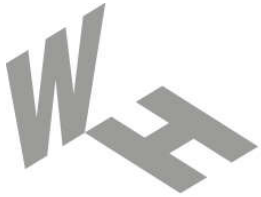


Westfälische Hochschule
Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

Der neue Personalausweis

Prof. Dr. (TU NN)
Norbert Pohlmann

Institut für Internet-Sicherheit – if(is)
Westfälische Hochschule, Gelsenkirchen
http://www.internet-sicherheit.de

Inhalt

- Einführung
- Technik
- Daten & Funktionen
- Anwendungen
- Prozesse für Beantragung und Ausstellung
- Restrisiko
- Zusammenfassung

Inhalt

- **Einführung**
- Technik
- Daten & Funktionen
- Anwendungen
- Prozesse für Beantragung und Ausstellung
- Restrisiko
- Zusammenfassung

Ziele

- Grundlegendes Verständniss für die Ziele und Möglichkeiten des neuen Personalausweises (nPA)
- Funktionalitäten und Eigenschaften des neuen Personalausweises
- Rahmenbedingungen und Spezifikationen

Ausgangssituation
→ Dilemma: Passwort-Authentisierung

- **Passworte, Passworte, … sind das Authentisierungs-Mittel im Internet!**
  - Passwort-Probleme
    - Verwendung von schlechten Passwörtern, oder
    - ein gutes Passwort wird für viele Dienste verwendet
    - Passworte werden im Klartext in HTTP-Sessions und in E-Mails über das Internet übertragen!
    - Passwort-Reset-Mechanismen sind sehr unsicher

- **Identifikationsbereiche liegen im Unternehmens- und Kundenumfeld!**
  - D.h. neben unterschiedlichen Passworten müssen wir uns auch oft noch unterschiedliche Identitäten merken!

- **Phishing-Problem** verursacht einen sehr großen Schaden (BKA)

Neuer Personalausweis – nPA
→ Vorteile der eID-Funktion

- **Deutlich höheres Sicherheitsniveau** im Vergleich zur herkömmlichen Passwort-Authentisierung im Internet!

- **Gegenseitige Authentifizierung**
  - nPA prüft das Berechtigungszertifikat *(Analogie …)*
  - eID-Server prüft die **Authentizität des nPAs**
  - Die AusweisApp prüft die Domäne des Dienstanbieters (Hash des SSL-Zertifikats) aus dem Berechtigungszertifikat
    → **Weniger Phishing-Angriffe!**

- **Zweifaktor-Authentisierung: Wissen (PIN) und Besitz (nPA)**
- Berechtigungszertifikat beschränkt die auszulesenden Merkmale
- Personenbezogene Daten gehen im Rahmen der eID-Funktion **nie** im Klartext über die Leitung

- **Hinweis:**
  Die eID-Funktion ersetzt die **Identitätsfeststellung** (nicht die Signatur!)
  - **Die eID-Funktion ist kein Verfahren zur Autorisierung einer Transaktion!**

Herausforderungen bei der Einführung

- **Rechtlich**
  - Personalausweisgesetz
  - Personalausweisverordnung
  - Verwaltungsvorschriften
  - Sonstige Änderungen (Signaturgesetz, GWG)

- **Gesellschaftspolitisch**
  - Informationelle Selbstbestimmung (hohe Anforderungen an den Datenschutz)
  - Elektronischen Identitätsnachweis (eID) als „Online-Ausweis“ etablieren

- **Organisatorisch**
  - Neue Organisationseinheiten/-stellen, zum Beispiel Vergabestelle für Berechtigungszertifikate, Sperr-Register etc
  - Neue Verfahren/Abläufe in den beteiligten Organisationen (insbesondere in den Personalausweisbehörden)

Rechtliche Rahmenbedingungen

- **Personalausweisgesetz (PAuswG)**
  - Personalausweisverordnung (PAuswV) mit Verweis auf Technische Richtlinien
  - Personalausweisgebührenverordnung
  - Verwaltungsvorschriften
  - Sonstige Änderungen (Signaturgesetz, Geldwäschegesetz)

- Weitere rechtliche Änderungen:
  - Passverordnungen

eID – Beispiele in Europa

- Finnland: FINEID seit 2000
- Estland: eCard seit 2002
- Belgien: eID seit 2003
- Österreich: eCard seit 2004
- Schweden: National eID seit 2005
- Italien: CIE & CNS seit 2006
- Portugal: Cartão de Cidadão seit 2007

- **Zwei unterschiedliche Konzepte:**
  - Lösungen, die eine bestimmte Karte für bestimmte Anwendungen einsetzen (z.B. belgische eID, deutscher nPA)
  - Lösungen, die auf Zertifikaten und Prozeduren beruhen, die keine bestimmte Karte erfordern (österreichische Bürgerkarte)

Zeitplan

2008

2009

2010

20.11.2008
Start Registrierung zentral koord.& offener Anwendungstest

1. Quartal 2009
Information zur Teilnahme am Feldtest

2. Quartal 2009
Auswahl Ausweisbehörden Feldtest

28.02.2009
Ende Registrierung für zentral koord. Anwendungstest

Ende Mai 2009
Auswahl Teilnehmer zentral koord. Anwendungstest

1.Quartal 2010
Start Feldtest

01.10.2009
Start zentral koord. Anwendungstest

2. Quartal 2010
Bericht Feldtest

01.01.2010
Start offener Anwendungstest

01.05.2010
Start Beantragung von Berechtigungszertifikaten

Ende Juni 2010
Bericht Anwendungstest

31.10.2010
Ende Anwendungstest

01.11.2010
Einführung neuer Personalausweis

Inkrafttreten von Gesetz und Verordnungen

Inhalt

- Einführung
- **Technik**
- Daten & Funktionen
- Anwendungen
- Prozesse für Beantragung und Ausstellung
- Restrisiko
- Zusammenfassung

Technik: Neuer Personalausweis
→ Übersicht

TR Lesegerät: 58 Seiten
TR Personalausweis: 42 Seiten

Nutzer (AusweissApp)

Authentisierung

Diensteanbieter

TR EAC: 117 Seiten

Auth.-Ergebnis

Authentisierung

TR eCard API: 492 Seiten
TR Kryptoverfahren: 112 Seiten
TR EAC-Box: 39 Seiten
TR PKI: 121 Seiten

→ Mehr als 1000 Seiten Spezifikationen!

eID - Server

TR eID - Server: 106 Seiten

Physischer Ausweis

- Alle Sichtausweisfunktionen bleiben erhalten
- Langlebiges Polykarbonat für den Kartenkörper
- Verkleinerung auf Scheckkartenformat TD-1 und
- Neuartige Sicherheitsmerkmale im Kartenkörper/Chip
- Kontaktlose Chipkarte (ISO 14443)

Chip

- Kontaktloser Chip kommuniziert mit einem passenden Kartenterminal, welches als Lese- oder Schreibgerät fungiert
- Datenübertragung mittels induktiver Kopplung
- Kryptographisch starker Zufallszahlengenerator unterstützt Kryptographie basierend auf elliptischen Kurven
- Neuer Personalausweis ist eine nach Signaturgesetz [SigG] bzw. Signaturverordnung [SigV] bestätigte sichere Signaturerstellungseinheit.
- ISO 14443-Schnittstelle, Typ A oder B bei 13,56 MHz
- Energieübertragung durch induktive Kopplung (Spezifikation!)
  - Datenübertragung durch Lastmodulation
  - Übertragungsrate 106, 212, 424 oder 847 kBit/s
  - Unique Identifier bei jeder Aktivierung zufällig
  - Reichweite max. 3 – 5 cm

Protokolle

- **Password Authenticated Connection Establishment (PACE):**
  - Aufbau eines verschlüsselten und integritätsgesicherten Kanals zwischen dem lokalen Kartenlesegerät und dem kontaktlosen Chip (Passwort-geschütztes Diffie-Hellman-Protokoll - / Elliptic Curve Cryptography)
  - Verwendung der PIN zur Schlüsselableitung

- **Terminalauthentisierung (TA):**
  - Dienstanbieter authentifiziert sich mit Berechtigungszertifikat *(Analogie …)*
  - Berechtigungszertifikate vom Ausweis-Chip verifizierbar
  - Challenge-Response Protokoll (eID-Server authentifiziert sich gegenüber nPA)

- **Chipauthentisierung: (CA)**
  - Prüfung des Ausweis-Chips auf Echtheit und somit auch der auf dem Chip gespeicherten Daten (nPA authentifiziert sich gegenüber eID-Server)
  - Aufbau eines stark gesicherten Ende-zu-Ende-Kanals zwischen Ausweis und eID-Server.

Die angefragten Daten des Personalausweises werden erst nach dem erfolgreichen Ablauf von PACE, TA und CA übertragen!

Die elektronischen Funktionen

Sichtausweis

Der neue Personalausweis vereint den herkömmlichen Ausweis und die drei neuen elektronischen Funktionen im Scheckkartenformat.

