# Einsatzmöglichkeiten der neuen elektronischen Personalausweise im Zutrittskontroll-Management






BOSCH

# Inhalt des Vortrags

Was ist ein Zutrittskontrollsystem?

Was kann ein elektronisches Ausweisdokument leisten?

Welche Voraussetzungen müssen erfüllt sein,
um Funktionen der elektronischen Ausweise zu nutzen?

Wo können elektronische Ausweisdokumente in Zukunft sinnvoll genutzt werden?

# Automatisierte und biometriegestützte Grenzkontrolle – ABG am Flughafen Frankfurt/Main

Vorstellung des ABG-Systems als Vertreter eines Zutrittskontrollsystems mit speziellen Merkmalen/Eigenschaften:

- Staatliche Behörde als Betreiber der Anlage
- Vereinzelung durch Schleusenprinzip
- Mögliche Nutzung integrierter RFID-Chips in Ausweisdokumenten zur Authentifizierung/Verifizierung von teilnehmenden Reisenden

# Zutrittskontrollsystem ABG - Schema einer Kontrollspur

**Schema einer Autocontrol-Spur:**

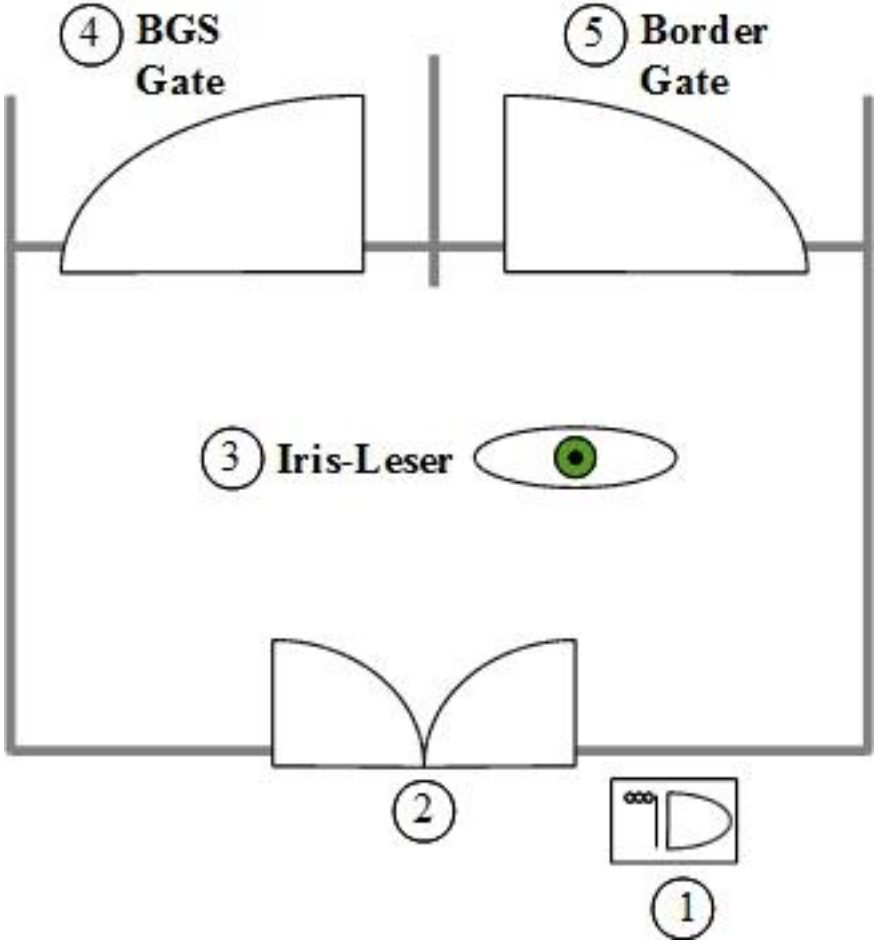
**Dokumentenleser (1)**

**Schleuseneingang (2)**

**Iris-Leser (3)**

**Kontrolltür zur manuellen Grenzkontrolle (4)**

**Freigabetür zum Grenzübertritt (5)**



# Zutrittskontrollsystem ABG - Foto einer Kontrollspur


ABG-System

# Digitale Daten auf dem Chip des nPA

1. **Sichtbar aufgedruckte personenbezogene Textdaten:**

   Familien- und Geburtsname, Vorname, Akademischer Titel, Tag und Ort der Geburt, Anschrift, Staatsangehörigkeit, Seriennummer, Ordens-/Künstlername, Daten der maschinenlesbaren Zone (MRZ)

