FACHHOCHSCHULE AACHEN STANDORT JÜLICH
FACHBEREICH 9 - MEDIZINTECHNIK UND
TECHNOMATHEMATIK

Einsatzmöglichkeiten der neuen elektronischen Personalausweise im Zutrittskontroll-Management

Seminararbeit
im Studiengang
„Scientific Programming“

Olaf Hinkens
Matse i.A., Bosch Access Systems GmbH, Aachen
Matrikelnummer: 993355
12.12.2011

Erstbetreuer:
Prof. Dr. Walter Hillen, FH Aachen - Campus Jülich
Zweitbetreuer:
Dipl.-Inform. Dieter Kämpfe, Bosch Access Systems GmbH - Aachen

Inhaltsverzeichnis

1 Einleitung

Kern der Seminararbeit ist die Untersuchung der neuen Funktionalitäten elektronischer Ausweisdokumente (e-Ausweise) und deren Einsatzmöglichkeiten in Zutrittskontrollsystemen. Die RFID-Chips der e-Ausweise, die seit einigen Jahren in Reisepässen und seit Herbst 2010 auch in allen Personalausweisen integriert sind, können genutzt werden, um automatisierte Zutrittsprozesse zu steuern.
Die automatisierte Grenzkontrolle am Flughafen Frankfurt/Main ist ein spezielles System, das im Laufe dieser Arbeit stellvertretend für Zutrittskontrollsysteme vorgestellt wird. Die Ausweisdokumente werden dort zurzeit optisch mit Dokumentenlesern erfasst. Diese sollen durch neue Modelle ersetzt werden, die Ausweise optisch und elektronisch erfassen können. Am Ende dieser Arbeit wird kurz auf neue Möglichkeiten zur weiteren Vereinfachung bzw. Automatisierung des Verfahrens eingegangen.

Zuvor werden die Voraussetzungen zur Schaffung einer solchen Infrastruktur untersucht, die die neuen Funktionalitäten der e-Ausweise verwenden kann. Abschließend wird der Nutzen für allgemeine Zutrittssysteme bewertet.

Die Bezeichnungen für elektronische Ausweisdokumente, die in dieser Arbeit verwendet werden, beziehen sich im Abschnitt über das Grenzkontrollprojekt auf elektronische Reisepässe (ePass). In der allgemeinen Zutrittskontrolle wird der Bezug auf elektronische Personalausweise (ePA oder nPA) sein. Es wird darauf hingewiesen, dass der ePass lediglich biometrische Merkmale speichert. Der ePA dagegen speichert weitere personenbezogene Daten.
Die Bezeichnungen ePA und nPA sind Synonyme für den neuen elektronischen Personalausweis, wobei das Kürzel nPA die neuere Variante ist. Um den Aspekt des Elektronischen hervorzuheben, wird in den folgenden Abschnitten das Kürzel ePA verwendet.

In Abschnitt 2 wurden die im Literaturverzeichnis unter dem Punkt ‚Dokumentenleser BorderGuard B5000' aufgeführten Hersteller-Handbücher und die unter dem Punkt ‚Interne Dokumente' angegebenen firmeninternen Dokumentationen verwendet. Analog wurden im dritten Abschnitt Dokumente verwendet, die unter den Punkten ‚Technische Richtlinie', ‚Whitepapers' und ‚Anwenderhandbuch' zu finden sind.

2 Grenzkontrolle am Flughafen Frankfurt/Main

Das Pilotprojekt „Automatisierte und biometriegestützte Grenzkontrolle – ABG“ im Auftrag des Bundesministerium des Inneren ist ein spezielles Zutrittskontrollsystem, durch das am Flughafen Frankfurt/Main die Ein– und Ausreisekontrollen für Flugreisende vereinfacht werden. Teilnehmenden Personen wird so im Non-Schengen-Flugverkehr die Ein- und Ausreise ohne manuelle Grenzkontrolle ermöglicht.
Das ABG-Verfahren ist im Sinne der Zutrittskontrolle ein Vereinzelungs-verfahren. D.h. eine Schleuse kann maximal von einer Person genutzt werden und wird in diesem Fall als Autocontrol-Spur bezeichnet.
Das ABG-Verfahren teilt sich in zwei Abschnitte: Enrolment (Registrierung) und Autocontrol (automatisierter Kontrollvorgang beim Grenzübertritt).

Voraussetzungen zur freiwilligen Teilnahme für Flugreisende sind die Vollendung des 18. Lebensjahrs, die Mitgliedschaft eines EU/EWR-Staates oder der Schweiz, Besitz eines Ausweisdokuments mit einer Maschinenlesbaren-Zone (MRZ, Machine Readable Zone) und die einmalige Registrierung durch die Bundespolizei. Dabei werden die Daten der MRZ des Ausweisdokuments erfasst und eine Aufnahme der Augen-Iris vorgenommen, deren biometrische Merkmale gespeichert werden. Diese Daten gelten als Teilnahme-bestätigung/Einwilligungserklärung am Pilotprojekt und werden zur biometrischen Authentifizierung bei späteren Grenzübertritten benutzt.

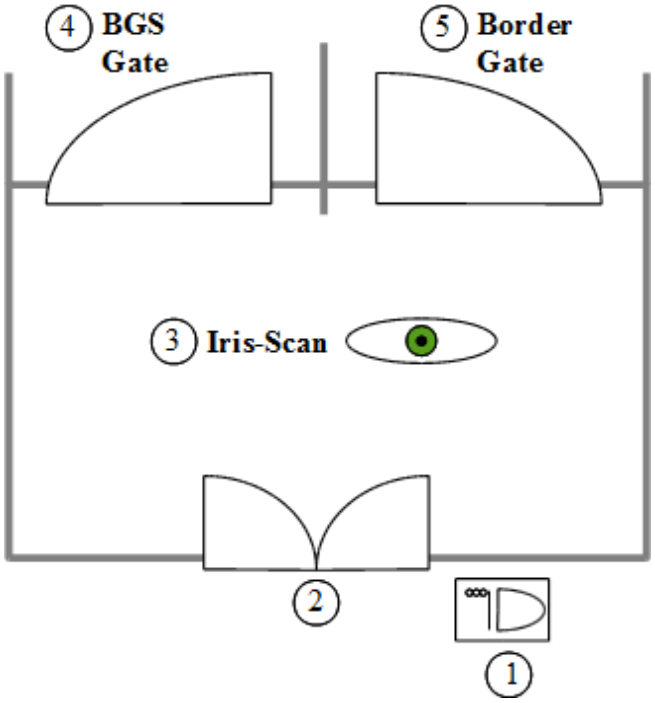

Abbildung 1: „Schema einer Autocontrol-Spur“: Dokumentenleser (1) zur Öffnung des Schleuseneingangs (2) durch registrierte Reisende, Iris-Scan (3) in der Schleuse, Kontrolltür (4) zur manuellen Grenzkontrolle , Freigabetür (5) zum Grenzübertritt