Elektronische Funktionen

- **Pflicht**
  - digitales Lichtbild
    nur lesbar für Behörden, die zur Identitätsfeststellung berechtigt sind, z.B. Polizei und Grenzkontrolle
- **Wunsch**
  - eID (wahrscheinlich nicht mehr)
  - Fingerabdrücke
- **Wunsch + Zusatzkosten**
  - Zertifikat für digitale Unterschrift (QES)
  - Bereitstellung nicht durch den Staat

Die elektronischen Funktionen

- **Hoheitliche Biometrieanwendung**
  - digitales Lichtbild und (auf Wunsch) zwei elektronische Fingerabdrücke
  - ausschließlich zur Identitätsfeststellung für berechtigte Behörden, z.B. Polizei und Grenzkontrolle
- **Elektronischer Identitätsnachweis**, (auch „eID-Funktion“ oder „Online-Ausweisfunktion“)
  - schafft einen Identitätsnachweis im Internet, wie es die Funktion als Sichtdokument außerhalb des Internets bietet
  - Login, Zugang zu Diensten, Übermittlung von Daten aus dem neuen PA
- **Signaturanwendung**
  - sichere, rechtsverbindliche und signaturgesetzkonforme elektronische Unterschrift
  - Unterschrift z.B. unter Verträge und Anträge

Daten für elektronische Funktionen
→ Hoheitliche Anwendungen

- **Hoheitliche (Biometrie-)Anwendung**
  - Digitales Gesichtsbild
  - Zwei Fingerabdrücke
  - Hashwerte der Datengruppen, Signatur über die Hashwerte und zugehöriges DS-Zertifikat
  - **Daten der maschinenlesbaren Zone:**
    - Dokumententyp
    - Familien- und Vornamen
    - Seriennummer
    - Staatsangehörigkeit
    - Geburtsdatum
    - Ablaufdatum
    - Prüfziffern
    - Leerstellen

Daten für elektronische Funktionen
→ Elektronischer Identitätsnachweis

- **Elektronischer Identitätsnachweis**
  - **Datenfelder**
    - Dokumententyp
    - ausgebender Staat
    - Ablaufdatum
    - Familien- und Vornamen
    - Ordens- und Künstlername
    - Doktorgrad
    - Geburtsdatum
    - Geburtsort
    - Anschrift
    - Alters- und Wohnortbestätigung

Daten für elektronische Funktionen
→ Signaturanwendung

- **Signaturanwendung**
  - Die Signatur muss separat bei einem privaten Anbieter erworben werden
  - Keine Daten im Auslieferungszustand des Ausweises vorhanden
  - Nach Aktivierung der Signaturfunktion
    - Signatur-Geheimnummer
    - Signaturschlüsselpaar
    - ggf. qualifiziertes Signaturzertifikat

Elektronischer Identitätsnachweis, eID-Funktion

- **Einsatzzweck**
  - Login, Zugang zu Diensten, Übermittlung von Daten
  - Identitätsnachweis, wie es die Funktion als Sichtdokument außerhalb des Internets bietet
  - Ermöglicht eine gegenseitige Authentisierung zweier Kommunikationspartner über das Internet
- **Funktion**
  - Elektronischer Nachweis der Identität des Ausweisnutzer
  - Diensteanbieter legitimieren sich mit einem staatlichen Berechtigungszertifikat
  - Berechtigungszertifikat gestattet nur das Auslesen der im Zertifikat zugelassenen Daten
- **Daten**
  - Übermittlung von personen- und dokumentenbezogenen Daten
  - Keine Übermittlung von biometrischen Daten

Gegenseitiger Identitätsnachweis

BürgerInnen

Ist das Unternehmen vertrauenswürdig?

Diensteanbieter weist sich mit Berechtigungs-zertifikat aus

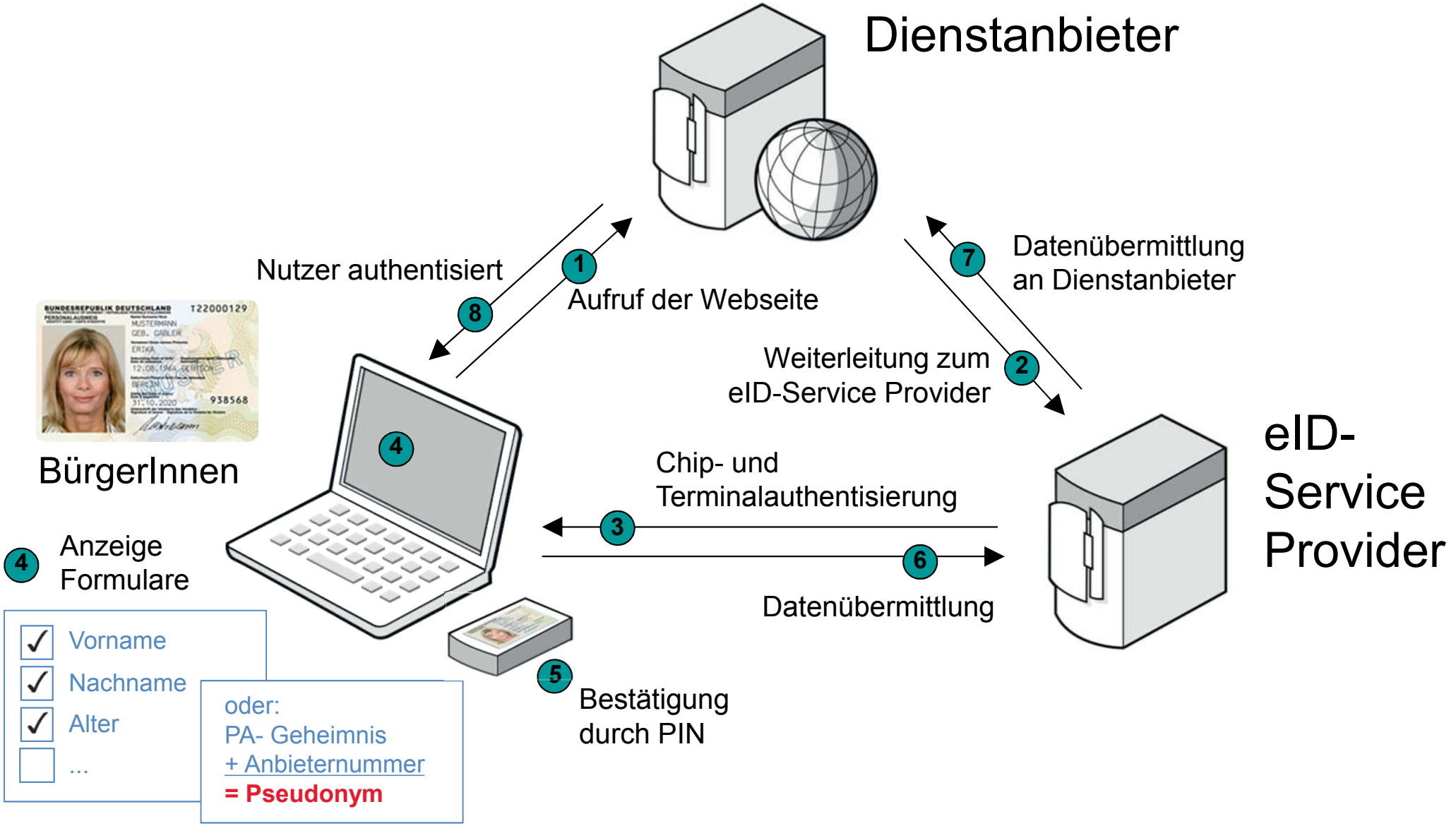
Sowohl Bürger als auch Diensteanbieter können sich bei Nutzung des neuen PA auf die Identität ihres Gegen-übers verlassen

Bürger weist sich mit neuem PA aus

Diensteanbieter

Gibt es die anfragende Person wirklich?

Authentisieren mit der eID-Funktion



Signaturanwendung (QES)

- **Einsatzzweck**
  - Signieren von Dokumenten
  - elektronisches Pendant zur herkömmlichen Unterschrift, Schriftformerfordernis

