Fraunhofer FOKUS

Institut für Offene Kommunikationssysteme

Fraunhofer FOKUS

Offline eID-Systeme

Anwendungsbeispiel: Spielgeräte

Kompetenzzentrum Öffentliche IT

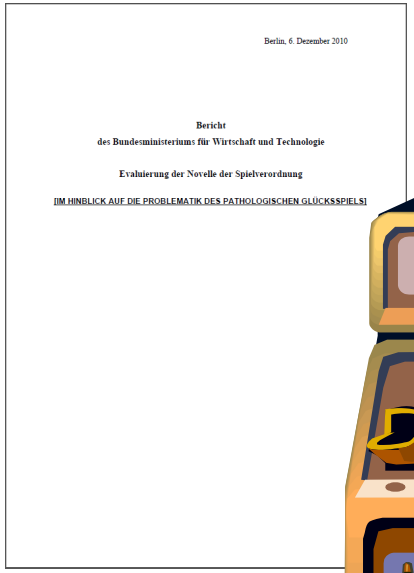
Fraunhofer FOKUS

Warum Spielgeräte?

- „Evaluierung der Novelle der Spielverordnung“ BMWi vom 8. Dezember 2010

- Ziele einer Spielerkarte
  - Jugendschutz
  - Verhinderung von Mehrfachbespielungen
  - Durchsetzung von Spielpausen
  - Einführung spielerbezogener Verlustgrenzen

- Physikalisch Technische Prüfanstalt des Bundes (PTB) prüft die technische Realisierung einer Spielerkarte


Berlin, 6. Dezember 2010

Bericht
des Bundesministeriums für Wirtschaft und Technologie

Evaluierung der Novelle der Spielverordnung

IM HINBLICK AUF DIE PROBLEMATIK DES PATHOLOGISCHEN GLÜCKSSPIELS

PTB

Spielerkartentypen

	Keine Gerätebindung	Gerätebindung
Keine Personenbindung	Modell A: Einfaches Kartenmodell	Modell B: Entwurf SpielV-Novelle
Personenbindung		Nicht praxisrelevant

Quelle: Prof. Richter, PTB, 2013

Vergleich der Kartentypen für eine Spielerkarte

	Modell A	Modell B SpielV-E	Modell C nPA	Modell C Datenspei-cherung
Kartenbindung	Keine Bindung	Gerätebindung	Spielerbindung	Spielerbindung
Herstellung	Beliebig	Gerätehersteller	Bundesdruckerei	Zu regeln
Ausgabe	Spielstätte	Spielstätte	Wie nPA	Autorisierte Stelle
Erforderlich technische Infrastruktur	Keine	Keine	Zertifikats-service für nPA	El. Spielgeräte-zertifikate, el. Zulassung, angepasster Vollzug, PKI-Anschluss
Karten-funktionen	Freischaltung	Freischaltung	Freischaltung	Freischaltung, Datenaufzeichn.
Wirkungen	Jugendschutz, Verhinderung des Parallelspiels	Wie Modell A + Pausen	Wie Modell A	Wie Modell A + Pausen, Spielerbezogene Grenzen

Quelle: Prof. Richter, PTB, 2013

Vergleich der Kartentypen für eine Spielerkarte - Fortsetzung

	Modell A	Modell B SpielV-E	Modell C nPA	Modell C Datenspei-cherung
Wirkungen	Jugendschutz, Verhinderung des Parallelspiels	Wie Modell A + Pausen	Wie Modell A	Wie Modell A + Pausen, Spielerbezogene Grenzen
Begleitende Absicherungen neben Bauart-zulassung	Kartenausgabe-/ Rüchnahme-regelung	Wie Modell A	Zertifikats-service für nPA	Schutz für - Spielerkarte - Spieldaten - el. Zulassung
Risiken	„Kartenschwarz-markt“, Fehlhandlungen in der Spielstätte, Kartenmissbrauch	Fehlhandlungen in der Spielstätte, Kartenmissbrach	keine	keine
Zusätzlicher Aufwand	Gering	Ja, deutlich höher als beim Modell A	(Soll untersucht werden)	Extrem hoch
Wirkungsgrad unter Beachtung der Risiken	Gering	Höher, da mehr Funktionen und weniger Risiken	Sehr hoch für Teilziele	Sehr hoch für alle Ziele