2.1 ABG – Systemübersicht

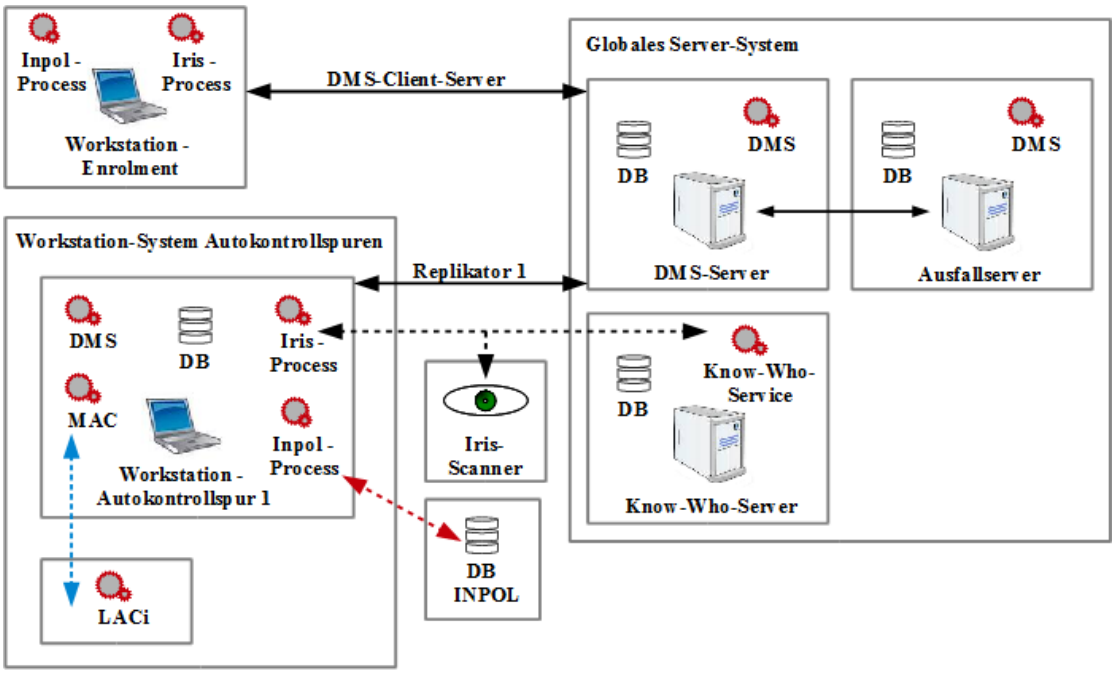

Abbildung 2: „Vereinfachtes ABG-Server-Workstation-System im Überblick“ mit LAC (Local Access Controller) mit RS232-Schnittstelle zum Dokumentenleser, MAC (Main Access Controller) zur Ablaufsteuerung einer Begehung, DMS (Data Management Server/Service) als zentraler Dienst zur Steuerung des Gesamtsystems, Iris-Prozess zur Aufnahme, Speicherung und Abgleichung der Augen-Iris, Inpol-Prozess zur Abfrage polizeilicher Fahndungssysteme (u.a. an Interpol-Datenbank)

Das Gesamtsystem ABG besteht aus einem redundant ausgelegtem Server (zentraler DMS-Server und inaktiver Ausfallserver), je eine Workstation für die vier Autocontrol-Spuren und zwei Workstations für die Enrolment-Prozesse im Registrierungsbüro der Bundespolizei. Alle Workstations sind mit den benötigten Peripherie-Geräten verbunden: Iris-Scanner und Dokumentenleser.
Die Enrolment-Stationen sind als DMS-Client mit dem zentralen DMS-Server verbunden. Dieser Server mit installierter Oracle-Datenbank fungiert als Datenmaster. Die Stammdaten der teilnehmenden Person werden dort gesichert, verwaltet und gepflegt. Alle erfassten Daten werden auf den inaktiven Ausfallserver repliziert.
Die neu erfassten Personendaten werden zusätzlich an alle Workstations der Autocontrol-Spuren über die jeweils zugeordneten Replikatoren-Prozesse gesendet. Dies ist nötig, da die Autocontrol-Spuren autonom arbeiten müssen. D.h. jede Workstation einer Autocontrol-Spur enthält ein komplettes System bestehend aus Oracle-Datenbank, DMS, MAC und den Prozessen INPOL, IRIS und dem Dialogsystem zur Überwachung und Steuerung der Autocontrol-Spuren durch Beamte der Bundespolizei.

Zusätzlich zum zentralen Datenserver und dem Ausfallserver wird ein dritter Server, der Know-Who-Server, betrieben. Dieser dient als Datenbank- und Applikationsserver für die Biometrie-Daten. In seiner lokalen Datenbank werden lediglich die Iris-Templates mit eindeutigen Iris-IDs gespeichert. Die Personendaten des DMS-Servers sind entsprechend mit der Iris-ID verknüpft. Personenbezogene Daten und Iris-Templates sind aus Datenschutzgründen auf mindestens zwei physikalisch verschiedenen Servern gesichert.

2.2 Die Dokumentenleser im ABG-System

Es sollen in Zukunft Dokumentenleser der amerikanischen Firma L1-Identity Solutions am Flughafen-Projekt ABG verwendet werden. Der offizielle Produktname lautet Color BorderGuard B5000 (kurz: BorderGuard). Im einfachsten Fall dient der BorderGuard lediglich als fotografisches Kopiergerät.

Nach ICAO-Standard (International Civil Aviation Organization, dt.: Internationale Zivilluftfahrtorganisation) besitzen international anerkannte Reisedokumente eine Maschinenlesbare-Zone in der zur besseren optischen Identifikation Text und Code in der Standard-Schrift OCR-B (Optical Character Recognition, Vorgänger: OCR-A) gedruckt sind.
Wird ein Dokument in den Scan-Bereich des BorderGuards eingebracht, wird dieser zuerst versuchen, die Identität des Dokuments festzustellen, indem ein Staat, Bundesland oder eine andere Gerichtsbarkeit und die Art des Dokuments identifiziert werden. Das Abbild (Image) des Ausweisdokuments wird mit unterschiedlichen Lichtarten erfasst, die sich in ihrer Wellenlänge unterscheiden:

- Sichtbares Image: Erfassung unter herkömmlichem weißen Licht (Wellenlänge 380-780 nm: für Menschen sichtbares Spektrum):
  Zur Erstellung des fotografischen Abbilds des Ausweisdokuments

- IR Image: Erfassung unter Infrarotem Licht (Wellenlänge: 780-1400 nm, nahes Infrarot NIR, kurz IR-A) zur Überprüfung, ob eine spezielle Druckfarbe verwendet wurde (B900 Test): Die MRZ und anderer Text sollte nach ICAO-Standard mit der speziellen Druckfarbe ‚B900 Ink' gedruckt werden, die IR-Licht absorbiert und damit sichtbar bleibt. Andere Elemente sollten nicht erscheinen, z.B. der Hintergrund. (Abbildung 3, links)

- UV Image: Erfassung unter Ultra Violettem Licht (Wellenlänge: 315-380 nm, nahes UV („Schwarzlicht"), kurz UV-A) für den UV-Helligkeits-Test: Das UV-Abbild des Dokuments kann so auf Anzeichen einer Fotokopie oder auf Verwendung von gefälschtem Papier untersucht werden. Ein authentisches Dokument erscheint dunkel unter UV-Licht und sollte lichtschwache grüne und rote UV-Muster enthalten. Der Hintergrundübergang scheint dabei von grün nach rot und wieder nach grün zu verlaufen. (Abbildung 3, rechts)

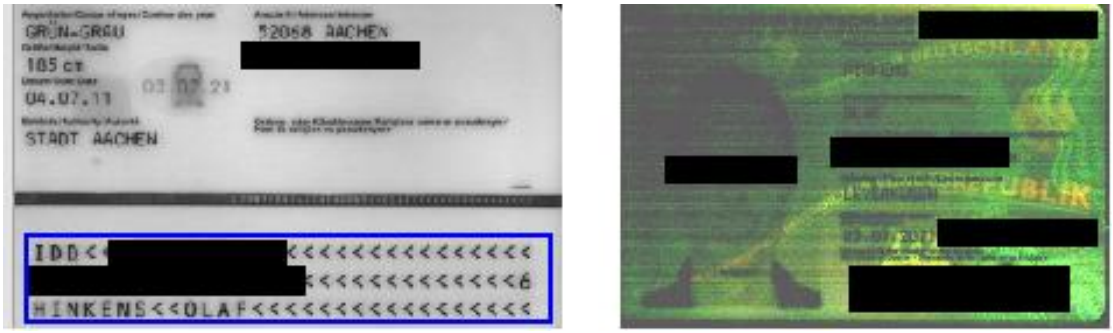

Abbildung 3: IR-Aufnahme (links) der Rückseite mit MRZ und UV-Aufnahme (rechts, aufgehellt) der Vorderseite eines neuen elektronischen Personalausweises

Die Ergebnisse der oben beschriebenen Tests und die Daten der MRZ, inklusive der Berechnung der Checksumme aus der MRZ, werden dem ABG-System zur weiteren Verarbeitung zur Verfügung gestellt. Nach entsprechender positiver biometrischer Verifikation und negativer grenzpolizeilicher Fahndungsabfrage kann der registrierte Reisende die automatisierte Grenzkontrolle passieren.