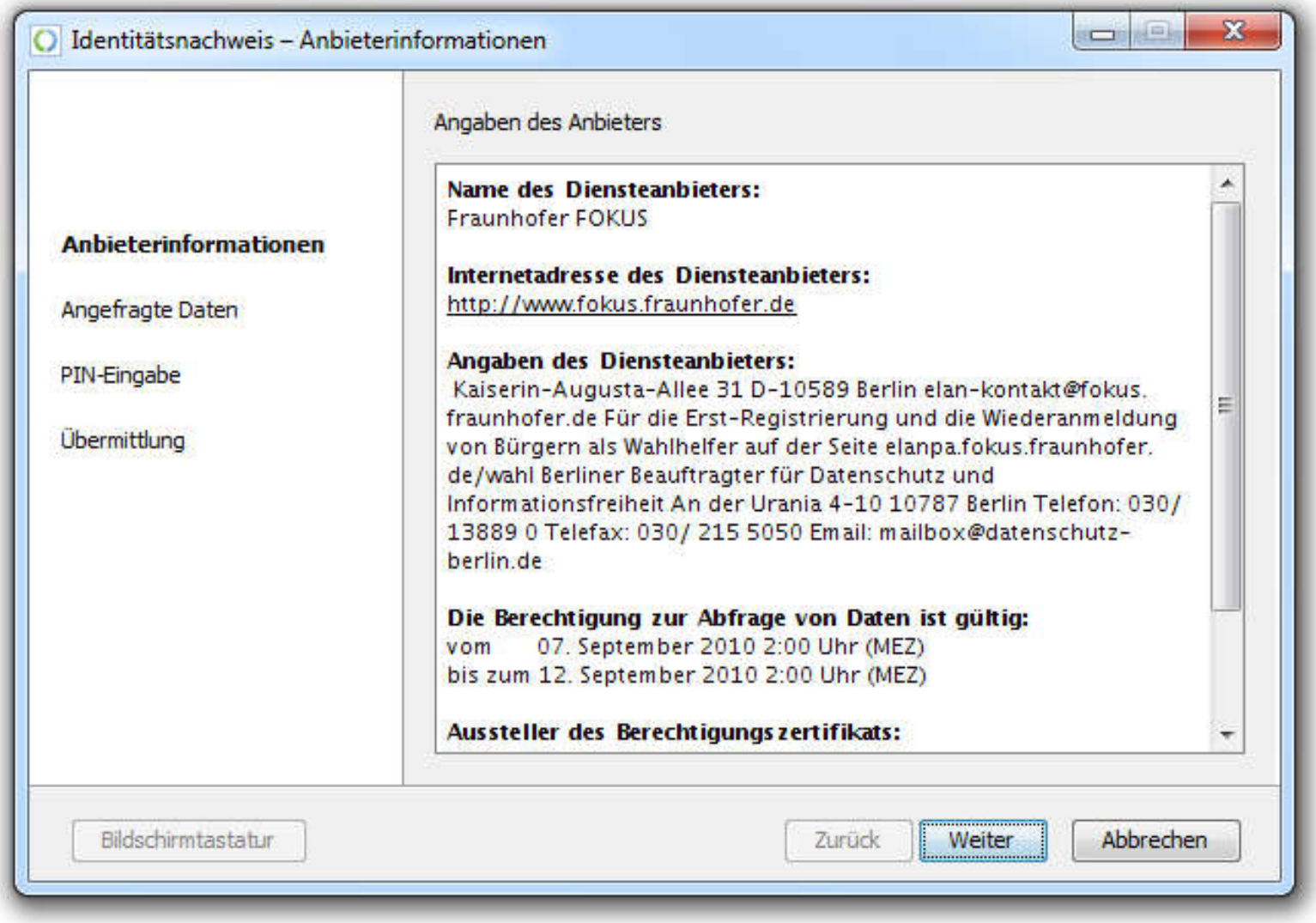
- **Funktion**
  - Personalausweis ist zur Erstellung von qualifizierten elektronischen Signaturen (QES) vorbereitet
  - Signaturanwendung kann bei Bedarf durch den Ausweisinhaber aktiviert werden
  - Bei Aktivierung wird eine Signatur-Geheimnummer (Signatur-PIN) vom Ausweisinhaber festlegt
  - Signaturschlüsselmaterial auf dem Chip des neuen Personalausweises wird erstellt
  - Qualifiziertes Signaturzertifikat wird bei einem Zertifizierungsdiensteanbieter kostenpflichtig erzeugt

- Signaturzertifikate der Signaturanwendung (bzw. konkret die privaten Signaturschlüssel) können nicht von einem abgelaufenen auf einen neuen Personalausweis übertragen werden

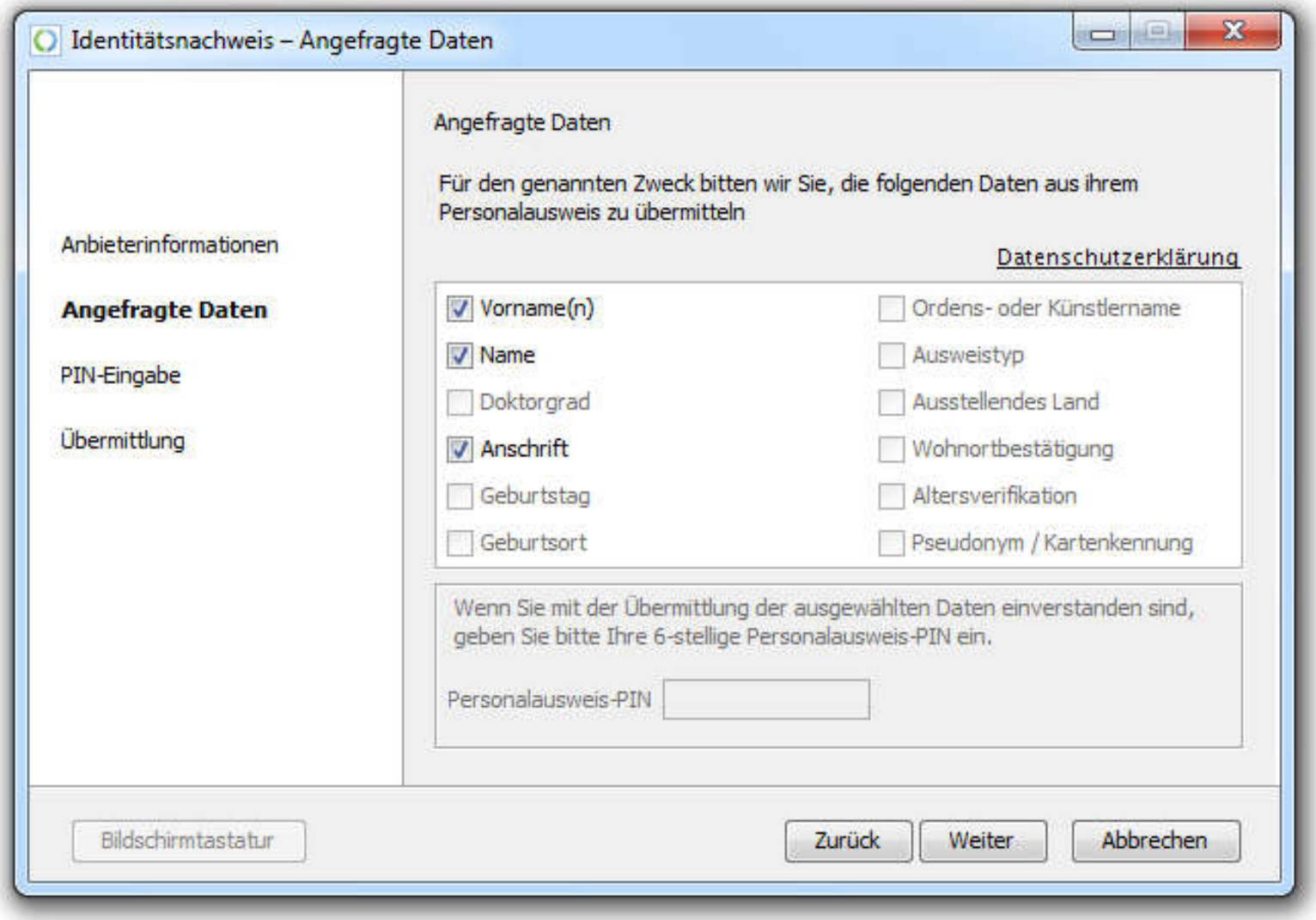
Identitätsnachweis
→ Übersicht

- **Funktion**
  - Kommunikation zwischen dem neuen Personalausweis und eID-Server
  - Software muss auf dem Computer des Bürgers installiert sein
- **Betriebssysteme**
  - Windows:
    - Win 2000
    - Win XP
    - Win Vista
    - Windows 7
  - Debian 5.0 (Kernel Version 2.6.26) und höher
  - Ubuntu 9.04 (Kernel Version 2.6.29) und höher
  - MacOS 10.5 und höher
  - OpenSuse 11.1 (Kernel Version 2.6.27) und höher

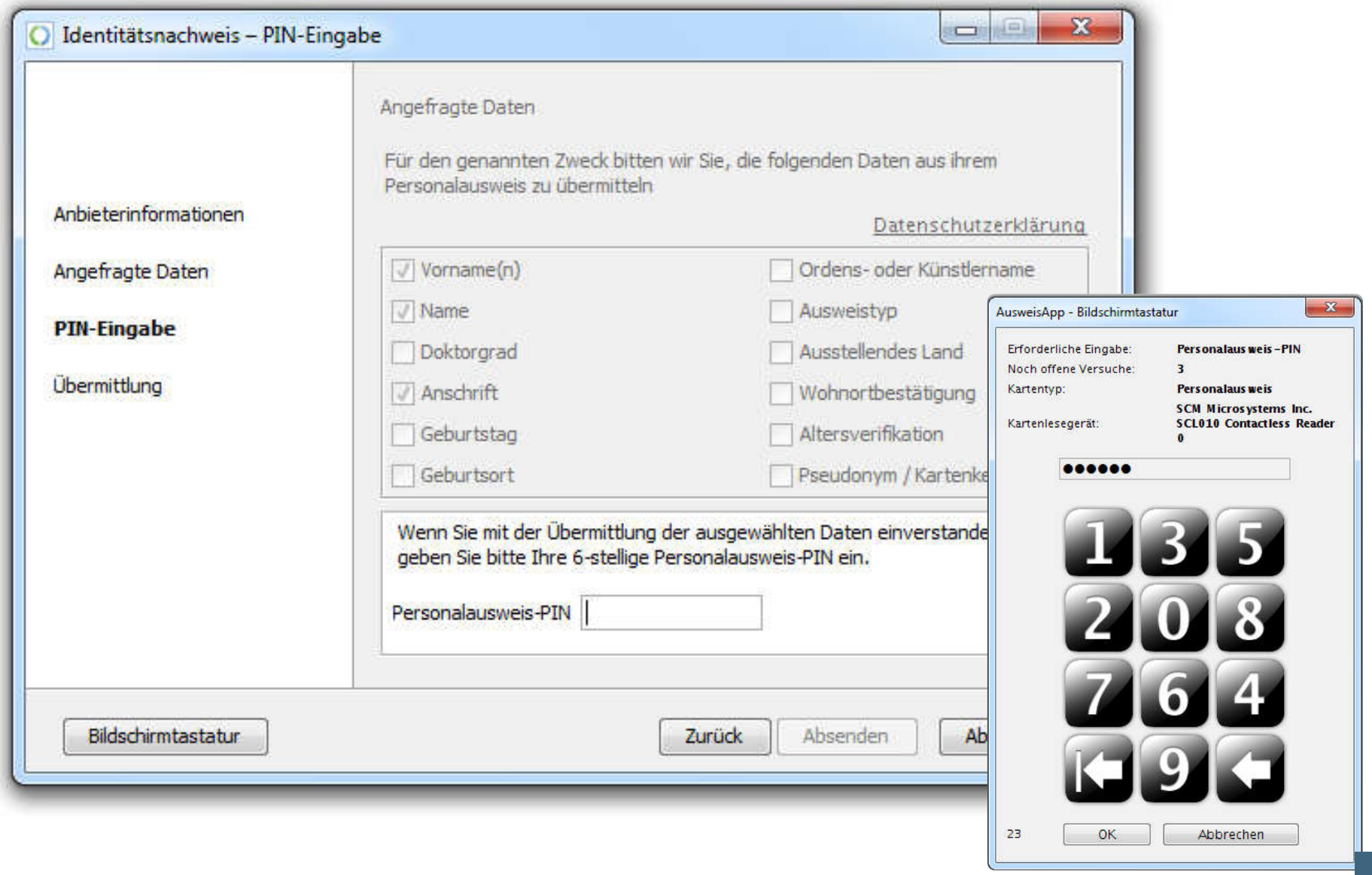
Identitätsnachweis
→ Ausweis App (1/3)