2. **Weitere digitale Daten des Ausweis-Chips:**

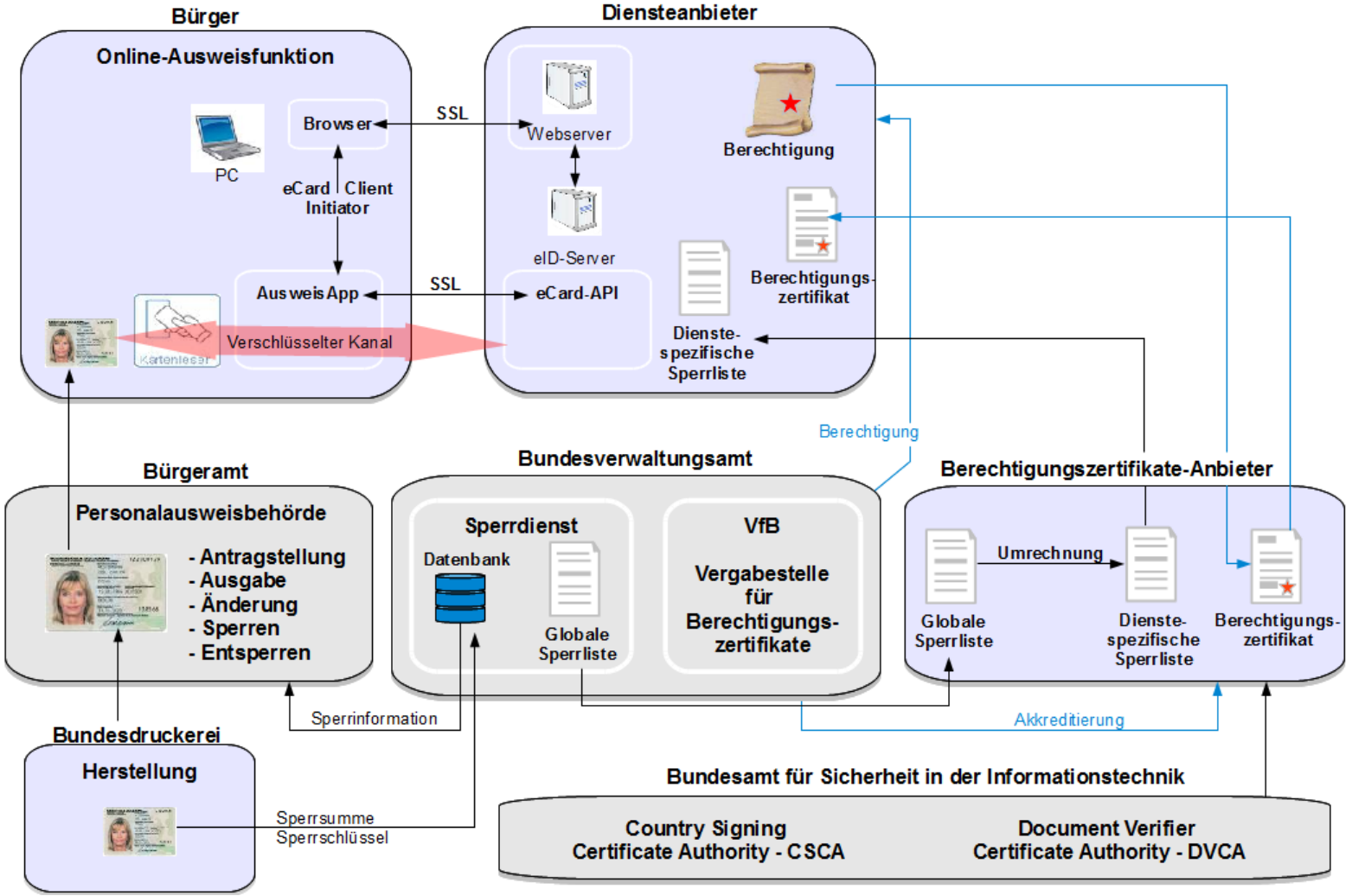
   Lichtbild, ggf. Fingerabdrücke, Daten zur Nutzung der Signaturfunktion (optional)