Mit dem neuen BorderGuard, der die bisherigen Dokumentenleser ersetzen wird, ist es außerdem möglich die integrierten RFID-Chips der e-Ausweise auszulesen. Das nächste Kapitel wird den neuen elektronischen Personalausweis stellvertretend für e-Ausweise und deren Funktionalitäten vorstellen. Die elektronischen Reisepässe enthalten lediglich biometrische Merkmale. Der ePA besitzt dagegen weitere Daten und daraus resultierende Funktionen, die in Zutrittskontrollsystemen von Interesse sind.

3 Der neue elektronische Personalausweis

Seit dem 1. November 2010 wird ausschließlich der neue elektronische Personalausweis (ePA) an die Bürger der BRD vergeben. Der integrierte Chip im ePA lässt neue Funktionen im Bereich der Online-Authentisierung und Online-Verifikation zu.
Vor allem Dienstleistungen von Unternehmen und Behörden sollen so in Zukunft einfach und sicher abgewickelt werden können. Geschäftsprozesse im Internet, bei denen die Überprüfung der Identität gesetzlich vorgeschrieben oder die Schriftform zwingend erforderlich ist, werden so erleichtert. Dadurch werden zahlreiche neue Anwendungen im Internet realisierbar.
Kernfunktion ist die elektronische Identitätsfunktion (eID-Funktion), die einen sicheren Identitätsnachweis beider Seiten - Ausweisinhaber und Dienstleister - beinhaltet. Der Identitätsnachweis erfolgt also nach dem Prinzip der Gegenseitigkeit.

3.1 Datenfelder des neuen elektronischen Personalausweises

Auf dem integrierten, kontaktlos lesbaren Chip des ePA sind neben den sichtbar aufgedruckten Text-Informationen des ePA auch biometrische Daten gespeichert. Die biometrischen Daten sind in jedem Fall das Lichtbild. Fingerabdrücke können mitgespeichert sein. Dies kann zurzeit noch von jedem Ausweisinhaber selbst bestimmt werden.

Folgende Daten sind nach [AB-WirtVerw] digital auf dem Chip abgelegt:

- Familienname und Geburtsname
- Vorname
- Doktorgrad
- Tag und Ort der Geburt
- Lichtbild
- Anschrift
- Staatsangehörigkeit
- Seriennummer
- Ordensname, Künstlername
- ggf. digitale Fingerabdrücke
- Daten der maschinenlesbaren Zone (MRZ)
- Daten zur Nutzung der Signaturfunktion

3.2 Funktionen des elektronischen Personalausweises

Es muss zwischen zwei grundsätzlichen Funktionen unterschieden werden:

1. Der Identitätsnachweis mit der Online-Funktion, die sogenannte eID-Funktion.

2. Die Unterschriftsfunktion mit einer qualifizierten elektronischen Signatur, die Signaturfunktion.

Die Signaturfunktion wird zum Abschluss rechtskräftiger Online-Verträge benutzt. Um die Signaturfunktion zu aktivieren, muss der Ausweisinhaber ein Signaturzertifikat bei einem privaten Anbieter eigenständig erwerben und anschließend in den Chip des ePA nachladen. Auf die Unterschriftsfunktion wird in dieser Arbeit nicht weiter eingegangen.
Grundsätzlich gilt, dass beide Funktionen nur genutzt werden können, wenn der Ausweisinhaber die Online-Funktion des ePA aktiviert hat. Desweiteren gilt, dass Daten des ePA nur übermittelt werden, wenn der Ausweisinhaber dies durch Eingabe seiner 6-stelligen PIN-Nummer bestätigt. Beide Funktionen nutzen unterschiedliche PIN-Nummern (eID-PIN und Signatur-PIN).
Zusammenfassend muss zwischen „Sicherem Identitätsnachweis“ (1.) und „Rechtsverbindlicher Unterschrift“ (2.) unterschieden werden.

3.3 Einige gesetzliche Grundlagen

Bei Nutzung des elektronischen Identitätsnachweises können nach Paragraph 18 Abs. 3 Satz 2 des PAuswG maximal folgende Daten übermittelt werden:

1. Familienname
2. Vorname
3. Doktorgrad
4. Tag der Geburt
5. Ort der Geburt
6. Anschrift
7. Dokumentenart
8. dienste- und kartenspezifisches Merkmal (Stichwort ‚Pseudonym-Funktion‘)
9. Abkürzung „D“ für Bundesrepublik Deutschland
10. Angabe, ob ein bestimmtes Alter über- oder unterschritten wird
11. Angabe, ob ein Wohnort dem abgefragtem Wohnort entspricht
12. Ordensname, Künstlername

[AB-WirtVerw]

Grundsätzlich gilt, dass der Abruf der Daten vom ePA durch den Dienstleister für den angegebenen Zweck der Datenerhebung zwingend erforderlich ist. Dies wird

unter anderem in Paragraph 21 Abs. 2 Nr. 1 des PAuswG im Kapitel „Rechtmäßigkeit des Abrufzweckes“ erläutert.
Im allgemeinen Datenschutzrecht gilt das Gebot der ‚Datensparsamkeit‘. Nach diesem Prinzip dürfen nur so viele personenbezogenen Daten erfasst werden, wie für den Geschäftszweck des Dienstleisters erforderlich sind (‚Erforderlichkeitsgrundsatz‘).
Wichtig ist die Unterteilung der Dienstleistungen in zwei (Geschäfts-)Bereiche: dem E-Government und E-Business. Im ersten Bereich tritt der Staat oder eine Behörde als Dienstleister auf, im zweiten Bereich sind dies private (nicht öffentliche) Dienstanbieter der Wirtschaft.
Nur ‚Hoheitliche Behörden‘ können die biometrischen Daten des ePA auslesen und zu Vergleichszwecken nutzen. Die Speicherung dieser Daten ist grundsätzlich verboten.

3.4 Voraussetzungen für private Dienstanbieter

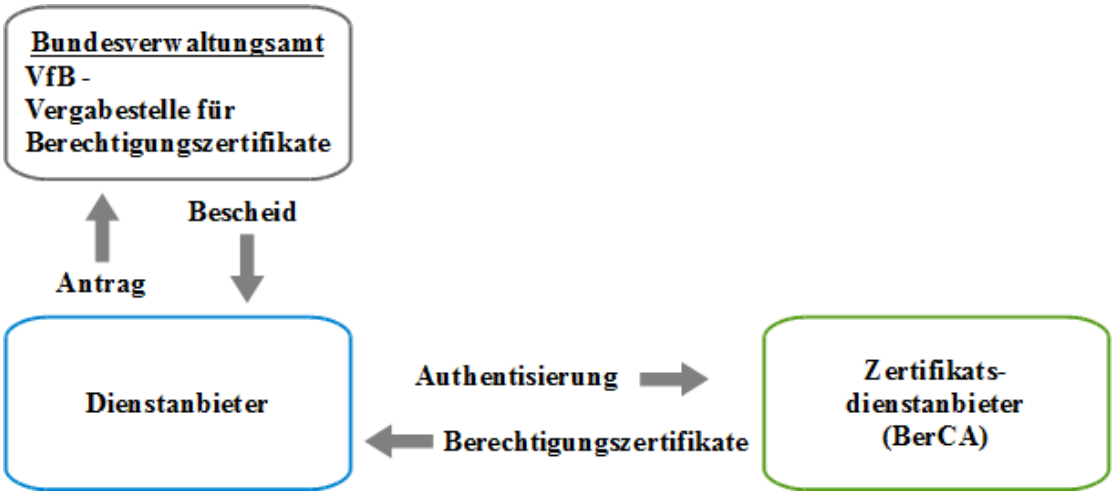

Abbildung 4: Vergabeprozess – Berechtigungszertifikat [AB-WirtVerw]