Identitätsnachweis
→ Ausweis App (2/3)



Identitätsnachweis
→ Ausweis App (3/3)

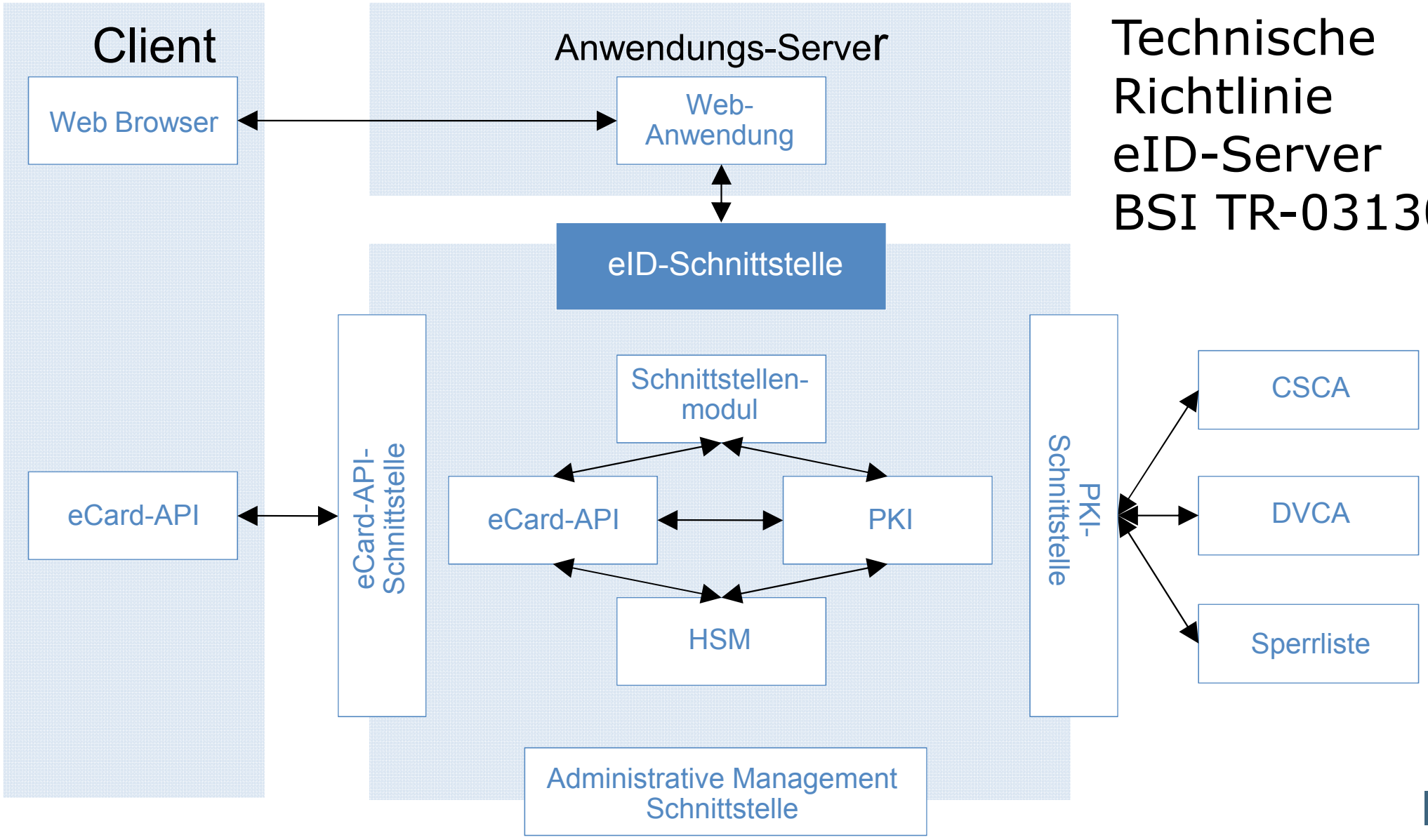


eID-Server / eID-Service

- **eID-Server**
  - Zentrale Komponente zur Abwicklung der eID-Funktion
  - Kostenpflichtige Nutzung durch Dienstanbieter
  - Stellt die Kommunikation zum Identitätsnachweis her
  - Übernimmt die Kommunikation zum Abruf von Berechtigungszertifikaten und Sperrlisten

- **eID-Service**: mandantenfähiger eID-Server
  - Mehrere Diensteanbieter nutzen einen eID-Service
  - Gleichzeitige Bearbeitung beliebig vieler Authentifizierungen für mehrere Dienstanbieter
  - Integrierte Verwaltung von Berechtigungszertifikaten der Diensteanbieter

eID-Server Schnittstellen



Technische Richtlinie eID-Server BSI TR-03130

eID-Server Schnittstellen

- **eID-Server Schnittstellen**
  - Identitätsnachweis (eCard-API)
    - Abwicklung der Sicherheitsprotokolle
    - Gesicherte Übertragung der Datengruppen aus dem neuen Personalausweis
  - Web-Anwendung Diensteanbieter (eID-Anbindung)
    - Gesicherte Übertragung der Datengruppen
  - Public Key Infrastructure
    - Verwaltung der Berechtigungszertifikate
    - Sperrmanagement

Berechtigungen und Berechtigungszertifikate

- Beantragung einer Berechtigung bei der Vergabestelle für Berechtigungszertifikate des BVA mit:
  - Unternehmensdaten (u.a. Name, Sitz)
  - Zweck des Berechtigungszertifikats
  - Beschreibung des Dienstangebots
  - Gewünschte Datenfelder
  - Handelsregisterauszug
  - Verantwortliche Datenschutzaufsichtsbehörde
  - Nutzungsbedingungen

Berechtigungen und Berechtigungszertifikate

- Nach Erforderlichkeitsüberprüfung wird die Berechtigung durch die Vergabestelle für Berechtigungszertifikate des BVA erteilt / abgelehnt
- diese Berechtigung wird für längeren Zeitraum erteilt
- Generierung von kurzlebigen Berechtigungszertifikaten (2 – 3 Tage Gültigkeit) durch Zertifizierungsdiensteanbieter
- gewählter eID-Service übernimmt Verwaltung der Berechtigungszertifikate
- Personalausweis validiert Berechtigungszertifikat

Beantragung von Berechtigungszertifikaten

Diensteanbieter

Beantragung einer Berechtigung für das Auslesen von eID-Daten aus dem Chip des Personalausweises

Antrag →

← Bescheid

Gebühr →

Vergabestelle für Berechtigungszertifikat

Antragsprüfung (Zweckbindung, Erforderlichkeit, Plausibilität usw.)