Quelle: Prof. Richter, PTB, 2013

Proof of Concept

Projektpartner

Begleitung und Beratung

Bundesministerium des Innern

Bundesamt für Sicherheit in der Informationstechnik

PTB

Projektsteuerung

Fraunhofer FOKUS

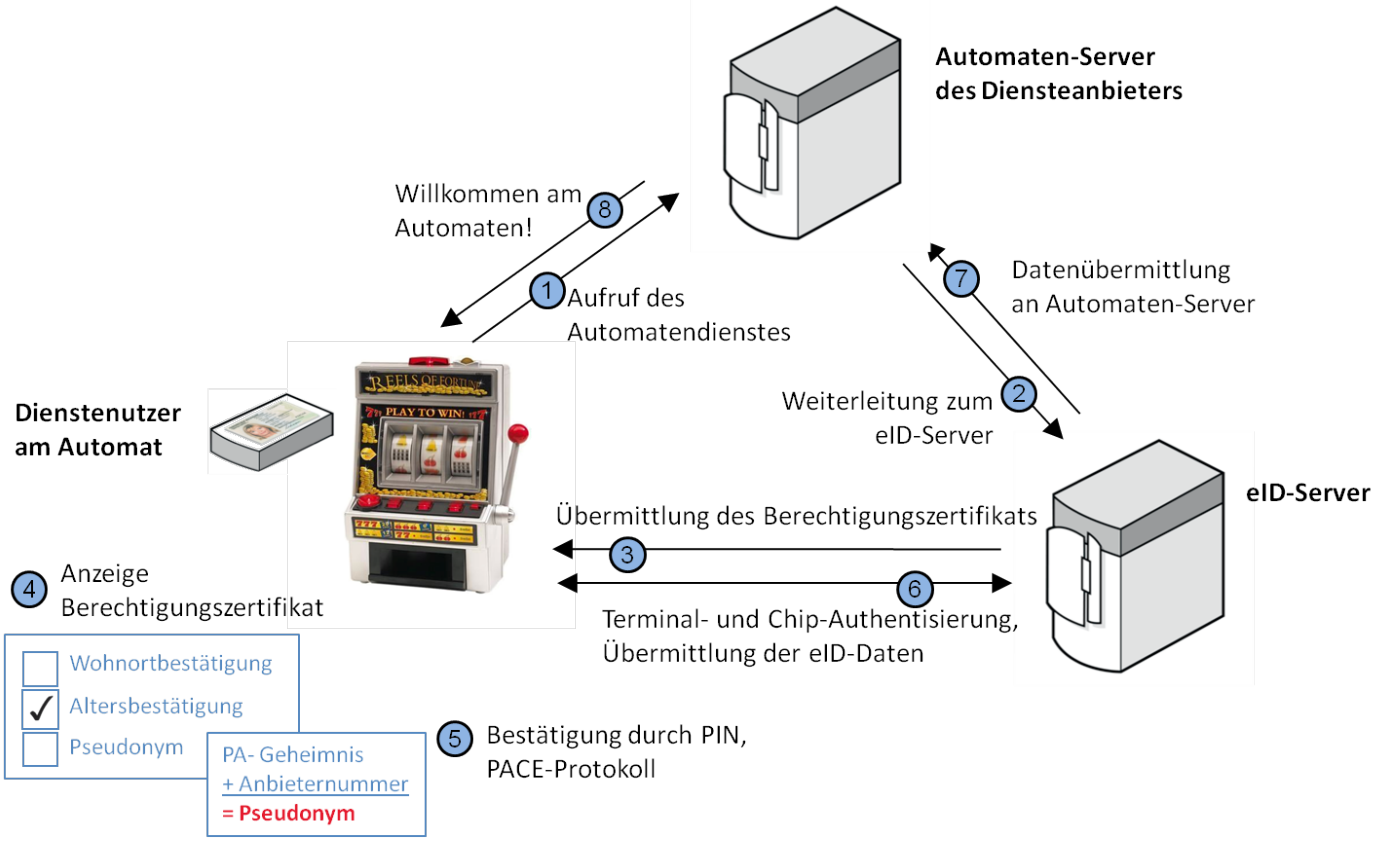
Ggf. weitere Partner