Erster Schritt zur Nutzung des elektronischen Identitätsnachweises als privater Dienstanbieter ist die Beantragung eines Berechtigungszertifikats bei der Vergabestelle für Berechtigungszertifikate (VfB) des Bundesverwaltungsamts (BVA). Die VfB prüft den Zweck, für den eine Berechtigung ausgestellt werden soll, die Dienstbeschreibung so wie die Notwendigkeit der Datenerhebung.
Nach Paragraph 21 PAuswG muss der Dienstanbieter folgende Voraussetzungen erfüllen, um die eID-Funktion zu nutzen (Quelle: [AB-WirtVerw]):

- Die Erforderlichkeit der zu übermittelnden Angaben für den beschriebenen Geschäftszweck muss nachgewiesen werden

- Maßnahmen für Datenschutz und Sicherheit

- Der Geschäftszweck besteht nicht in der geschäftsmäßigen Übermittlung der Daten und es liegen keine Anhaltspunkte für die geschäftsmäßige oder unberechtigte Übermittlung der Daten vor

- Keine Anhaltspunkte für missbräuchliche Verwendung der Berechtigung

Erst nach Erhalt eines positiven Bescheids durch die VfB kann der Dienstleister bei einem Zertifizierungsdienstanbieter (‚Berechtigungszertifikateanbieter', kurz ‚BerCA') ein entsprechendes technisches Berechtigungszertifikat erwerben.
Der Dienstanbieter kann nun selbst entscheiden, ob er einen eigenen eID-Server für seine Dienstleistung im Internet betreibt oder es wird ein privater eID-Service-Anbieter gewählt, der den eID-Server verwaltet und seine Dienste online zur Verfügung stellt. Im zweiten Fall wird der IT-Dienstleister, der die Aufgaben des Identitätsnachweises erbringt, „eID-Service-Provider" genannt und seine Dienstleistung „eID-Service".

3.5 Technischer Ablauf der Online-Authentisierung

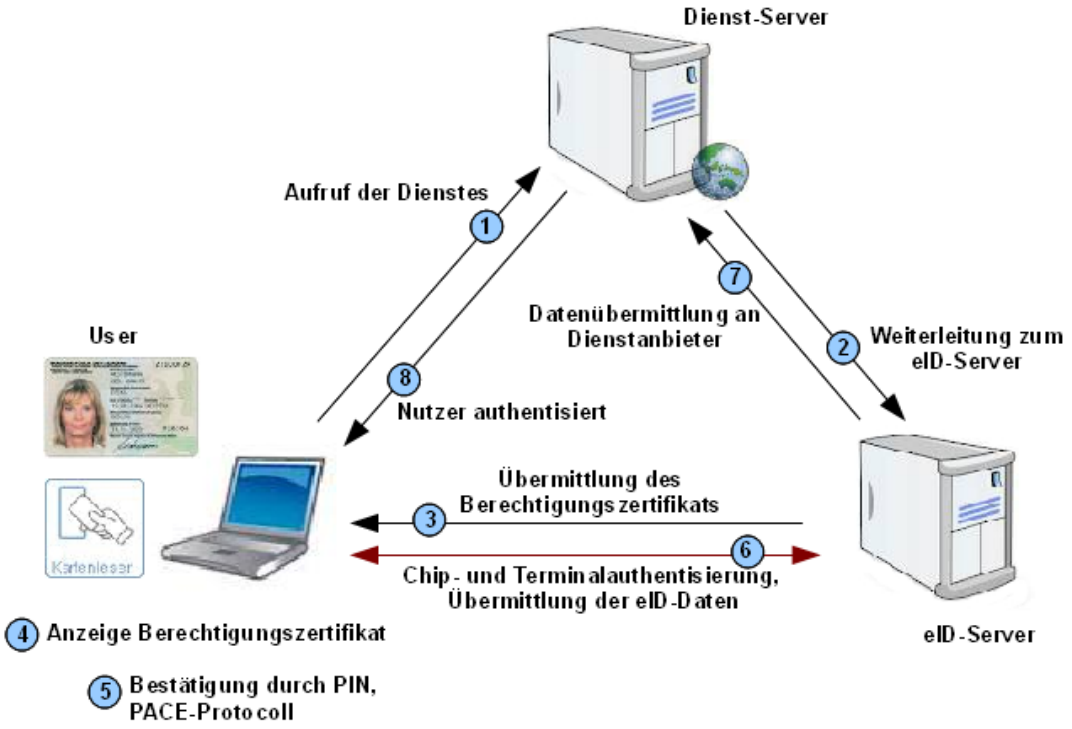

Abbildung 5: Ablauf der Online-Authentisierung [Quelle: WP-Automat]

Die Online-Authentisierung wird im Folgenden am Beispiel eines Webdienstes, wie in [AB-eID], kurz beschrieben:

1. Der Ausweisinhaber ruft die Webseite eines Dienstanbieters auf. Dieser benötigt eine Online-Authentisierung mit Hilfe des neuen ePA.

2. Der (Web-)Dienst leitet die Authentisierungsanfrage an den eID-Server weiter.

3. Anschließend beginnt der Aufbau sicherer Kanäle zwischen dem eID-Server, der Client-Software (Ausweisinhaber nutzt z.B. AusweisApp des Bundes), dem Lesegerät so wie dem Ausweischip. Dabei werden die Authentizität des Ausweisinhabers und des Dienstanbieters so wie die Integrität (Fälschungssicherheit) des Ausweises geprüft.
   Der Identitätsnachweis kann so nach dem Prinzip der Gegenseitigkeit erfolgt (siehe Abschnitt 3.8. Kryptografische Protokolle: Terminal-Authentisierung und Chip-Authentisierung).

4. Dem Nutzer werden durch die Client-Software das Berechtigungszertifikat des Dienstleisters und die angefragten Ausweisdaten angezeigt. Der Ausweisinhaber entscheidet nun, welche Daten tatsächlich übermittelt werden sollen.

5. Durch Eingabe der 6-stelligen PIN-Nummer bestätigt der Ausweisinhaber die Übermittlung seiner Daten. Die sichere Verbindung zum Ausweischip und die Korrektheit der PIN-Nummer wird dabei durch das PACE-Protokoll (Password Authenticated Connection Establishment, siehe Abschnitt 3.8. Kryptografische Protokolle) geprüft.

6. Übermittlung der Ausweisdaten an den eID-Server.

7. Der eID-Server leitet das Ergebnis der Authentisierung und die Ausweisdaten an den anfragenden Webdienst weiter.

8. Das Ergebnis der Authentisierung und die Ausweisdaten werden vom Web-Dienst ausgelesen. Der jeweilige Dienst entscheidet, ob das Ergebnis der Authentisierung als positiv bewertet werden kann und gewährt dem Nutzer so Zugriff auf den eigentlichen Web-Dienst.

3.6 Anforderungen an eID-Server

Ein eID-Server hat nach [BSI TR-03130] folgende Aufgaben:

1. Bereitstellung der sicheren Kommunikation zwischen Client-Software, ePA und Client-PC (PC des Users/Bürgers).

2. Nach Feststellung der Authentizität, der Gültigkeit des ePA und Prüfung des Sperrmerkmals werden die Ergebnisse der eID-Funktion an die anfragenden Systeme des Dienstanbieters übermittelt.

3. Regelmäßige Aktualisierung und Erneuerung der eigenen Berechtigungszertifikate durch Berechtigungszertifikatsdienstanbieter (BerCA) und Abruf aktueller Sperrlisten.