Entscheidung, auf welche Daten der Diensteanbieter zugreifen darf

Genehmigung oder Versagung Berechtigung

Zertifizierungsdiensteanbieter

Verwendung des Berechtigungszertifikats für den elektronischen Identitätsnachweis (Diensteanbieter weist sich damit gegenüber dem Ausweisinhaber aus)

← Bereitstellung

Ausstellung von Berechtigungszertifikaten (mit kurzen Laufzeiten)

← Bereitstellung

Sperrlisten für gestohlene/ verlorene Personalausweise

Inhalt

- Einführung
- Technik
- **Daten & Funktionen**
- Anwendungen
- Prozesse für Beantragung und Ausstellung
- Restrisiko
- Zusammenfassung

Datenfelder

		sichtbar	maschinenlesbar	Chip
1)	a) "IDD" für Personalausweis		x	x
	b) "ITD" für vorläufigen Personalausweis		x	
2)	Familienname und Geburtsname	x	x	x
3)	Vorname(n)	x	x	x
4)	Doktorgrad	x		x
5)	Geburtstag	x	x	x
6)	Geburtsort	x		x
7)	Lichtbild	x		x
8)	Unterschrift	x		
9)	Größe	x		
10)	Augenfarbe	x		
11)	Anschrift, bei Anschrift im Ausland die Angabe "keine Hauptwohnung in Deutschland“	x		x
12)	Staatsangehörigkeit	x		
13)	Abkürzung "D" für deutsche Staatsangehörigkeit		x	x
14)	Seriennummer	x	x	x
15)	Ordens- oder Künstlername	x		x
16)	letzter Tag der Gültigkeitsdauer		x	x
17)	Prüfziffern		x	
18)	Leerstellen		x	
19)	Fingerabdrücke, Bezeichnung der erfassten Finger, Angabe zur Qualität der Abdrücke			x

Übermittlung von Daten

- Daten, die immer an den eID-Service übermittelt werden, um zu überprüfen, ob ein abgelaufener oder gesperrter Ausweis vorliegt:
  - Dienste- und kartenspezifisches Sperrmerkmal
  - Ergebnis der Gültigkeitsprüfung des Ausweises
- Abrufbare personenbezogene Daten gemäß Berechtigungszertifikat:
  - Vor- und Familienname(n), Doktorgrad
  - Ordens-, Künstlername
  - Geburtstag und -ort
    - Angabe, ob ein bestimmtes Alter über- oder unterschritten ist
  - Anschrift , Wohnort-ID
    - Angabe, ob Wohnort mit bestimmten Wohnort übereinstimmt
  - Dokumentenart („Personalausweis“) und ausstellendes Land („D“)
  - Dienste- und kartenspezifisches Kennzeichen für den pseudonymen Zugang

PIN – Personal Identification Number (Geheimnummer)

- **Funktion**
  - Auslieferung mit einer 5-stelliger Transport-PIN (Aktivierungscode)
  - Ändern in eine neue 6-stellige Geheimnummer bei erstmaliger Nutzung
  - Dient der Freigabe der Datenübermittlung im Rahmen des elektronischen Identitätsnachweises

- **Ändern**
  - Mit Kenntnis der aktuellen Geheimnummer jederzeit an einem für den elektronischen Identitätsnachweis ausgestatteten Computer
  - Ohne Kenntnis der aktuellen Geheimnummer in der Personalausweisbehörde nach vorhergehender Identifizierung des Ausweisinhabers

- **Falscheingabe der Geheimnummer**
  - Zweimalige Falscheingabe: Eingabe der Zugangsnummer, um den dritten Eingabeversuch freizuschalten
  - Dreimalige Falscheingabe: Eingabe der PUK (Entsperrnummer) → maximal zehn Mal nutzbar

PUK - Entsperrnummer

- **Funktion**
  - PUK (Personal Unblocking Key) ist zehnstellig
  - PUK wird zufällig erzeugt und Bestandteil des PIN-Briefes
  - dient dem Entsperren der eID-PIN und der Signatur-PIN nach dreimaliger Falscheingabe
  - eID-PIN und die Signatur-PIN sind jeweils mit einem Rücksetzzähler ausgestattet, die ein jeweils maximal zehnmaliges Zurücksetzen des Fehlbedienungszählers der eID- bzw. Signatur-PIN mit Hilfe des PUK erlauben

Zugangsnummer (CAN = Card Access Number)

- **Funktion**
  - Die Zugangsnummer ist eine auf der Vorderseite des neuen Personalausweis aufgedruckte sechsstellige dezimale zufällige Nummer (lässt sich nicht berechnen)
  - Dient der Absicherung gegen unberechtigten Zugriff auf die Kommunikation zwischen Personalausweis und Lesegeräten
  - Dient als Passwort für PACE für den Aufbau eines sicheren Kanals zwischen Ausweis und Kartenlesegerät, wenn die eID-PIN nicht erforderlich ist, z.B.:
    - hoheitliche Kontrolle, Visualisierung der Ausweisdaten in der Meldebehörde
    - Änderungsdienst in den Ausweisbehörden
    - Nachweis, dass Ausweis physisch vorliegt für Signaturanwendung
  - Dient zum Freischalten eines dritten Eingabeversuch der eID-PIN
  - Die Zugangsnummer besitzt keinen Fehlbedienungszähler
  - Die Zugangsnummer ist nicht eindeutig und keine Identitätsnummer

Pseudonymer Zugang

- **Funktion**
  - Dienst- und kartenspezifisches Kennzeichen, dient als Wiedererkennungskennzeichen
  - PA-Chip erzeugt Pseudonym aus der eindeutigen Kennung des Dienstes im Berechtigungszertifikat und einem chip-individuellen gespeicherten Geheimnis (dem privaten Schlüssel für Restricted Identification)
  - Pseudonym ist eindeutig pro neuer Personalausweis & Dienst, verhindert so Nutzerprofilbildung
  - Ändert sich bei Ausstellung eines neuen Personalausweises

- **Anwendungsgebiete**
  - Wiedererkennung eines Personalausweises ohne erneute Übermittlung der personenbezogenen Daten
  - Pseudonymer Zugang zu Dienstleistungen, die keine personenbezogenen Daten benötigen (z.B. bei Downloaddiensten)

Altersbestätigung

- **Funktion**
  - Überprüfung eines Mindestalters ohne Preisgabe des Geburtsdatums
    - Diensteanbieter prüft ob Personalausweisinhaber vor einem bestimmten Datum geboren wurde
    - Dienstanbieter sendet Testdatum
    - Wenn das Geburtsdatum früher oder gleich dem Testdatum ist, dann antwortet der neue Personalausweis positiv („true“).
  - Altersabfrage ist pro Eingabe der Geheimnummer nur einmal möglich

- **Anwendungsgebiete**
  - Zugangsbeschränkungen und altersabhängige Inhaltsfilterung

Wohnortbestätigung

- **Funktion**
  - Überprüfung ob ein angegebener Wohnort dem tatsächlichen Wohnort entspricht – ohne Preisgabe der Adresse
    - Prüfung ob Ausweisinhaber an einem bestimmten Wohnort gemeldet ist
    - Diensteanbieter sendet vollständigen oder Teile des Amtlichen Gemeindeschlüssels (Ländercode, Bundesland, Regierungsbezirk, Stadt/Landkreis, Gemeinde), Ausweis meldet bei einer Übereinstimmung „true“ zurück, ansonsten „false“
  - Wohnortabfrage ist pro Eingabe der Geheimnummer nur einmal möglich
- **Anwendungsgebiete**
  - Anbieter kann Dienste ortsbezogen einschränken, z.B. auf Einwohner eines bestimmten Bundeslandes
- **Weitere Möglichkeiten zur Ermittlung des Wohnorts**
  - Wohnort kann aus der Anschrift ermittelt werden
  - Amtlicher Gemeindeschlüssel kann direkt ausgelesen werden

Inhalt

- Einführung
- Technik
- Daten & Funktionen
- **Anwendungen**
- Prozesse für Beantragung und Ausstellung
- Restrisiko
- Zusammenfassung

