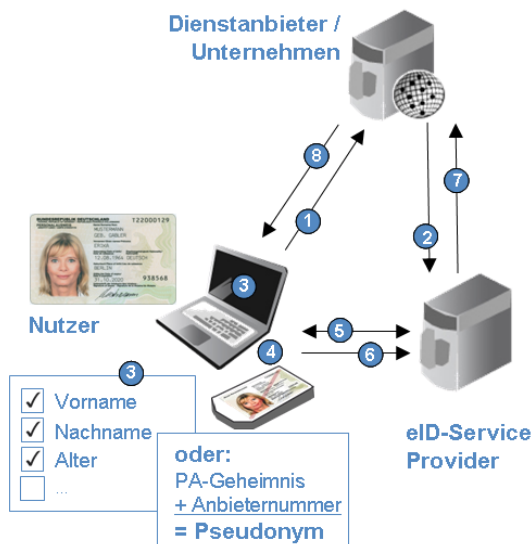
Ausweisinhalt für eID-Funktion

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), Doktorgrad
- 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 („Pseudonym“) (wird aus den Daten errechnet! „Cookie“)

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

Buchungsablauf/Identifikationsnachweis



1. Aufruf der Webseite/Zugriff auf den Softwaredienst
2. Weiterleitung zum eID-Service Provider
3. Auswahl Datenfelder
4. Bestätigung durch PIN und PACE
5. Terminal- und Chipauthentisierung
6. Datenübermittlung
7. Übermittlung der Daten aus Schritt 6 an den Diensteanbieter
8. Nutzer authentisiert

Bildquelle: Christian Hoffmann, CCnPA

- Jede Buchung kann nur mit Identitätszertifikat erfolgen, erfordert also eine 6-stellige PIN-Eingabe und einen Verbindungsaufbau zum eID-Serviceprovider.
- Das Identitätszertifikat muss realtime eingeholt werden, eine Speicherung mit regelmäßigem Update der Zertifikate ist nicht möglich.
- Nach Angaben dauert die Abwicklung des Zertifikats heute ca. 10 – 15 Sekunden / Buchung.
- Das Zertifikat ist kostenpflichtig (nach Angaben im Test ca. 6.000 €/ 100.000 Buchungen).
- Das Pseudonym („Cookie“) ist pro Ausweis eindeutig, ändert sich aber mit neuem Ausweis.
- Verifikation nur mit Ausweis und 6-stelligem PIN, hinterlegte biometrische Daten stehen dazu nicht zur Verfügung.
- Der Ausweisleser bzw. seine Software muss zertifiziert sein. Der PC bzw. Server mit seinem Ausweisleser für die Abwicklung der Identitätsprüfung muss einen direkten Internet-Anschluss besitzen.

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 Zutrittsregelung ist wie auch die Einführung einer Zutrittsregelung 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 kostenpflichtig,
- der Nutzer muss mindestens 16 Jahre alt sein
- jeder Identifikationsnachweis dauert ca. 10 – 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. Kantinendatenerfassung, genutzt werden. Da keine zusätzlichen Informationen auf dem Ausweis gespeichert bzw. geschrieben werden können, ist der Einsatz in Anwendungen, bei denen Daten auf dem ePA abgespeichert werden müssen, z.B. Guthaben oder zeitlich begrenzte Berechtigungen, nicht möglich.

Quellen:

www.bmi.bund.de; www.bsi.bund.de; www.personalausweisportal.de

https://www.bsi.bund.de/cln_174/DE/Themen/ElektronischeAusweise/Personalausweis/personalausweis_node.html

<http://www.personalausweisportal.de>

BHE e.V.	Feldstr. 28 66904 Brücken	Telefon: 0 63 86/92 14-0 Telefax: 0 63 86/92 14-99	Internet: www.bhe.de E-Mail: info@bhe.de
-----------------	--------------------------------------	---	--