Diverse Spielgerätehersteller

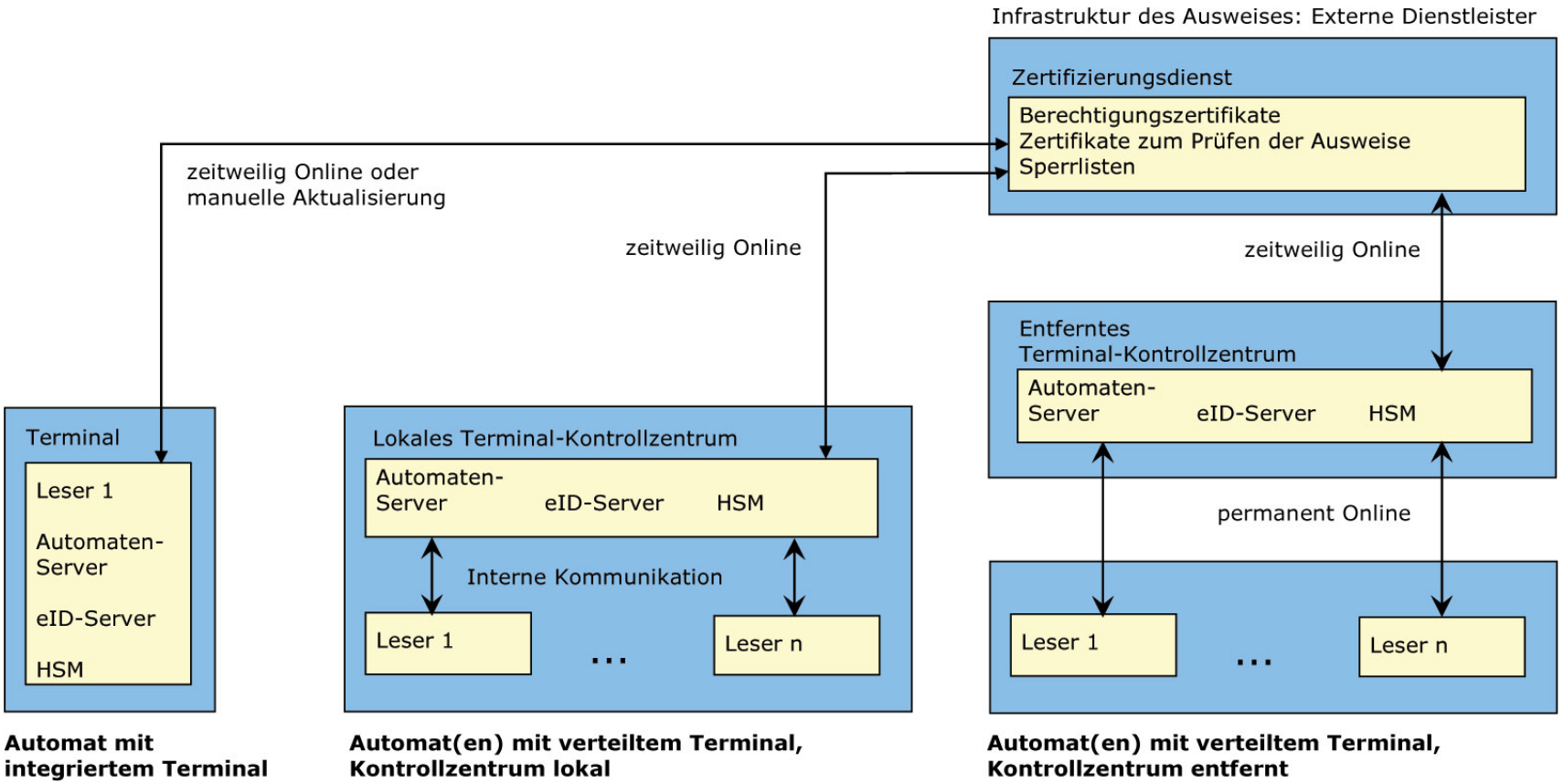
Use-Cases

- Altersverifikation
  - Jugendschutz 
- Eindeutige Identifikation
  - Verhinderung von Mehrfachbespielungen 
  - Prüfung ggü. Spielerdatei 
  - Durchsetzung von Spielpausen 
  - Einführung spielerbezogener Verlustgrenzen 