Mögliche Anwendungen

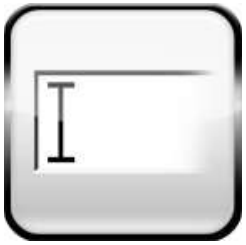
Zugang mit Pseudonym

Altersverifikation

Bürgerdienste

Kiosksysteme / Infoterminals

Automat. Formularbefüllung



Elektronische Signatur

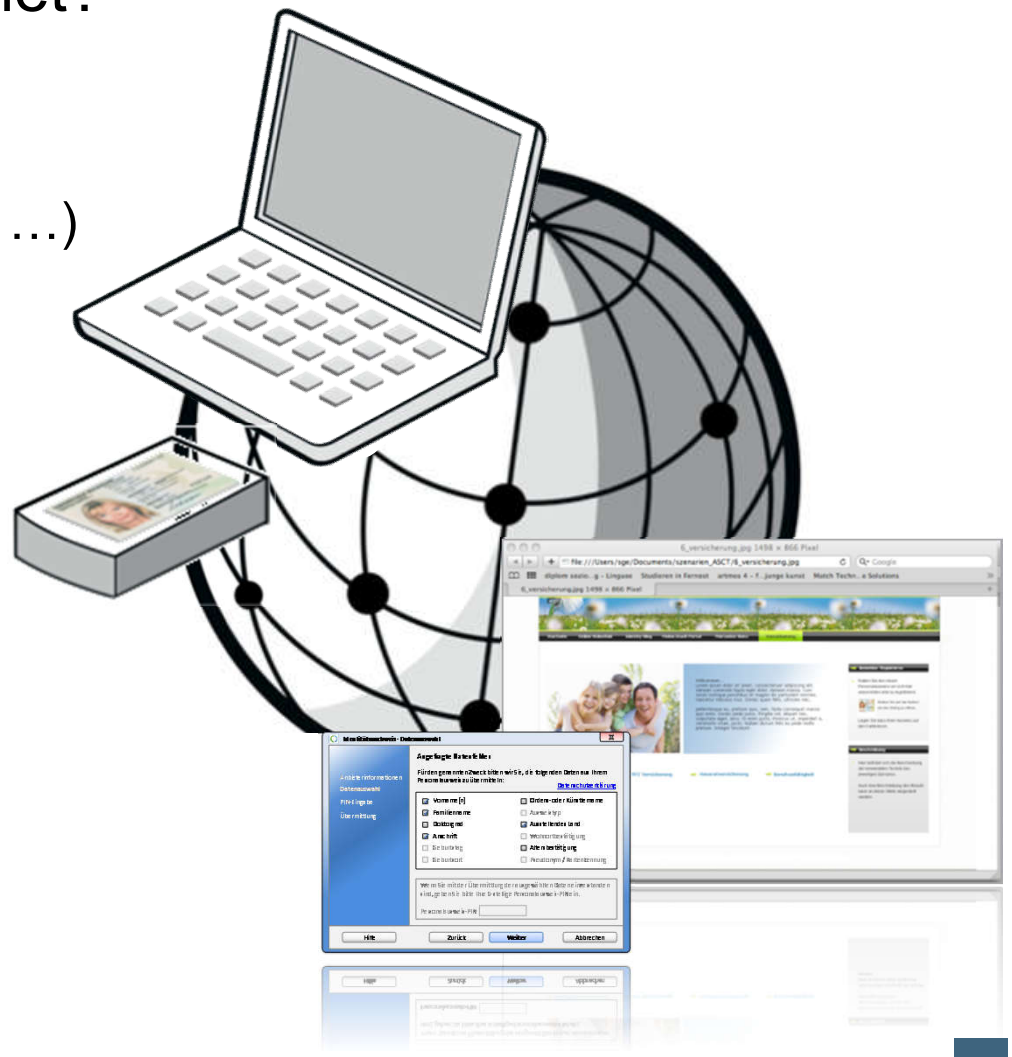
Online-Registrierung

Zutrittskontrollen

Barrierefreie Internetdienste

Erforderliche Komponenten

- Welche Komponenten benötigt der Bürger für das Ausweisen im Internet?
  - Computer (PC, Notebook, Smartphone, …)
  - Internetbrowser
  - Internetanbindung
  - Nutzer-Software
  - Kontaktloses Kartenlesegerät
  - Neuer Personalausweis



Nutzungsvoraussetzungen für die eID-Funktion

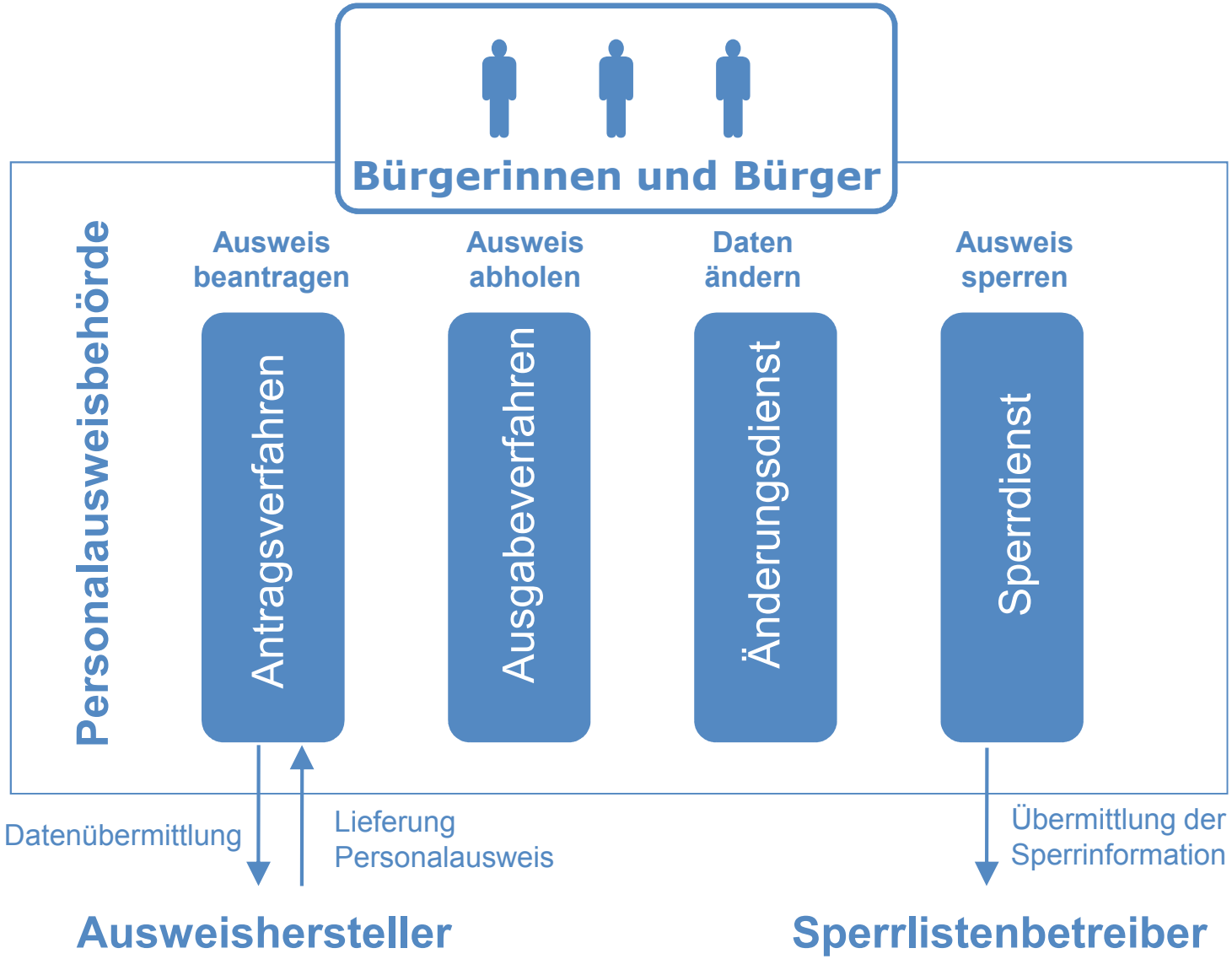
- **Auf Seiten des Bürgers**
  - Der neue Personalausweis mit aktivierter eID-Funktion
  - Kontaktloser Kartenleser (ISO14443)
    - Klasse-1-Leser ohne PIN-Pad für eID-Anwendung („Standardleser“)
    - Klasse-3-Leser mit PIN-Pad für eID-Anwendung und Signaturanwendung („Komfortleser“)
  - Nutzer-Software (z.B. Identitätsnachweis)
  - Browser
- **Auf Seiten des Dienstanbieters**
  - Berechtigungszertifikat
  - Anbindung an eID-Server
  - Integration in eigenes Dienstangebot

Inhalt

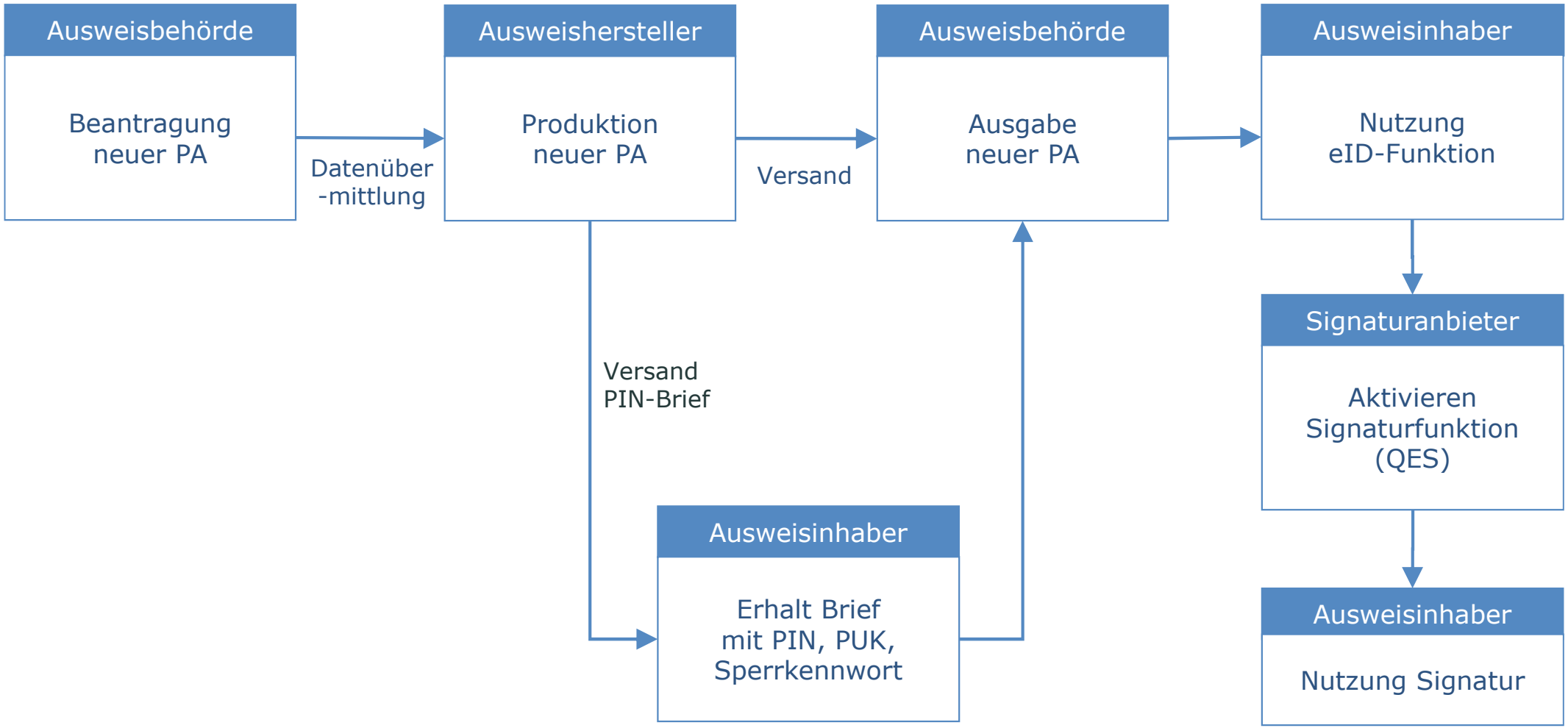
- Einführung
- Technik
- Daten & Funktionen
- Anwendungen
- **Prozesse für Beantragung und Ausstellung**
- Restrisiko
- Zusammenfassung

Prozesse für den neuen Personalausweis

PA beantragen/abholen/ändern/Daten anzeigen und sperren



Rollen im Beantragungs- und Ausgabeprozess



Aufgaben der Personalausweisbehörden

- Speicherung des Sperrkennwortes im Personalausweisregister
- Quittierung Empfang des Sperrkennworts und des Ausweisdokuments gegenüber Ausweishersteller
- Sichere Verwahrung des neuen Personalausweis bis zur Abholung
- Entgegennahme der Sperr- und Entsperraufträge von Ausweisinhabern
  - Dokumentierung Zeitpunkt der Sperrung/Entsperrung
  - Aktualisierung des Sperrstatus im Personalausweisregister
  - Auskunft an Bürgerinnen/Bürger über Sperrstatus und Sperrkennwort
- Übermittelung Sperrhash für Sperrung, Entsperrung oder Sperrauskunft an den Sperrlistenbetreiber

Neue Abläufe in den Personalausweisbehörden

Beantragung

- Erfassung und Qualitätssicherung des Gesichtsbildes
- Ggf. Erfassung und Qualitätssicherung der Fingerabdrücke
- Elektronische Übermittlung aller Ausweisantragsdaten
- Versand PIN/PUK
- Ausgabe des Informationsmaterials zu den neuen Funktionen (insb. eID-Funktion)
- Schriftliche Bestätigung des Empfangs des Informationsmaterials durch Antragsteller

Ausgabe

- Ausgabe des Personalausweises
- Schriftliche Erklärung bzgl. Erhalt des PIN/PUK-Briefes
- Schriftliche Erklärung ob eID-Funktion genutzt werden soll
- Ggf. Ausschalten der eID-Funktion im Chip und Speichern dieser Tatsache im lokalen PA-Register
- Nutzung eines PA-Lesers zum Anzeigen der im Chip gespeicherten Daten
- Löschung der Fingerabdrücke spätestens bei Abholung des Ausweises

Änderungsdienst

- Ein- und Ausschalten der eID-Funktion im Chip
- Änderung der Geheimnummer
- Änderung der Anschrift im Chip und Aufkleber auf Personalausweis, Speicherung im Melderegister

Sperrdienst

- Übermittlung des Sperrkennwortes vom Ausweishersteller zur PA-Behörde
- Speicherung des Sperrkennwortes im PA-Register
- Bei Abhandenkommen eines Ausweises mit eingeschalteter eID-Funktion und im Sterbefall: Übermittlung der Sperrinformation an den Sperrlistenbetreiber und Speicherung dieser Tatsache im PA-Register
- Bei Meldung des Wiederauffindens: Veranlassung der Entsperrung im Sperrregister

Sperrmöglichkeiten

Bürger

Sperr-/Entsperrmeldung nach Identifizierung

Sperrmeldung unter Angabe Name, Vorname, Geburtsdatum und Sperrkennwort

Sperrmeldung unter Angabe Name, Vorname, Geburtsdatum, Sperrkennwort

Ausweisbehörde (Berechnung Sperrhash)

BürgerService 0180-1-33 33 33* (Berechnung Sperrhash)

Sperr-Notruf 0180-1-33 33 33* (Berechnung Sperrhash)

Sperrung/ Entsperrung mit Sperrhash

Sperrung mit Sperrhash

Sperrung mit Sperrhash

Sperrlistenbetreiber

Sperrliste mit allgemeinen Sperrmerkmalen

Zertifizierungs-diensteanbieter

Abgleich dienste- und kartenspez. Sperrmerkmal

Sperrliste

Dienstespezifische Sperrliste

Diensteanbieter

* 3,9 ct/min aus dem deutschen Festnetz, max. 42 ct/min aus dem deutschen Mobilnetz, auch aus dem Ausland erreichbar

Sperrmanagement

Sperrung (persönlich, auch telefonisch)

- Feststellen der Identität
- Dokumentation des Zeitpunkts der Sperrmeldung
- Auslösen der Sperrung durch Übermittlung der Sperrinformation an Sperrlistenbetreiber (§ 10 Abs. 5 PAuswG) und Protokollierung des Zeitpunkts
- Empfang Erfolg bzw. Misserfolg vom Sperrlistenbetreiber
- Information des Ausweisinhabers über die Sperrung
- Speichern der Tatsache, dass der Personalausweis gesperrt wurde, im Personalausweisregister (§ 23 Abs. 3 Nr. 17 PAuswG)

Entsperrung (nur persönlich)

- Feststellen der Identität
- Dokumentation des Zeitpunkts der Entsperrmeldung
- Auslösen der Entsperrung durch Übermittlung der Entsperrinformation an Sperrlistenbetreiber und Protokollierung des Zeitpunkts
- Empfang Erfolg bzw. Misserfolg vom Sperrlistenbetreiber
- Information des Ausweisinhabers über die Entsperrung
- Löschen der Tatsache, dass der Personalausweis gesperrt wurde, aus dem Personalausweisregister (§ 23 Abs. 3 Nr. 17 PAuswG)

Sperrprozess

Bürger

Sperr- / Entsperrmeldung nach Identifizierung

Ausweisbehörde
(Berechnung Sperrhash)

Sperre / Entsperre mit Sperrhash

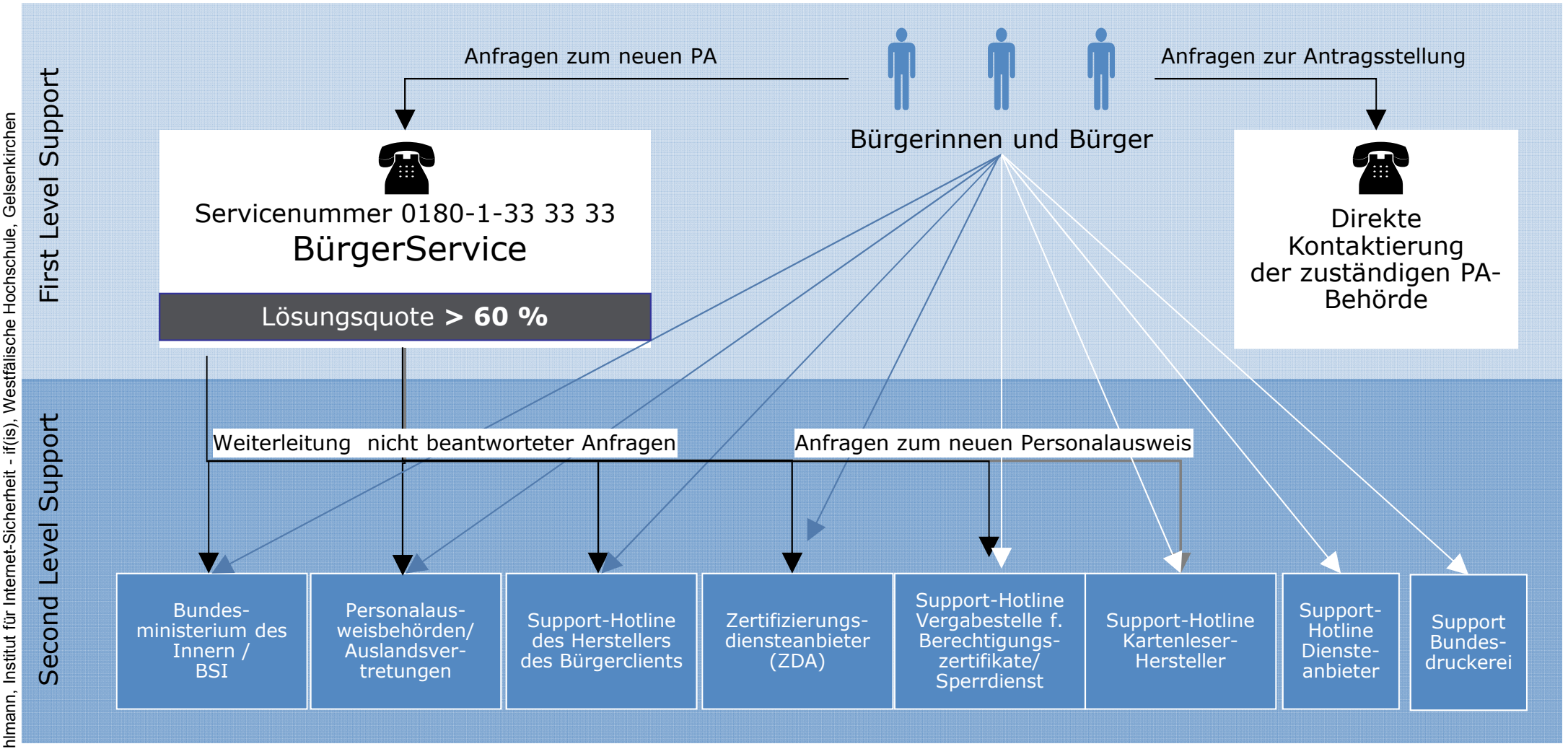
Sperrmeldung unter Angabe Name, Vorname, Geburtsdatum und Sperrkennwort

Sperr-Hotline
(Berechnung Sperrhash)

Sperre mit Sperrhash

Sperrlistenbetreiber

Bürgerservicezentrum/Bürgerhotline



Standardverfahren: Über BürgerService
Nicht-Standardverfahren: Über BürgerService
Standardverfahren: Direkt an Second Level Support
Nicht-Standardverfahren: Direkt an Second Level Support

Inhalt

- Einführung
- Technik
- Daten & Funktionen
- Anwendungen
- Prozesse für Beantragung und Ausstellung
- **Restrisiko**
- Zusammenfassung

Restrisikobereich (1)
→ Kartenlesegeräte

- 3 Kategorien an Lesegeräten für den nPA (BSI TR 03119)
  - Basisleser (Cat-B)
  - Standardleser (Cat-S)
  - Komfortleser (Cat-K)

Logo für zertifizierte Lesegeräte

Merkmal	Basisleser	Standardleser	Komfortleser
Kontaktlose Schnittstelle	x	x	x
Kontaktbehaftete Schnittstelle	o	o	x
Pinpad	o	x	x
Zweizeiliges Display	o	o	x
Qualifiz. Signatur	–	–	x

Restrisikobereich (1)
→ Restrisiko: Basisleser (1/2)

- **Risiko: Abgriff der geheimen PIN**
  - Bei Lesegeräten ohne Pinpad (Basisleser) UND
  - Infektion des PCs mit Schadsoftware

➔ Eingabe der PIN am Pinpad eines Kategorie S- oder K- Lesegeräts (Standard- oder Komfortleser) viel sicherer!

Für die Online-Authentisierung sollten Lesegeräte mit sicherem Pinpad bevorzugt verwendet werden (Standard- und Komfortleser).

Restrisikobereich (1)
→ Restrisiko: Basisleser (2/2)

- **Bei bekannter PIN und aufliegendem nPA: Identitätsmissbrauch per entferntem Zugriff möglich!**

- **Ablauf der Online-Authentisierung kann automatisiert werden**
  - Vollständig bei Basislesern
  - Nur eingeschränkt bei Standard- und Komfortlesern (PIN-Eingabe muss manuell erfolgen!)

Standard- und Komfortleser schützen nicht nur vor dem Auslesen der PIN am PC, sondern darüber hinaus auch vor einem automatisierbaren Missbrauch der Online-Authentisierung.

Restrisikobereich (1)
→ Die Vorteile des Komfortlesers

- Der Komfortleser verfügt zusätzlich über ein Display und unterstützt die QES
- Authentisierungs-Gegenstelle wird verlässlich im Display angezeigt
- Darstellung von Berechtigtem und den Berechtigungen ist **authentisch**
- Erfordert die **manuelle Interaktion** (PIN-Eingabe) des Benutzers bevor eine Online-Authentisierung abgeschlossen werden kann

Restrisikobereich (1)
→ Empfehlungen beim Einsatz: Basisleser

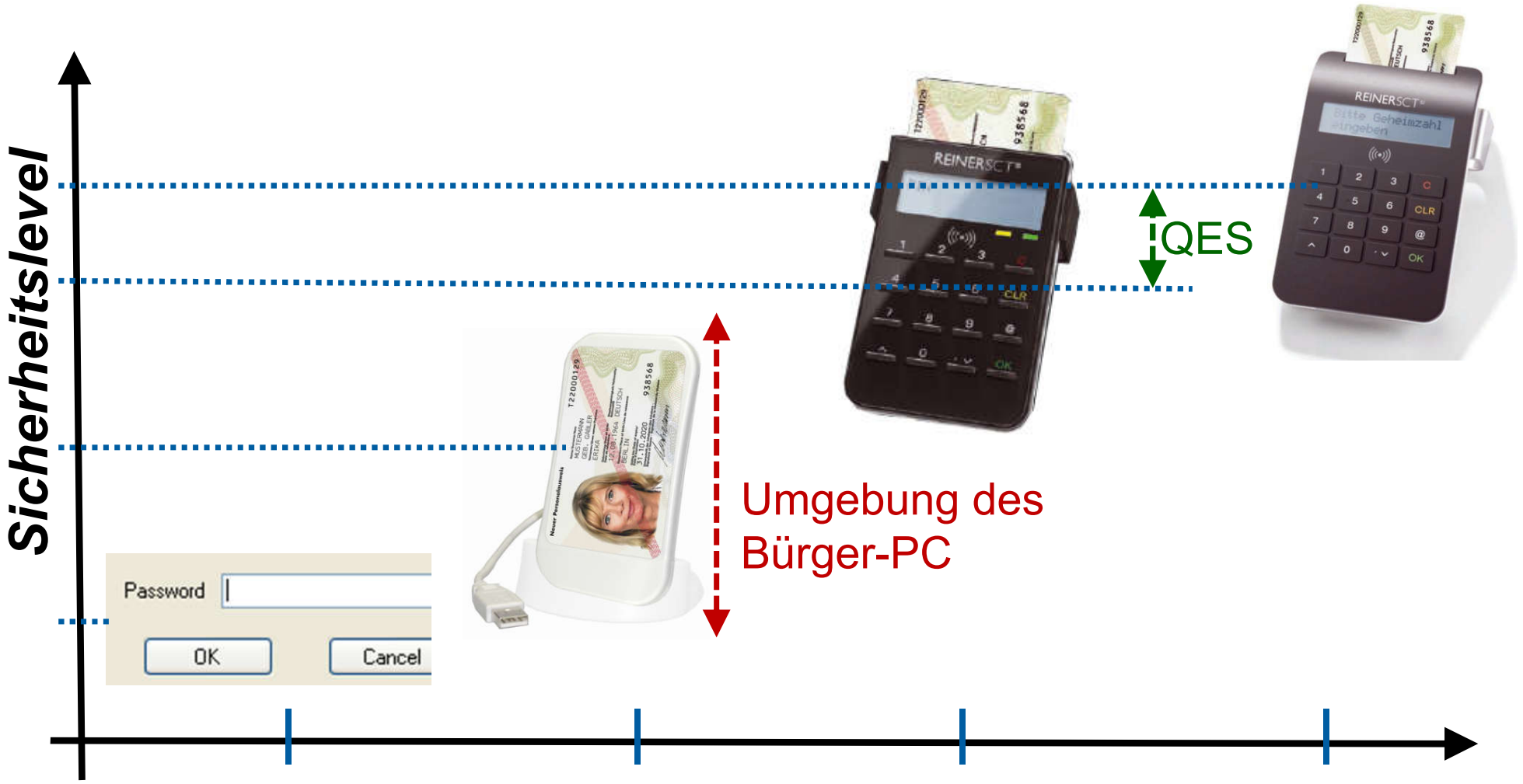
- Der Benutzer sollte eine **starke PIN** verwenden!
- Es sollte sichergestellt werden, dass der **nPA nur während einer Online-Authentisierung auf dem Lesegerät** aufliegt und danach vom Lesegerät genommen wird.
- Die Integrität und Vertrauenswürdigkeit des „Bürger-PCs“ muss mit gängigen Grundschutztechniken wie **Firewall, Antivirus-Programmen und Software-Updates** gewahrt werden.
- Der Benutzer sollte bei der Verwendung eines Basislesers durch ein **optisches und/oder akustisches Signal** darauf hingewiesen werden, dass eine Online-Authentisierung gestartet wird.

Vor der Installation der AusweisApp sollte die Integrität des PCs sichergestellt werden. Siehe auch: www.botfrei.de

Restrisikobereich (2)
→ Aufklärung (z.B. Missbrauch / Verlust)

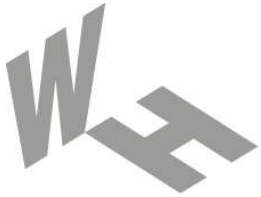
http://www.personalausweisportal.de

Einschätzung der Restrisiken
→ Sicherheitslevel



Zusammenfassung

- **Die eID-Funktion des neuen Personalausweis ist sicherer als Benutzername und Passwort!**
- Phishing-Angriffe werden bei der Verwendung der eID-Funktion sehr aufwändig!
- Standard- und Komfort-Leser sind deutlich sicherer als ein Basis-Leser!
- **Der Benutzer muss Kompetenzen entwickeln, um seinen Computer (PC, Notebook, Smartphone, …) sicher einzurichten, unabhängig vom neuen Personalausweis!**
- Wir brauchen eine höhere Sicherheit, um die neuen Möglichkeiten vertrauenswürdig nutzen zu können.
- Der nPA ist ein Schritt in die richtige Richtung!
- **Jeder sollte seinen Betrag dazu leisten, um die Zukunft sicher zu gestalten!**



Westfälische Hochschule
Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

Der neue Personalausweis

Vielen Dank für Ihre Aufmerksamkeit
Fragen ?

Prof. Dr. (TU NN)
Norbert Pohlmann

Institut für Internet-Sicherheit – if(is)
Westfälische Hochschule, Gelsenkirchen
http://www.internet-sicherheit.de

if(is)
internet-sicherheit.