Weitere Technische Richtlinien (TR) sind zu beachten:

- Einhaltung der eCard-API-Spezifikation gemäß BSI TR-03112 durch die Software des eID-Servers
- Spezielle Anforderungen nach BSI TR-03130 für eID-Server

Übernimmt ein eID-Service-Provider die Online-Authentisierung müssen die kryptografischen Schlüssel für die Kommunikation zwischen dem Dienstanbieter und dem eID-Service jeweils auf beiden Seiten mit dem gleichen Sicherheitsniveau gespeichert werden.

3.7 Schnittstellen des eID-Servers

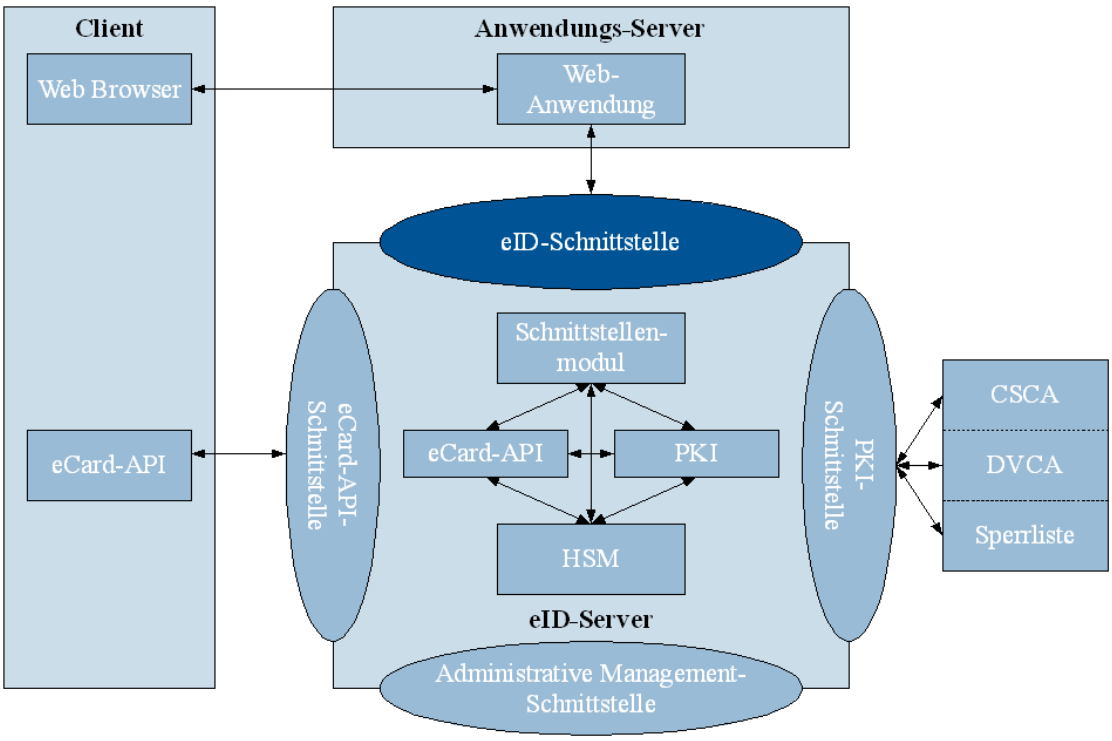

Abbildung 6: Funktionseinheiten eID-Server [Quelle: BSI TR-03130]

Die in Abbildung 6 dargestellten Soft- und Hardware-Komponenten eines eID-Servers stellen die Kommunikation zur clientseitigen eCard-API her. Desweiteren sind Kommunikationsschnittstelle zum Abruf von Terminal-Berechtigungszertifikaten (DVCA-Zertifikate, Document Verifying Certificate Authority), Sperrlisten und CSCA-Zertifikaten (Country Signing CA) enthalten.

Um die Sicherheit und Echtheit der Daten während der Übertragung zwischen eID-Server und Anwendungsserver zu gewährleisten, sind die Daten verschlüsselt und signiert.

- eID-Schnittstelle:
  Hauptaufgabe ist die gegenseitige Authentisierung und die Weiterleitung der Daten aus dem ePA des Users an den aufrufenden Dienst des Anbieters.

- eCard-API-Schnittstelle:
  Es existieren zwei eCard-API-Implementierungen: eine Client- und eine Serverseitige. Auf Seite des Clients läuft z.B. die AusweisApp des Bundes, die sich mit der serverseitigen eCard-API-Implementierung verbindet, nachdem eine Authentisierungsanfrage durch den Browser des Anwenders erfolgt ist. Diese Verbindung wird vom eID-Server verwendet, um Daten des ePA auszulesen.

- PKI-Schnittstelle:
  (Schnittstelle zur Public-Key-Infrastruktur und Berechtigungszertifikate-anbieter)
  Die Berechtigungen zum Auslesen des ePA werden durch eine PKI-Infrastruktur (PKI) abgebildet. In der PKI betreibt jede Nation eine CVCA (Country Verifying Certificate Authority). Unterhalb dieser Instanz werden meist mehrere DVCA (Document Verifying CA) betrieben, die Terminal-Berechtigungszertifikate ausstellen (Stichwort: Zertifikatskette; Anmerkung: DVCA wird auch Berechtigungs-CA, kurz BerCA, genannt). Mit Hilfe dieses Terminal-Berechtigungszertifikats authentisiert sich der Dienstleister gegenüber dem ePA, um Daten auszulesen. Dabei enthält das Terminal-Berechtigungszertifikat genaue Angaben, welche Informationen aus dem ePA ausgelesen werden dürfen.
  Die übermittelten Ausweisdaten werden durch ein Zertifikat der DSCA (Document Signing CA) signiert, um die Echtheit des ePA auf elektronischem Weg zu prüfen. Analog zur CVCA/DVCA-Infrastruktur wird die DSCA unterhalb einer CSCA (Country Signing CA) betrieben.
  Zusammenfassend werden über die PKI-Schnittstelle dem eID-Server die Berechtigungszertifikate, die diensteanbieterspezifischen Sperrlisten und andere benötigte Zertifikate, Sperr- und Defektlisten nach Richtlinie BSI TR-03130 vom BerCA zur Verfügung gestellt.

- Administrative Management-Schnittstelle:
  Der eID-Server benötigt initiale Einstellungen und Schlüssel, um seine spezifizierten Dienste zu betreiben und zu konfigurieren. Dazu gehören unter anderem folgende Parameter: Adresse und Port des eCard-API-Servers, des Sperrlistendienstes, der DVCA und CSCA, so wie Authentisierungszertifikate.

Letztere werden benutzt, um durch den eID-Server im Namen des Dienstanbieters Terminal-Berechtigungszertifikate bei einer DVCA abzuholen.

- Hardwareschnittstelle HSM (Hardware Security Modul):
  Internes oder externes Peripheriegerät, das durch das BSI zertifiziert ist, um geeignete Schlüsselpaare zu generieren, zu speichern und zu nutzen. Diese müssen nach kryptografischen Algorithmen gemäß BSI TR-03130 erzeugt werden. So werden die Vertrauenswürdigkeit und die Integrität der Daten durch das HSM sicher gestellt.