Technische Anbindung des nPA
Komponenten-basierte Sicht

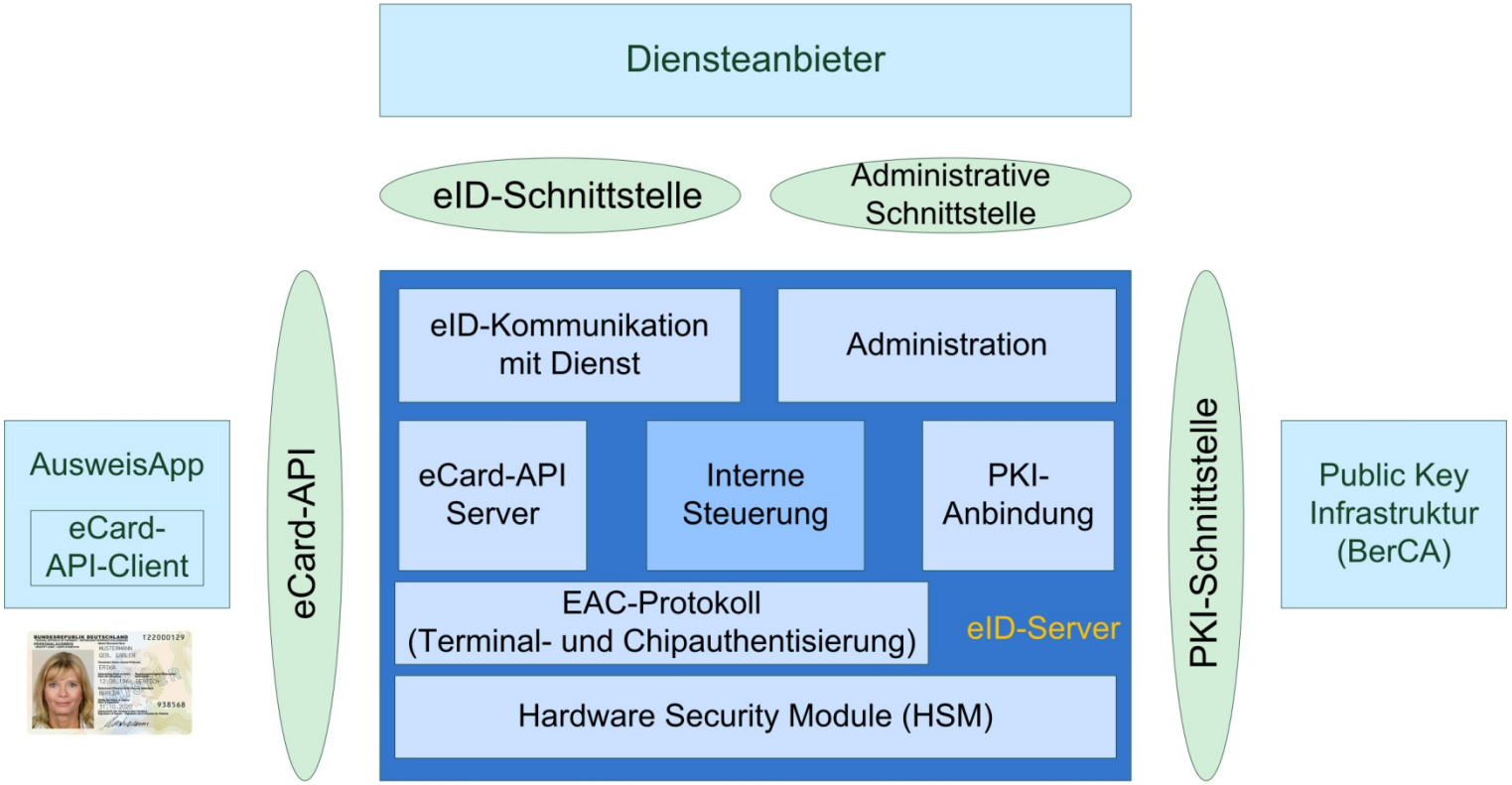


Möglichkeiten der Anbindung



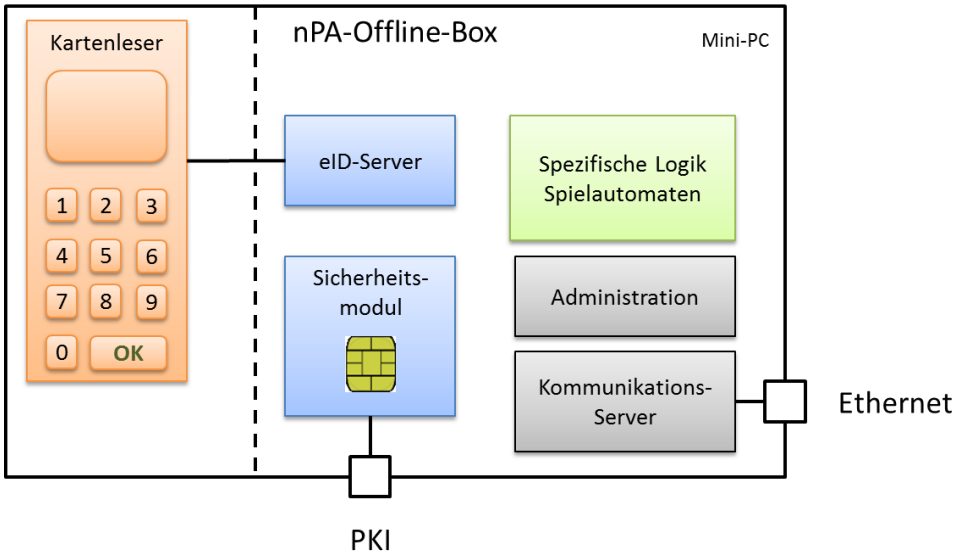
Architektur

eID-Server



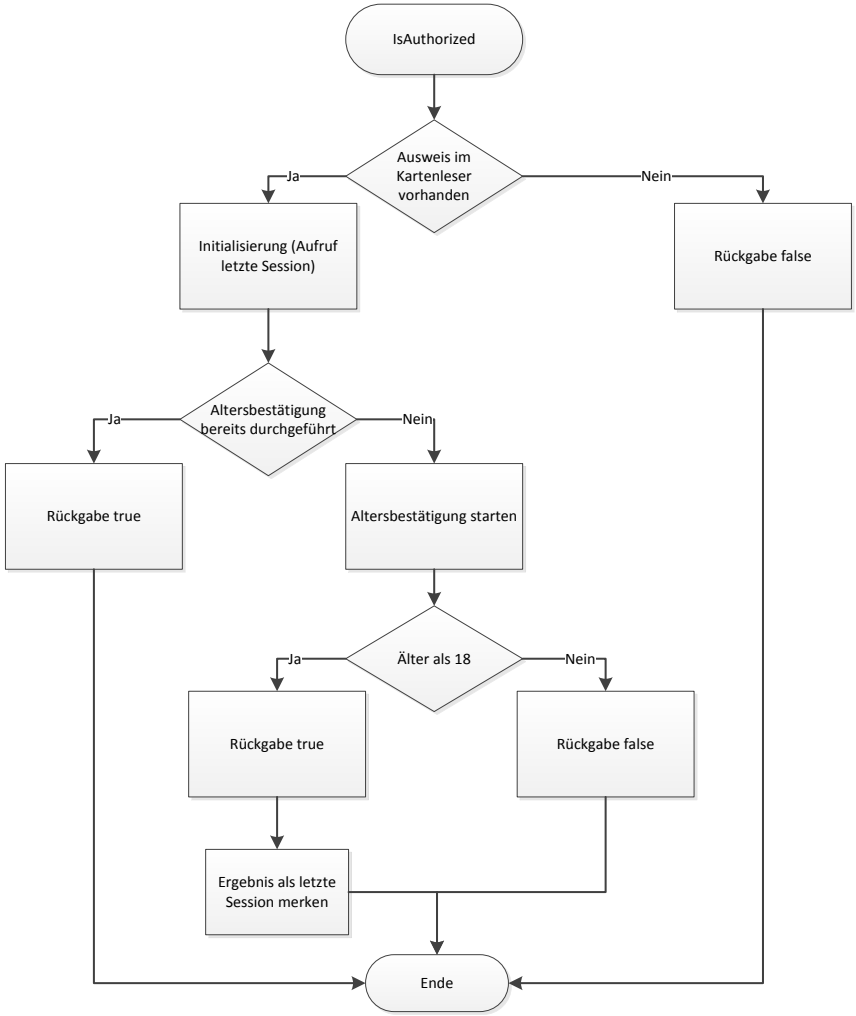
Technische Realisierung

- Kombiniert Sicherheitsanforderungen aus nPA & Spielgerät
  - Kein Eingriff in Logik des Spielgerätes
  - Minimale Schnittstelle
- Kapselung der nPA-Offline-Funktionalität in separate Hardware-Komponente
  - Inkl. Sperrlisten & Berechtigungszertifikat
  - Übernimmt Aufgaben eines eID-Servers und Clients
- Einfache Integration



Schnittstellen

- Ausschließlich PULL aus Sicht des Spielgerätes
- Ethernet mit einfachem ASCII-Protokoll
- Periodische Abfrage: isAuthorized
  - Altersverifikation
  - Mehrfachbespielung
- Zusätzlich Schnittstellen-Simulator für Entwickler



Spezifikation

- Automatenhersteller benötigt kein spezifisches Personalausweis-Wissen

Kommando	Rückgabewerte	Beschreibung
restart	**-**	Setzt die nPA-Offline-Box zurück in ihren Initialzustand. Diese Funktion ist ggf. relevant für Fehlerfälle. Diese Funktion liefert keinen Rückgabewert.
isAuthorized		Durchführung der Prüfung auf Spielberechtigung.
	true	Der Personalausweis steckt zum Zeitpunkt der Abfrage im Kartenleser. Die Altersverifikation gegen das Alter 18 wurde erfolgreich durchgeführt.
	false:n	Der Personalausweis ist nicht im Kartenleser vorhanden, die PIN wurde falsch eingegeben, der Ausweis ist gesperrt oder die Altersverifikation war nicht erfolgreich.
	error:m	Kommunikation zum Kartenleser nicht möglich, Berechtigungszertifikat ungültig oder ein sonstiger unvorhergesehener Fehler ist aufgetreten. (ggf. werden die möglichen Fehlerfälle mit Fehlercodes differenziert)
getDetails	**String**	Gibt eine Information zurück, warum der letzte isAuthorized-Aufruf 'false' oder 'error' zurück gab. Falls der letzte isAuthorized-Aufruf 'true' war, wird die Eindeutige Kennung des Ausweises (Restricted ID (RI)) zurückgegeben.
exit	**-**	Beendet die Verbindung zur nPA-Offline-Box. Diese Funktion liefert keinen Rückgabewert.

Erster Proof of Concept

- Für Showcases geeignet
- Mini-PC: Raspberry Pi
- Linux
- Kartenleser (Reiner SCT)
- Zunächst Soft-Zertifikate
- Fraunhofer Implementierung zur Anbindung des nPA (in C)
- Geeignet für weitere Offline-Szenarien

Wie geht es weiter?

- Weitere Anwendungsfälle für teilweise oder vollständige Offline-Systeme:
  - Ticketing
  - Paketzustellung
  - Automaten

Offene Fragen:

- Berechtigungszertifikate
  - Gültigkeit?
  - Aktualisierungsprozess?
    - Rollen, Mechanismen
  - Ausgestaltung des Sicherheitsmoduls

- Technische Richtlinie Offline eID?

Diskussion

Offene Fragen

Vielen Dank für Ihre Aufmerksamkeit!

Christian Welzel

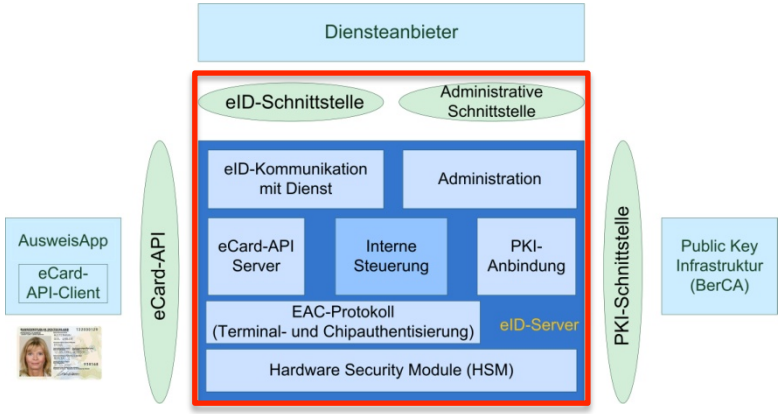
Fraunhofer FOKUS
Kaiserin-Augusta-Allee 31
10589 Berlin, Deutschland

Tel + 49 30 3463 7173
Fax + 49 30 3463 8000

www.oeffentliche-it.de
www.fokus.fraunhofer.de

Technische Richtlinien

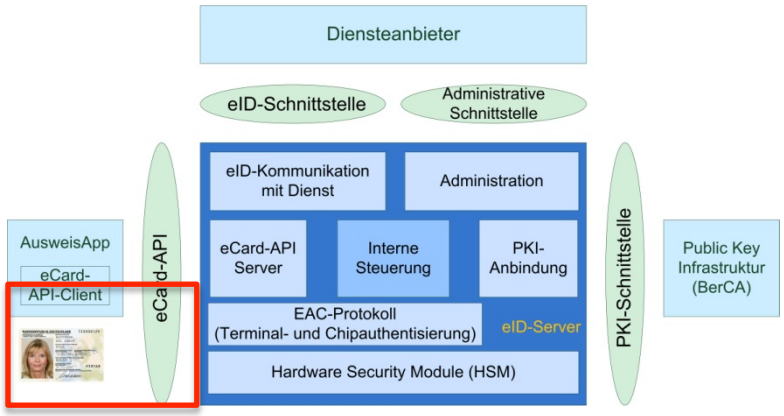
eID-Server



- TR-03130 eID-Server
  - TR-03130 "eID-Server"
  - Anbindung des eID-Service an (Web-)Anwendungen
  - Definiert Schnittstellen und Sicherheitsanforderungen an die Hard- und Software-Systeme des eID-Servers
  - Übernimmt die sichere Kommunikation mit der Client-Software, dem Personalausweis und dem PC der Bürgerinnen und Bürger
  - Stellt die Authentizität und die Gültigkeit des Personalausweises fest, prüft, ob dieser gesperrt wurde, und übermittelt die Ergebnisse der eID-Funktion an die weiteren Systeme des Diensteanbieters
  - Bezieht regelmäßig neue Berechtigungszertifikate sowie aktualisierte Sperrlisten
  - Pre-Shared Keys vom eID-Server für TLS-Verbindungen

Technische Richtlinien

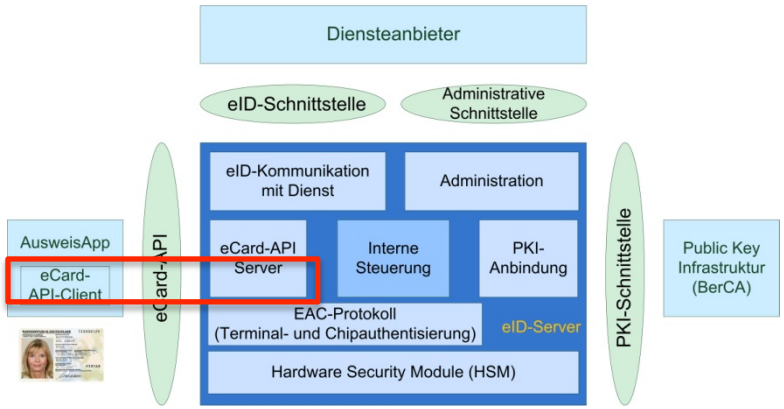
Architektur neuer PA, Tests



- TR-03127 Architektur
  - Architektur elektronischer Personalausweis und elektronischer Aufenthaltstitel
  - Daten und Funktionen, Zugriff auf Ausweisdaten
  - Ausweisausgabe, PIN und PUK
  - Hintergrundsysteme: Berechtigungs-PKI, Sperrlisten, Sperrmerkmal
- TR-03105 Konformitätstests
  - Conformity Tests for Official Electronic ID Documents
    - Part 3.3: "Test plan for eID-Cards with Advanced Security Mechanisms - EAC 2.0"
    - Part 5.2: "Test plan for eID-Card compliant Reader Systems with EAC 2.0"