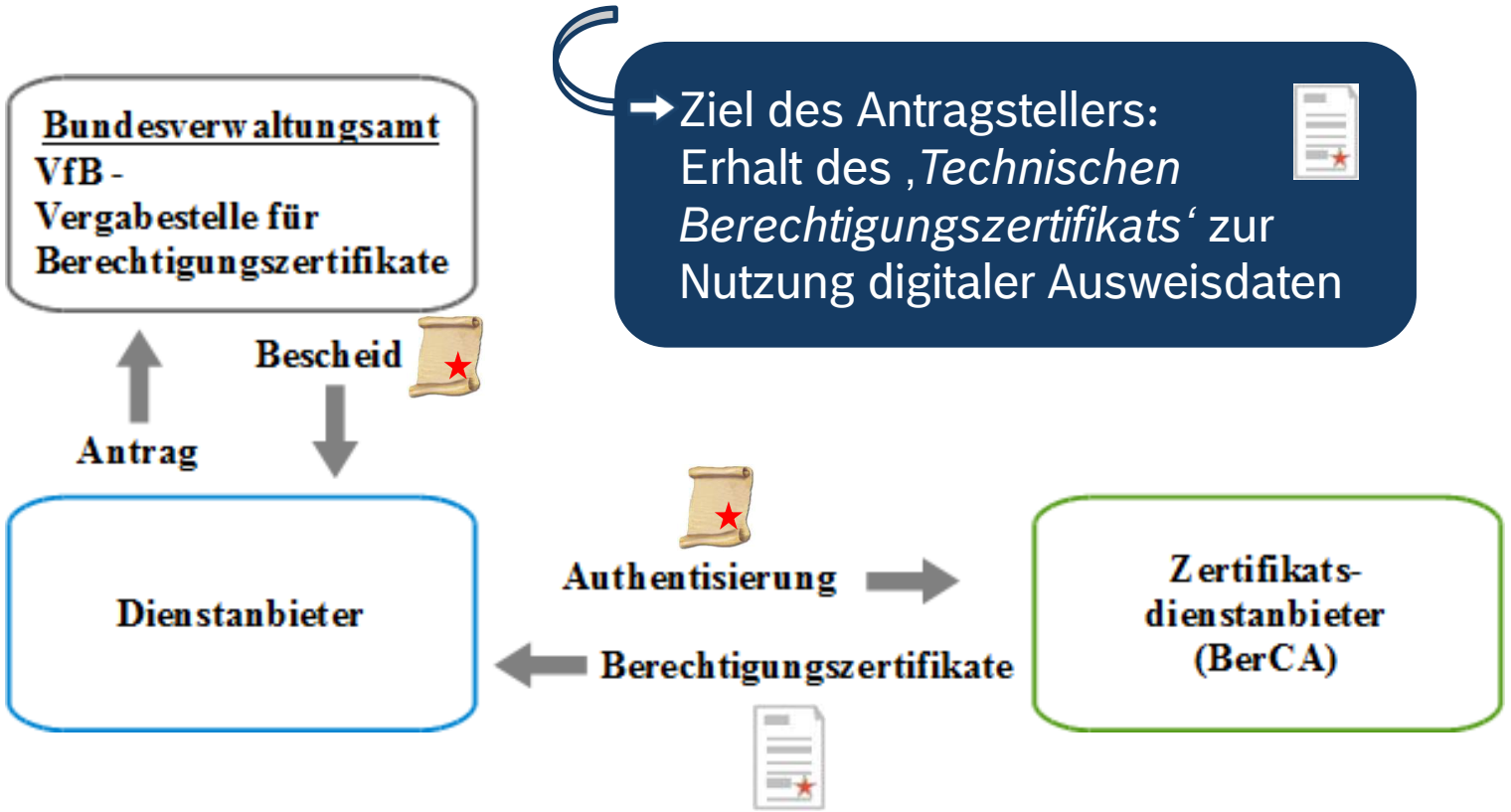
BOSCH

# Der neue elektronische Personalausweise - Infrastruktur-Übersicht



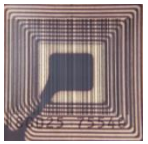

[Quelle: „Anwenderhandbuch für Wirtschaft und Verwaltung“, BMI Dez. 2010]

# Genehmigungsweg für Zertifikatausstellung




[Quelle: „Der Personalausweis – Anwenderhandbuch für Wirtschaft und Verwaltung“, Stand Dezember 2010, Herausgeber: Bundesministerium des Inneren]

# Grundfunktionen des Ausweis-Chips



**Grundfunktionen:**

1. **eID-Funktion (Elektronische Identität):**

   Online Identitätsnachweis zur sicheren gegenseitigen Authentisierung:

   u.a. Alters-und Wohnortverifikation, Pseudonym-Funktion

2. **Signaturfunktion:**

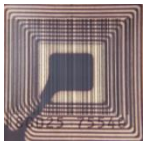
   Zum Abschluss rechtskräftiger Online-Verträge durch „Rechts-verbindliche Unterschrift“ (zusätzliches Signaturzertifikat nötig)





BOSCH

# Grundsätze für den Datenaustausch



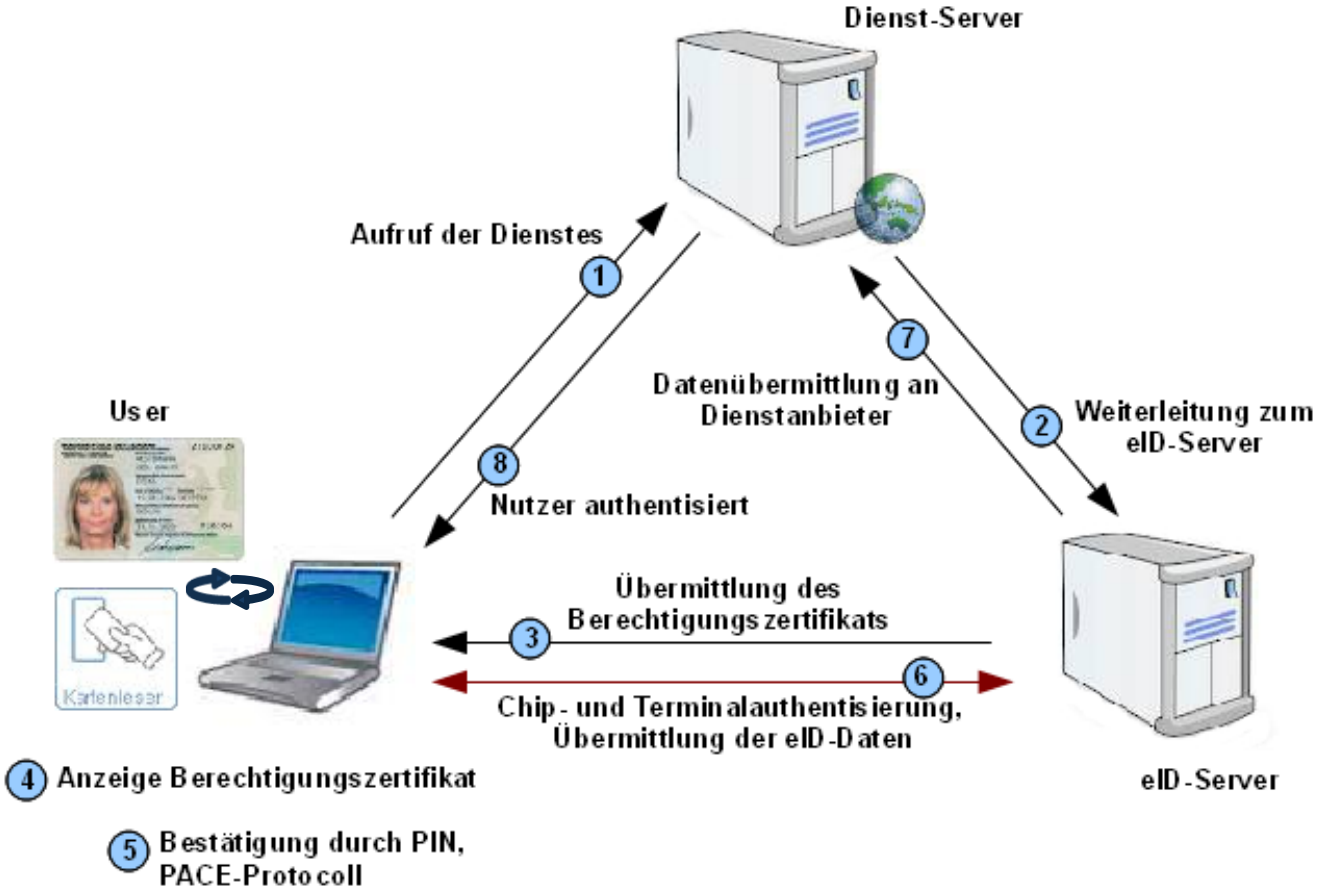
**Grundsätze:**

a) Online-Funktion des nPA muss durch Ausweisinhaber aktiviert sein

b) Anzeige der Datenschutzbestimmung, des Berechtigungszertifikats und welche Daten auf Basis des Zertifikats ausgelesen werden, inklusiver einer Aus-/Abwahlmöglichkeit

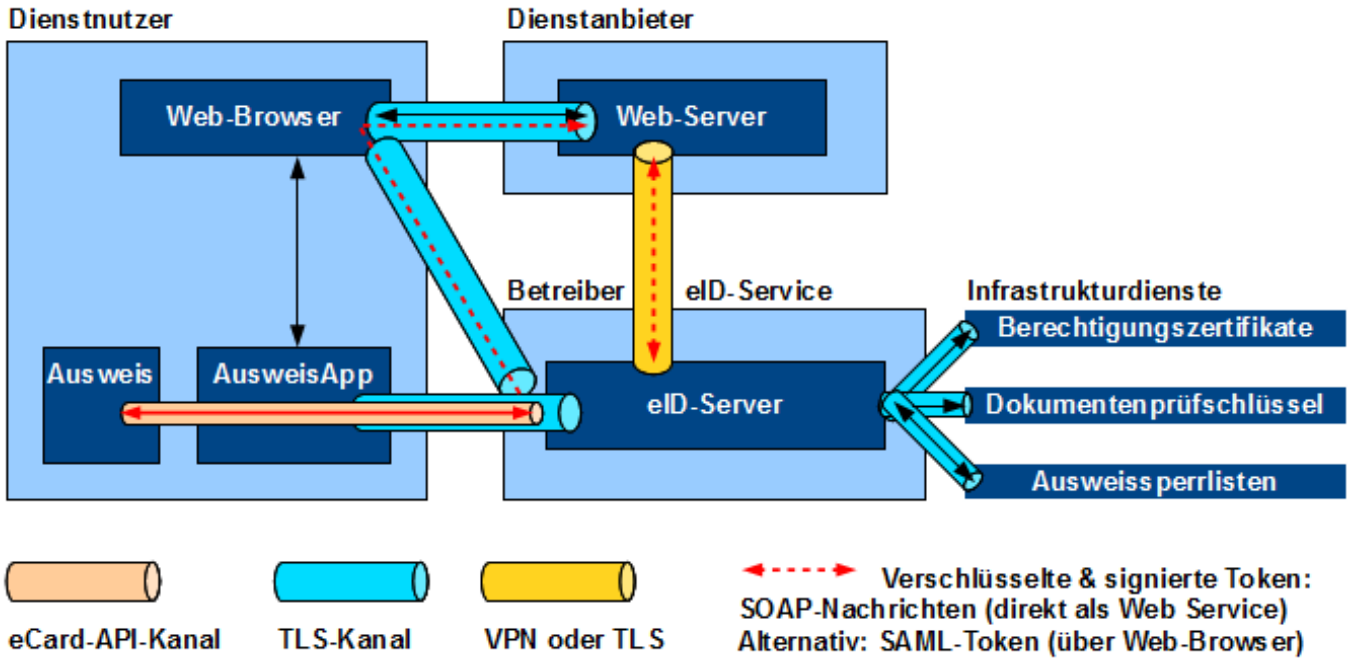
c) Übermittlung der Chip-Daten muss durch PIN-Eingabe (6-stellig) des Ausweisinhabers bestätigt werden

# Technischer Ablauf der Online-Authentisierung




[Quelle: "White Paper – Neuer Personalausweis – Einsatz in Automaten", Version 1.0 März 2011, Herausgeber: Bundesministerium des Inneren]

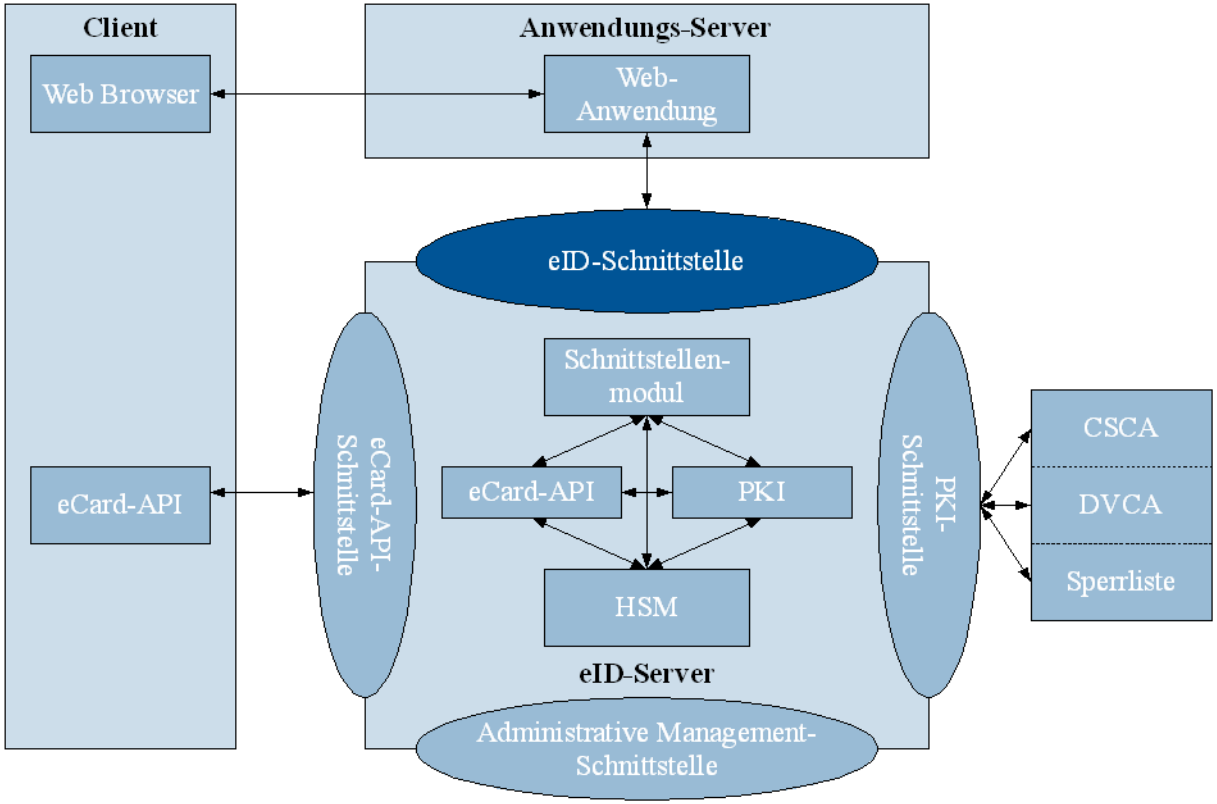
# Kommunikationsverbindungen bei Nutzung eines eID-Services




[Quelle: „White Paper – Neuer Personalausweis – Sicherheitsanforderungen für Dienstanbieter", Version 1.0 März 2011, Herausgeber: Bundesministerium des Inneren

TCP/IP-Modell

# Schnittstellen des eID-Servers




[Quelle: „Technische Richtlinie eID-Server“, kurz BSI TR-03130, Version 1.4.1 vom 08.10.2010, Herausgeber: Bundesamt für Sicherheit in der Informationstechnik ]

# Dienste- und Kartenspezifische Kennzeichnung – DKK

Der nPA unterstützt die Erzeugung einer dienste- und kartenspezifischen Kennzeichnung: dem **Pseudonym**.

Die **Pseudonym-Funktion** als Wiedererkennungszeichen benötigt:

- eine initiale Anmeldung des Users beim Dienstanbieter,
- die Berechnung des Pseudonyms aus der Dienstanbieterkennung *und* einem auf dem Ausweis-Chip gespeichertem Geheimnis und
- die Speicherung des Pseudonyms durch den Dienstanbieter.

Die Berechnung des Pseudonyms erfolgt durch *jeden* Dienstanbieter neu.

➡ Verhindert den direkten/einfachen Abgleich zweier Pseudonyme durch verschiedene Dienstanbieter





BOSCH

# Zutrittskontrolle mit der Pseudonym-Funktion des nPA

Zusammenfassung einiger Voraussetzungen und grundlegender Entscheidungen:

- Einhaltung zahlreicher gesetzlicher Bestimmungen: u.a. Datenschutz, Zertifikat-Bestätigung durch PIN-Eingabe…
- Gültige/s Berechtigungszertifikat/e
- Regelmäßige Aktualisierung der Sperrlisten und Zertifikate
- Entscheidung über Aufbau einer lokalen eID-Server-Infrastruktur oder Nutzung eines privaten eID-Service-Providers

# Zutrittskontrolle mit der Pseudonym-Funktion des nPA

Vorteile bei Aufbau einer lokalen eID-Server-Struktur:

a. Sichere Kommunikation ➡ eID-Service muss nicht zwingend im „öffentlichem“ Netz zugänglich sein

b. „Geringere laufende Kosten“ ➡ keine Highend-Produkte für Server nötig (Anmerkung: „Kostenfaktor“ ist vernachlässigbar)

c. Hoher Datenschutz durch Pseudonym-Funktion und durch weitere Datenverteilung auf mehrere Server

# Kosten privater eID-Service-Provider

- Ein vorläufiges Preismodell der Bundesdruckerei GmbH:

| **Einmalige Kosten** | | **Laufende Jahreskosten** | |
|---|---|---|---|
| Obligatorischer Testbetrieb: | 500 € | Bereitstellung eines Standardzertifikats: | 2000 € |
| Einrichtungsgebühr: | 500 € | Nutzungsgebühr für eID-Service mit max. 100.000 ePA-Zugriffen pro Jahr: | 5000 € |
| Telefon- und Mail-Support: | 1500 € | | |
| Gesamtkosten: | 2500 € | Gesamtkosten: | 7000 € |

- Kostengünstiges Modell der init-AG: Einmalige Kosten 750 € und laufende Jahreskosten ca. 3000 €.

[Quelle: http://blog.die-eid-funktion.de/2010/12/07/erste-preismodelle-von-eid-service-providern/ Titel „Erste Preismodelle von eID-Service-Providern“ 07.Dez. 2010, Zuletzt besucht am 06.12.2011]

# Zutrittskontrolle mit der Pseudonym-Funktion des nPA

Problematiken bei Nutzung der Pseudonym-Funktion in der Zutrittskontrolle:

a. Allgemeine Verbreitung des nPA in der BRD und in Europa

b. Mitarbeiter aus nicht EU-Staaten unberücksichtigt

c. Deaktivierter nPA des Arbeitnehmers/Ausweisbesitzers

d. Mischbetrieb aus herkömmlichen Kartentechnologien und elektronischen Ausweisdokumenten

# Zutrittskontrolle mit der Pseudonym-Funktion des nPA

Problematiken bei Nutzung der Pseudonym-Funktion in der Zutrittskontrolle:

e. Erhöhte Anforderungen an Kartenleser: Tastatur zur PIN-Eingabe und Dialogfeld zur Anzeige von Zertifikaten etc.

f. Verbindungsverlust zum Server mit aktuellen Sperrlisten- und informationen

g. Erhöhter Verwaltungs- und Arbeitsaufwand, z.B. durch regelmäßige Zertifikaterneuerung oder Hardware-Instandhaltung

# Zutrittskontrolle mit der Pseudonym-Funktion des nPA

Problematiken bei Nutzung der Pseudonym-Funktion in der Zutrittskontrolle:

h. Anbindung spezieller Systeme an öffentliche Netze kritisch: regelmäßige manuelle Aktualisierung der Sperrlisten über sichere dritte Kanäle erforderlich ➡ Verwaltungs- und Arbeitsaufwand

i. Kompatibilität zu alten Anlagen, in denen punktuell reine Offline-Leser eingesetzt werden ➡ Hard-/Software-Anforderungen

j. Allgemeine Akzeptanz der Bürger/Arbeitnehmer zur Nutzung elektronischer Ausweisdokumente

# Zusammenfassendes Fazit - Teil 1

- Anforderungen zur Nutzung des nPA in Zutrittskontrollsystemen sind technisch umsetzbar.
- Neue technische Entwicklungen werden die Akzeptanz zur Nutzung der nPA weiter einschränken: z.B.

  Integrierter **RFID-Chip** in modernem Smartphone (Stichwort „NFC-Handy“) und andere neue technische Lösungen.

- Vorteile: Komfortabel, höhere Nutzungs-Akzeptanz, Kompatibilität, weite Verbreitung, unabhängig von Staatsangehörigkeit

# Zusammenfassendes Fazit - Teil 2

Die **eID-Funktionen** des nPA werden *kein* Standard-Feature im Produkt „Zutrittskontrollsystem“ sein.

- Erzielter Nutzen im Geschäftsbereich „E-Business“ ist gering.
- Sinnvoller Einsatz z.B. beim Enrolment im System.
- Kosten für Groß-Projekte nicht relevant.

Weiterführende Szenarien im Geschäftsbereich „E-Government“ denkbar, da dort uneingeschränkter Zugriff auf alle Daten existiert, inklusive der Biometrie-Daten.

➡ Registrierung für ABG-Projekt mit nPA, automatisierte Grenzkontrollen für EU-Reisende mit gültigem nPA

Aussichten auf Bachelorarbeit…
…Testumgebung implementieren!

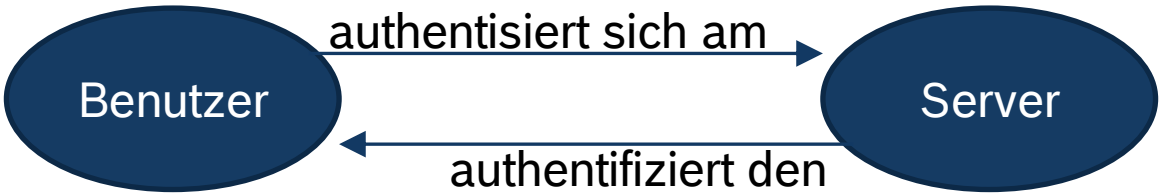
---

Vielen Dank!

Fragen?

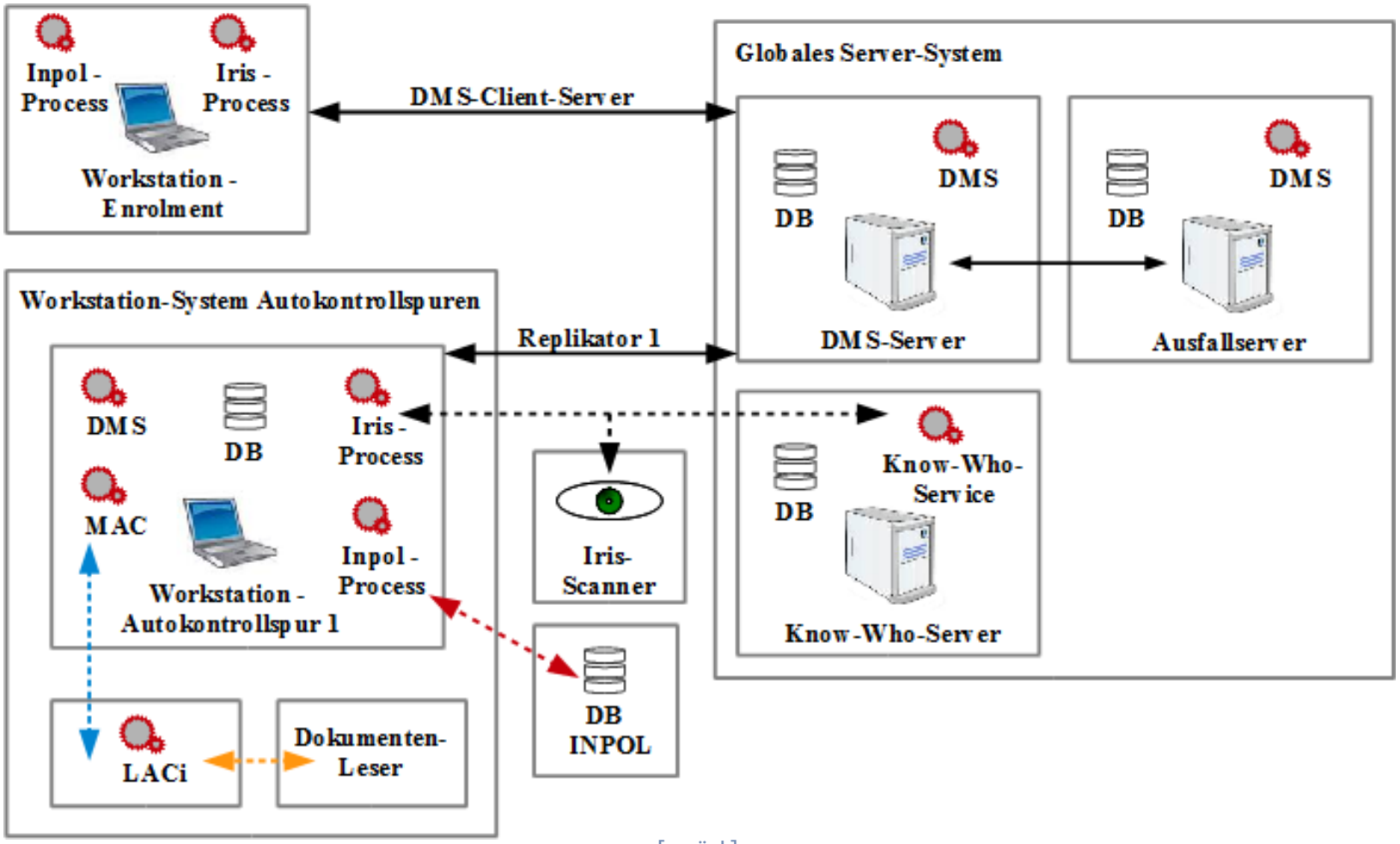
# Authentifizierung, Authentisierung und Verifizierung

**„Authentifizierung** (griechisch αυθεντικός *authentikós* ‚echt', ‚Anführer'; Stammform verbunden mit lateinisch *facere* ‚machen') ist der Nachweis (Verifizierung) einer behaupteten Eigenschaft einer Partei, die beispielsweise ein Mensch, ein Gerät, ein Dokument oder eine Information sein kann, und die dabei durch ihren Beitrag ihre **Authentisierung** durchführt. „
[Quelle: http://de.wikipedia.org/wiki/Authentifizierung, Jan. 2012]



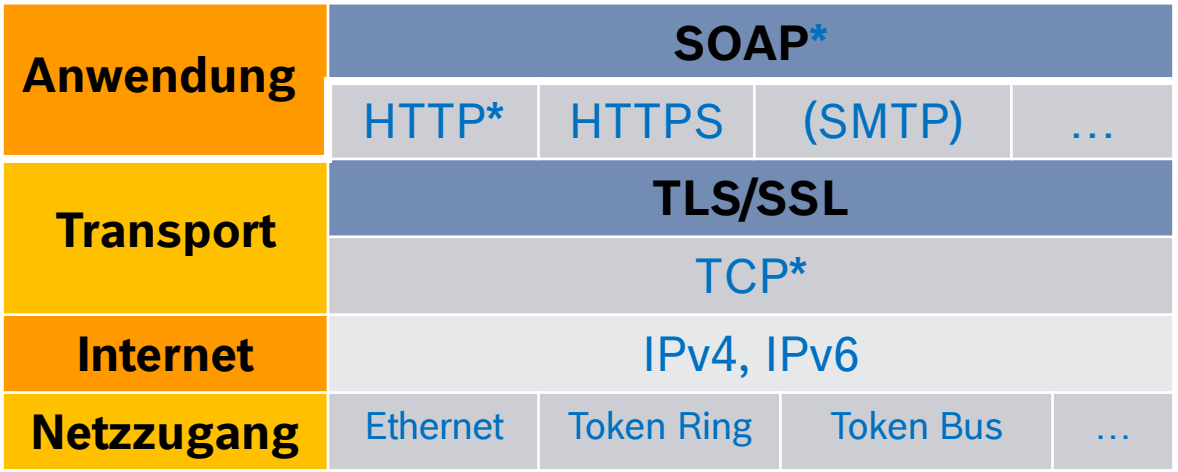

[zurück]

# Zutrittskontrollsystem ABG - Systemübersicht




[zurück]

# TLS und SOAP im TCP/IP-Referenzmodell




- SOAP (Simple Object Access Protocol): Netzwerkprotokoll, XML-Struktur
- TLS (Transport Layer Security): Verschlüsselungsprotokoll zur Datenübertragung

[zurück]