3.8 Kryptografische Protokolle

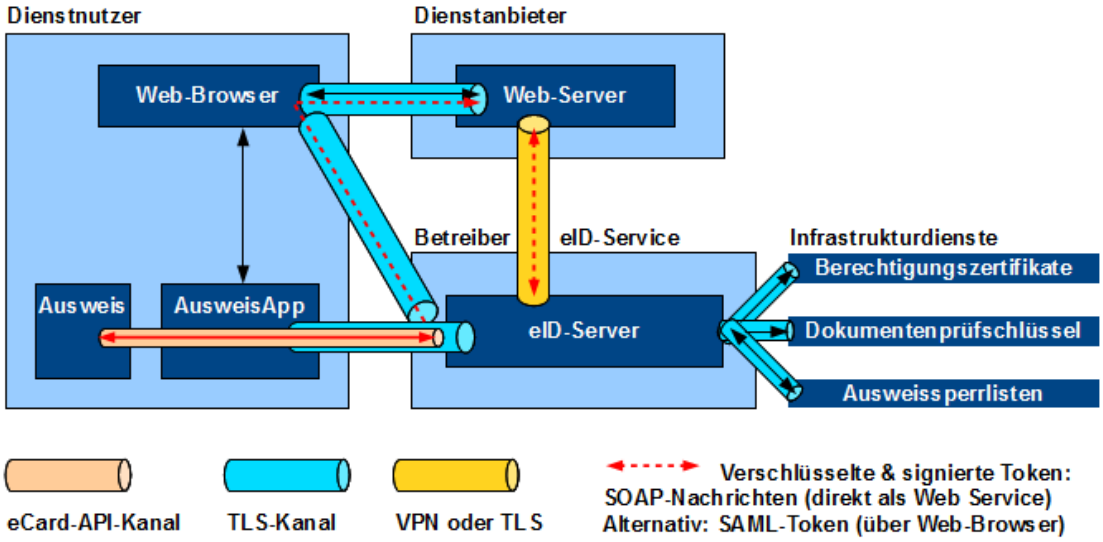

Abbildung 7: Kommunikationsverbindungen bei Nutzung eines eID-Service [Quelle: WP-Sicherheit]

In Abbildung 7 werden die verschiedenen Verbindungen zwischen dem Dienstnutzer, dem Dienstanbieter und dem eID-Service-Provider dargestellt. Alle Verbindungen sind mindestens mit dem TLS-Verfahren (seit Version 3.0 Transport Layer Security, vorher SSL genannt) gesichert, so dass die Kommunikation auf Basis von HTTPS erfolgen kann. Als Alternative können teilweise VPN-Verbindung genutzt werden. Die TLS-Zertifikate sollten von Zertifizierungsstellen bezogen werden, bei denen die öffentlichen Schlüssel den meisten Browsern bekannt sind. So entfällt die manuelle Überprüfung durch den Dienstnutzer.
Nach Abbildung 7 werden zwischen eID-Service-Provider und Dienstanbieter signierte SOAP-Nachrichten (Simple Object Access Protocol) ausgetauscht, um Echtheit und Integrität der angehängten Daten digital abzusichern. Alternativ können signierte SAML-Token (Security Assertion Markup Language) über den Web-Browser des Dienstnutzers vom eID-Service zum Dienstanbieter genutzt werden, um eID-Daten zu versenden.

Für den mehrstufigen Aufbau eines sicheren Kanals auf Anwendungsebene, also zwischen Ausweis-Chip, Kartenleser und Dienstanbieter (eCard-API-Kanal plus TLS-Verbindung), werden kryptografische Protokolle genutzt. Diese erzeugen bei Ausführung einen definierten Sicherheitszustand im Ausweis-Chip, der z.B. bei Abbruch der Session aus Sicherheitsgründen sofort gelöscht wird.

- PACE (Password Authenticated Connection Establishment):
  Zuständig für die sichere PIN-Eingabe und den Aufbau eines verschlüsselten und sicheren Kanals zwischen lokalem Kartenleser bzw. AusweisApp (abhängig von verwendetem Kartenleser) und dem Ausweis-Chip.

- Terminal-Authentisierung:
  Nach Aufbau des sicheren Kanals, nutzt der Ausweis-Chip die Terminal-Authentisierung zur Verifikation, ob der Dienstanbieter berechtigt ist, Ausweisdaten auszulesen. Dies erfolgt durch die Prüfung der Berechtigungszertifikate.

- Chip-Authentisierung:
  Diese dient zum Aufbau einer sicheren Ende-zu-Ende-Verbindung zwischen ePA und dem Dienstanbieter (bzw. eID-Server). Anschließend können Daten aus dem Chip gelesen werden. Dabei wird die Echtheit des Ausweis-Chips geprüft und somit implizit ein Echtheitsnachweis der ausgelesenen Daten erbracht.

3.9 Die Pseudonym-Funktion

Der ePA unterstützt die Erzeugung einer dienste- und kartenspezifischen Kennzeichnung (DKK), dem sogenannten Pseudonym. Damit kann der Ausweisinhaber nach einer initialen Anmeldung beim Dienstanbieter (Terminal) leichter wiedererkannt werden.
Bei erstmaliger Identifikation durch den Diensteanbieter werden neben den persönlichen Daten auch das dienste- und kartenspezifische Kennzeichen, das Pseudonym, ausgelesen. Das Pseudonym ist ein Wiedererkennungszeichen, das durch jeden Diensteanbieter neu festgelegt bzw. neu berechnet wird. So wird u.a. sicher gestellt, dass verschiedene Diensteanbieter durch einfachen Abgleich der Pseudonyme nicht erkennen können, welche Dienste bereits genutzt worden sind.
Die Berechnung des Pseudonyms erfolgt durch eine eindeutige Kennung des Anbieters, übermittelt durch sein Zertifikat, und einem auf dem Ausweis-Chip gespeichertem Geheimnis.
Der pseudonyme Zugang erleichtert also die Identifikation bereits bekannter User. Bei erneuter Nutzung des Dienstes wird lediglich das Pseudonym ausgelesen bzw. berechnet. Diese Vorgehensweise erhöht die Sicherheit, gewährleistet die Anonymität des Users und steht im Einklang mit dem Prinzip der Datensparsamkeit.

4 Abschließende Beurteilungen

In diesem letzten Abschnitt der Seminararbeit wird eine einfache Kosten-Nutzen-Analyse diskutiert, die den Schwerpunkt auf den Nutzen der integrierten Chips in Ausweisdokumenten im Vordergrund hält. Desweiteren werden Möglichkeiten für das ABG-Projekt vorgestellt, um die automatisierte Grenzkontrolle zu verbessern.

4.1 Der neue elektronische PA in Zutrittskontrollsystemen

Die neuen Funktionalitäten des ePA könnten im Bereich der Zutrittskontrolle in Zukunft eine Rolle spielen. Die Vorteile liegen in der sicheren Datenübertragung und in den einzelnen Funktionalitäten, besonders in der Pseudonym-Funktion. Diese Eigenschaften sind in einem Zutrittskontrollsystem u.a. aus Datenschutzgründen wichtig und wünschenswert.
Um einen Dienst mit qualifizierter Online-Authentisierung anzubieten, muss der Betreiber der Zutrittskontrollanlage

a) zwischen dem Betreiben eines eigenen eID-Servers und

b) der Nutzung eines privaten eID-Services durch einen qualifizierten Provider wählen.

Beide Strategien hängen stark von der eigentlichen Dienstleistung des Betreibers ab. Einerseits sind die Verwaltung und der dauerhafte Betrieb eines eigenen Servers in Betracht zu ziehen, anderseits können diese Aufgaben auch durch einen privaten eID-Service-Provider erbracht werden. Neben verschiedenen hohen laufenden Kosten und Verwaltungsaufwänden sind ebenso die Sicherheit und die Erreichbarkeit des Dienstes zu gewährleisten.
Bei privaten eID-Service-Providern bestimmen sowohl die Anzahl der Authentisierungs-Anfragen als auch die Erreichbarkeit des Services die laufenden Kosten.
Ein vorläufiges Preismodell nach [eID-Prov] der Bundesdruckerei GmbH geht von folgenden Kosten aus:

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 €

Tabelle 1: Preismodell nach [eID-Prov] der Bundesdruckerei GmbH

Für das erste Jahr ergibt sich die Gesamtsumme von 9500 €. Für die nachfolgenden Jahre ist mit laufenden Kosten in Höhe von 7000 € pro Jahr zu rechnen. Nach [eID-Prov] bietet die init-AG kostengünstigere Lösungen, die von einmaligen 750 € für die Einrichtungsgebühr und jährlichen Kosten von etwa 3000 € ausgehen.
In Zutrittskontrollsystemen wird die Nutzung eines eigenen eID-Servers aus Sicherheitsgründen bevorzugt werden, da der eID-Service nicht im öffentlichen Netz zugänglich sein soll. Daraus ergeben sich andere Kostenschwerpunkte. Die Kosten für die Einrichtung eines eigenen eID-Servers können in Abhängigkeit der benutzten Hardware und vor allem in unterschiedlich langen Implementierungsphasen verschieden hoch ausfallen. Die laufenden Jahreskosten lassen sich grob in Wartung des Servers und Erneuerung der verschiedenen Zertifikate einteilen. Nach [AB-WirtVerw] muss dafür mit ungefähr 2500 € laufenden Kosten pro Jahr gerechnet werden.
In großen Projekten spielen die anfallenden Mehrkosten keine Rolle. Dagegen werden kleinere Projekte an den erhöhten Kosten für die Hardware und den laufenden Kosten eher scheitern.