Technische Richtlinien

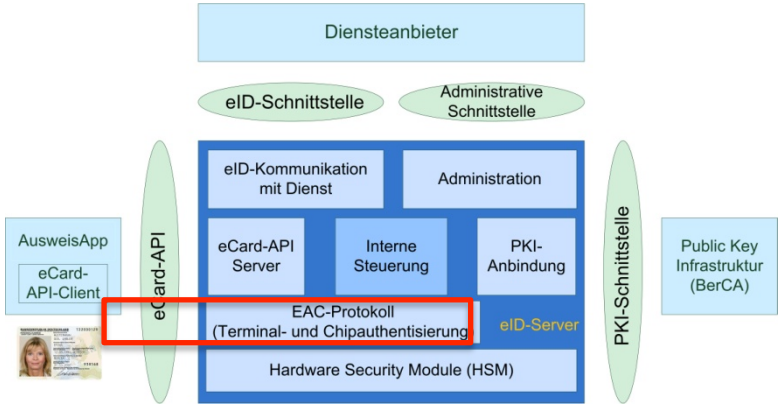
eCard API



- TR-03112 eCard-API
  - eCard-API-Framework (7 Teile, ca. 470 Seiten)
  - Web-Service-orientierte Schnittstelle für Karten der eCard-Strategie
  - Technische Basis für AusweisApp, eID-Server, Kommunikation
  - Nutzung an zwei Stellen: Client-Seite (auf dem PC des Bürgers) und auf Server-Seite (eID-Server des Diensteanbieters)
  - Ansteuerung Kartenleser, Durchführung der Sicherheitsprotokolle
    - Client-Software reagiert auf Authentisierungsanfragen via dem Browser des Nutzers
    - Verbindet sich mit der eCard-API-Schnittstelle des eID-Servers
    - Verbindung nutzt der eID-Server, um die Daten aus dem neuen Personalausweis zu lesen

Technische Richtlinien

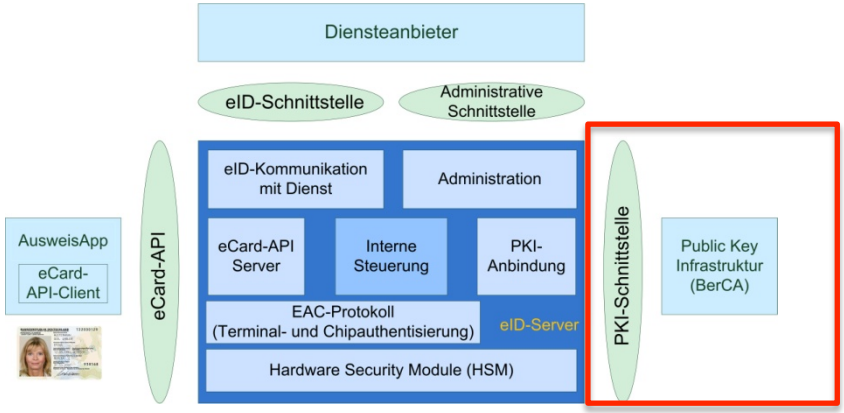
EAC Protokoll



- TR-03110 EAC, PACE, Restricted Identification (RI)
  - Advanced Security Mechanisms for Machine Readable Travel Documents
  - Wichtigstes technisches Dokument für "Extended Access Control"
  - Protokolle:
    - Password Authenticated Connection Establishment (PACE)
    - Terminal Authentication (TA)
    - Chip Authentication (CA)
  - Berechtigungszertifikate als "Card Verifiable Certificates"
  - Kartenkommandos & Secure Messaging gem. ISO 7816

Technische Richtlinien

PKI, Zertifikate



- TR-03128 PKI für EAC
  - "EAC-PKI'n für den elektronischen Personalausweis
  - Rahmenkonzept für Aufbau und Betrieb von Document Verifiern der Berechtigungs-PKI'n (EAC-PKI: Extended Access Control) für die hoheitliche und nicht-hoheitliche Verwendung
  - Struktur und Abläufe der EAC-PKI zur Zertifizierung von Zugriffsrechten
- TR-03129 Zertifikatsmanagement
  - PKIs for Machine Readable Travel Documents
    Kommunikationsprotokolle für die Verwaltung von Zertifikaten und CRLs