In Zutrittssystemen der privaten Wirtschaft mit einer großen Anzahl an Mitarbeitern müssen weitere Nachteile betrachtet werden:

- Frühestens in 10 Jahren verfügen alle Bundesbürger über e-Ausweise
- Mitarbeiter aus nicht EU-Staaten müssen berücksichtig werden
- Saisonabhängige Zeitarbeiter mit zeitlich beschränkten Zutrittsausweisen
- Deaktivierter ePA des Arbeitnehmers/Ausweisinhabers
- Mischbetrieb aus herkömmlichen Kartentechnologien und elektronischen Ausweisdokumenten
- Alle Leser, die auf Daten des ePA zugreifen, müssen zumindest ein Tastaturfeld für die PIN-Eingabe zur Übertragungsbestätigung besitzen und evtl. ein Dialogfeld zur Anzeige der Zertifikate haben.
- Kompatibilität zu alten Anlagen ist fraglich, vor allem, wenn teilweise reine Offline-Leser benutzt werden.
- Verbindungsverlust zum Server mit aktuellen Sperrlisten und -informationen

In kritischen Systemen gibt es Vorgaben, die unter Umständen die Nutzung der neuen ePA stark einschränken oder sogar völlig unbrauchbar machen. In sensiblen Systemen wie Kernkraftwerken darf keine Anbindung an ein

öffentliches Netz hergestellt werden. Dies ist vor allem ein Nachteil bei der Pflege der Sperrlisten, welche regelmäßig über sichere Importmöglichkeiten aktualisiert werden müssten. Das bedeutet zumindest einen erhöhten Verwaltungs- und Arbeitsaufwand.

Die neusten Generationen der sogenannten Smart-Phones besitzen einen integrierten RFID-Chip, der auf herkömmliche Weise in der Zutrittskontrolle genutzt werden könnte. Desweiteren werden diese Handys sich schneller und weiter verbreiten als die ePA, so dass alle Mitarbeiter unabhängig ihrer Herkunft diese Art der Verifizierung nutzen könnten. Auch die allgemeine Akzeptanz zur Nutzung der ePA ist meiner Meinung nach geringer als die Nutzung eines RFID-Chips im eigenen oder firmeneigenen Handy.

Zusammenfassend werden die neuen Funktionalitäten des ePA kein Standard im offiziellen Produkt eines Zutrittskontrollsystems werden. Auf herkömmliche Kartentechnologien wird nie ganz verzichtet werden können. Bei zusätzlicher Nutzung der ePA werden erhöhte Anforderungen für Hard- und Software-Komponenten erforderlich sein.
Die Anforderungen sind alle technisch umsetzbar. Der erzielte Nutzen für private nicht öffentliche Auftraggeber hält sich in Grenzen. In wenigen Fällen kann dies sinnvoll eingesetzt werden, z.B. zur Erstregistrierung eines Nutzers in Verbindung mit der Pseudonym-Funktion zur späteren Verifikation.
Es sind durchaus Szenarien bei speziellen Kunden denkbar, bei denen die Nutzung der ePA gewollt ist. Hoheitliche Behörden sind ein Beispiel für besonders spezielle Kunden, da ihnen ermöglicht wird, uneingeschränkt auf alle Daten der e-Ausweise, inklusive der Biometrie-Daten, zu zugreifen.

4.2 Ausblick für das ABG-Projekt

Die eingesetzten Dokumentenleser könnten in Zukunft genutzt werden, um die automatisierte Grenzkontrolle im Rahmen des ABG-Projekts zu vereinfachen. Eine zentrale Voraussetzung für Reisende mit deutscher Staatsangehörigkeit wäre der Besitz eines gültigen elektronischen Ausweisdokuments.
Dieser könnte genutzt werden, um einen, im weitesten Sinn, automatisierten Registrierungsprozess durch zuführen. Der nicht-registrierte Reisende würde seinen e-Ausweis zur Öffnung der Schleuse vom Dokumentenleser erfassen lassen. Dabei erkennt das System, das es sich um einen nicht-registrierten Reisenden handelt und ein Prozess zum Auslesen des integrierten Chips würde gestartet. Nach elektronischer Echtheitsüberprüfung des Ausweisdokuments würde die Schleuse geöffnet werden. Nach Eintritt des Reisenden erfolgen das biometrische Erfassen der Iris, die Speicherung des Templates und der personen-bezogenen Daten auf den entsprechenden Servern. Abschließend müsste der Beamte, der die Autocontrol-Spuren per Videosystem überwacht, entscheiden, ob weitere grenzpolizeiliche Maßnahmen durchzuführen sind. Anderenfalls wäre der

Reisende jetzt zur Nutzung der automatisierten Grenzkontrolle registriert und der erstmalige Grenzübertritt kann erfolgen. Bei der nächsten Ein- oder Ausreise würde das ABG-System erkennen, dass es sich um einen registrierten Benutzer handelt und der bisherige Prozessablauf zur automatisierten Grenzkontrolle würde gestartet.
Weitere Szenarien wären umsetzbar, indem zum Beispiel Fingerprintleser an jeder Autocontrol-Spur im ABG-System integriert würden. Nicht registrierte deutsche Reisende könnten durch Abgleich der gespeicherten Fingerabdrücke im Chip des Ausweises identifiziert werden und so die automatisierte Grenzkontrolle nutzen. Für deutsche Staatsangehörige wäre so ein Ausfall des zentralen Know-Who-Servers ohne Bedeutung. Die Autocontrol-Spuren würden in diesem Fall autonom über den Durchtritt entscheiden. Für alle anderen berechtigen Reisenden der EU würde das alte Verfahren verwendet werden.

6 Literaturverzeichnis

- Technische Richtlinie
  https://www.bsi.bund.de/ContentBSI/Themen/Elekausweise/TRundSchutzprofile/TR_Spez/TRnachArtRichtlinieSpez.html

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

- ‚Whitepaper' http://www.ccepa.de/whitepaper

[WP-Sicherheit] ‚White Paper – Neuer Personalausweis – Sicherheitsanforderungen für Dienstanbieter', Version 1.0 von März 2011, Herausgeber: Bundesministerium des Inneren

[WP-Automat] ‚White Paper – Neuer Personalausweis – Einsatz in Automaten', Version 1.0 von März 2011, Herausgeber: Bundesministerium des Inneren

[WP-eID] ‚White Paper – Neuer Personalausweis – eID-Server und eID-Service', Version 1.0 von März 2011, Herausgeber: Bundesministerium des Inneren

- Anwenderhandbuch
  http://www.personalausweisportal.de/SharedDocs/Downloads/DE/Material-Dienstleister/anwenderhandbuch.html?nn=830452

[AB-WirtVerw] ‚Der Personalausweis – Anwenderhandbuch für Wirtschaft und Verwaltung', Stand Dezember 2010, Herausgeber: Bundesministerium des Inneren

- URL-Quelle ‚Preismodelle':
  http://blog.die-eid-funktion.de/2010/12/07/erste-preismodelle-von-eid-service-providern/

[eID-Prov] Titel: „Erste Preismodelle von eID-Service-Providern" vom 07.Dez. 2010, Zuletzt besucht am 06.12.2011

- Interne Dokumente:

[ABG-Intern] ‚ABG in Aixagon II – Einrichtung einer automatisierten und biometriegestützten Grenzkontrolle", Version 1.1 vom 28.10.2010, Herausgeber: Micos GmbH

[ABG-Admin] ‚ABG –Automatisierte und biometriegestützte Grenzkontrolle – Administratoren-Handbuch', Version 1.3 vom 19.01.2004, Herausgeber: Micos GmbH

[ABG-Ausschr] ‚Pilotprojekt für die Einrichtung einer automatisierten und biometriegestützten Grenzkontrolle (ABG) auf dem Flughafen Frankfurt/Main', Version 1.5, Herausgeber: Beschaffungsamt des Bundesministeriums des Innern

- Dokumentenleser ‚BorderGuard B5000'

[IA-IDK] ‚iA-thenticate 5.4 – Integrator's Development Kit (IDK) – Programmer's Guide', Version 5.4, Stand Juli 2009, Herausgeber Viisage Technologie, Web-Adresse: http://www.l1id.com

[IA-Exam] ‚iA-Examiner 5.4 – User's Guide', Version 5.4, Stand Dez. 2008, Herausgeber L-1 Identity Solutions, Web-Adresse: http://www.l1id.com

7 Glossar

ABG
Automatisierte und biometriegestützte Grenzkontrolle am Flughafen Frankfurt/Main

AusweisApp
Kostenlose Software des Bundes zur Kommunikation zwischen ePA, Kartenleser und Dienstanbieter bzw. dessen eID-Service

B900 Ink/Test
Die MRZ und anderer Text sollte nach ICAO-Standard mit der speziellen Druckfarbe ‚B900 Ink' gedruckt werden, die IR-Licht absorbiert und unter infrarotem Licht sichtbar bleibt.

BerCA
Berechtigungszertifikatanbieter, auch Zertifizierungsdienstanbieter genannt, bei dem (nach positivem Bescheid durch die VfB) der antragstellende Dienst-anbieter ein technisches Berechtigungszertifikat erwerben kann, um seinen online-Dienst mit eID-Funktion zu betreiben.

BorderGuard
Dokumentenscanner/-leser der Firma L1-Identity Solutions, Produktname: Color BorderGuard B5000, siehe Seite 6

BSI
Bundesamt für Sicherheit in der Informationstechnik

BVA
Bundesverwaltungsamt, siehe dazu VfB

CA
Certificate Authority

CSCA
Country Signing Certificate Authority, siehe Seite 14

CVCA
Country Verifying Certificate Authority, siehe Seite 14

DKK
Dienste- und kartenspezifische Kennzeichnung: Der ePA unterstützt die Erzeugung einer DKK, dem sogenannten Pseudonym, das als Wiedererkennungsmerkmal genutzt werden kann. (siehe Seite 16)

DMS
Data Management Server/Service: Software-Modul zur Verwaltung und Steuerung des Gesamtsystems aus MAC, LAC, INPOL, IRIS und weiteren Prozessen. Beinhaltet u.a. den Aufbau und die Pflege der Datenbank/en, sowie Logbuch-Verwaltung und grafisches Dialogsystem

DSCA
Document Signing Certificate Authority, siehe Seite 14

DVCA
Document Verifying Certificate Authority, siehe Seite 14

e-Ausweise
Ausweisdokumente mit integriertem kontaktlos lesbarem RFID-Chip

E-Business
Geschäftsbereich, in dem private (nicht öffentliche) Dienstanbieter der Wirtschaft auftreten.

eCard-API
Framework zur Bereitstellung einer Software-Schnittstelle, um verschiedenen Anwendungen die Nutzung von Chipkarten, z.B. der ePA, zu erleichtern

E-Government
Geschäftsbereich, in dem der Staat (öffentliche, hoheitliche Behörden) als Dienstleister auftritt.

eID-Daten
Daten, die elektronisch auf dem Ausweis-Chip des ePA gespeichert sind und ausgelesen werden können

eID-Funktion
Elektronische Identitätsfunktion zum sicheren und gegenseitigem Identitätsnachweis zwischen Ausweisinhaber und Dienstleister, der auf Daten des Ausweises zugreifen will.

eID-PIN
6-stellige personenbezogene PIN-Nummer des ePA zur Bestätigung der Datenübertragung an anfragenden Dienstleister

eID-Server
Hauptaufgabe des Servers ist die Bereitstellung des eID-Services für die sichere Kommunikation zwischen Dienstanbieter und Ausweis-Chip des ePA.

eID-Service
Service des eID-Servers, um den sicheren Datenaustausch zwischen Ausweis-Chip und berechtigten Dienstanbieter zu gewährleisten.

eID-Service-Provider
Externer Dienstanbieter, der berechtigten und zertifizierten (dritten) Diensten, seinen eID-Service online zur Verfügung stellt.

ePA
Der neue elektronische Personalausweis mit integriertem kontaktlos lesbarem RFID-Chip, auf dem biometrische und personenbezogene Daten gespeichert sind.

ePass
Elektronischer Reisepass mit integriertem kontaktlos lesbarem RFID-Chip, auf dem lediglich biometrische Daten gespeichert werden.

HSM
Hardware Security Modul: Internes oder externes Peripheriegerät, das durch das BSI zertifiziert ist, um geeignete kryptografische Schlüsselpaare zu generieren, zu speichern und zu nutzen. (siehe Seite 15)

ICAO
International Civil Aviation Organization, dt.: Internationale Zivilluftfahrtorganisation

INPOL
Software-Prozess/-Dienst zur Abfrage polizeilicher Fahndungssysteme, u.a. Anfragen an Interpol-Datenbank

IRIS (-Prozess)
Software-Prozess/-Dienst zur Aufnahme der Augen-Iris und damit verbundener Vergleichsanfrage an den Know-Who-Server

LAC
Local Access Controller: Hardware/Software-Modul mit RS232 Schnittstelle zum Dokumentenleser zur Steuerung von Türkontakten bzw. elektrischen Signalen

MAC
Main Access Controller: Software-Modul zur Verifikation registrierter Benutzer; Zentraler Prozess der Ablaufsteuerung einer Begehung an einer Autocontrol-Spur

MRZ
Engl.: Machine Readable Zone, dt.: Maschinenlesbare Zone
Maschinenlesbare Zone auf einem international anerkannten Reisedokument, in der die Standardschrift OCR-B zur besseren optischen Erkennung von Text und Code verwendet wird.

nPA
Der neue elektronische Personalausweis: neuste Bezeichnung für den ePA, siehe ePA

OCR
Optical Character Recognition, Standardschrift-Art in MRZ, siehe auch MRZ

PACE
Password Authenticated Connection Establishment, siehe Seite 16

PAuswG
Personalausweisgesetz: Gesetz über Personalausweise und den elektronischen Identitätsnachweis

PKI
Public-Key-Infrastructure, siehe Seite 14

RFID
Radio-Frequence Identification

SAML
Security Assertion Markup Language

SOAP
Simple Object Access Protocol

TLS
Transport Layer Security (bis Version 3.0 SSL (Secure Socket Layer) genannt): Verschlüsselungsprotokoll zur sicheren Datenübertragung im Internet

TR
Technische Richtlinie

VfB
Vergabestelle für Berechtigungszertifikate des Bundesverwaltungsamtes (BVA)

VPN
Virtual Private Network: sichere Kommunikationsverbindung in einem Netzwerk

8 Eidesstattliche Erklärung

Hiermit versichere ich, dass ich die Seminararbeit mit dem Thema

„Einsatzmöglichkeiten
der neuen elektronischen Personalausweise
im Zutrittskontroll-Management“

selbständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt habe, alle Ausführungen, die anderen Schriften wörtlich oder sinngemäß entnommen wurden, kenntlich gemacht sind und die Arbeit in gleicher oder ähnlicher Form noch nicht Bestandteil einer Studien- oder Prüfungsleistung war.

Name des Autors: Olaf Hinkens

Aachen, den 12.12.2011

Unterschrift des Studenten: