Der neue, elektronische Personalausweis

Maximilian Imhof
Betreuer: Holger Kinkelin
Seminar Future Internet SS2011
Lehrstuhl Netzarchitekturen und Netzdienste
Fakultät für Informatik, Technische Universität München
E-Mail: imhof@in.tum.de

KURZFASSUNG

Jeder Bundesbürger ist dazu verpflichtet, ab seinem 16. Lebensjahr ein Ausweisdokument mit sich zu führen. Aufgrund dessen wird jeder Bürger früher oder später den neuen Personalausweis beantragen müssen. Bislang gab es weder einen Standard-Identitätsnachweis für die Online-Welt, noch war es möglich rechtskräftige Willenserklärungen im Internet abzuschließen. Der fehlende Identitätsnachweis ermöglicht Cyberkriminalität wie zum Beispiel Phishing oder Identitätsdiebstahl. Die Einführung des neuen, innovativen Personalausweises soll Onlinegeschäfte erleichtern und die Kriminalität im zukünftigen Internet erschweren oder gänzlich verhindern. Um den elektronischen Identitätsnachweis zu realisieren, wurde eine neue Infrastruktur mit dazugehörigen Sicherheitsmerkmalen entwickelt. Am 1. November 2010 war es soweit und der neue Ausweis wurde eingeführt. Doch neben den innovativen Vorteilen kamen auch Sicherheitslücken sowie weitere Probleme zum Vorschein. Der Personalausweis ist in der hoheitlichen Funktion im Moment das sicherste Ausweisdokument in Deutschland. Die Nutzung der Onlinefunktionen muss sich allerdings noch bei den Nutzern sowie bei den Dienstanbietern etablieren.

Schlüsselworte

nPA, eID, QES, Infrastruktur, PersAuswG, CAN, eID-PIN, PACE, EAC, PA, PKI, CSCA, CVCA

1. EINLEITUNG

„1400 Buchdruck, 1930 Fernseher, 1941 Computer, 1956 Faxgerät, 1969 Kartenchip, 1. November 2010 elektronischer Personalausweis". Unter dem Titel „Gute Ideen aus Deutschland" wirbt das Bundesministerium des Inneren (BMI) für den neuen Personalausweis [7]. Seit dem 1. November 2010 kann dieser in Deutschland in den Bürgerämtern beantragt werden. Die elektronische Multifunktionskarte gilt im Reiseverkehr, in der Personenkontrolle sowie in der elektronischen Welt. Der Ausweis wurde nicht nur als modernes, sichereres hoheitliches Dokument eingeführt, sondern auch mit zusätzlichen elektronischen Funktionen versehen, wie dem elektronischen Identitätsnachweis (eID) und der qualifizierten elektronische Signatur (QES). Mit diesen Funktionen können Onlinegeschäfte des alltäglichen Lebens sicherer abgeschlossen und Verträge unterzeichnet werden.

Im folgenden Abschnitt wird allgemein auf den neuen Personalausweis eingegangen. Im Besonderen werden die Einführung, der Aufbau mit den Erneuerungen und weitere Informationen die zu beachten sind, erläutert. Der dritteAbschnitt gibt einen Überblick über die drei neuen Funktionen: Die hoheitliche Biometriefunktion, der elektronische Identitätsnachweis und die qualifizierte elektronische Signatur. Der elektronische Identitätsnachweis wird Allgemein erläutert. Desweiteren wird die Infrastruktur beschrieben. Im Anschluss werden die Komponenten zur Nutzung der Funktionen für die Bürger als auch für Unternehmen veranschaulicht. Der 5. Abschnitt handelt von Sicherheitsmechanismen zum Schutz der personenbezogenen Daten. Die Sicherheitslücken werden neben weiteren Problematiken im nächsten Abschnitt thematisiert. Abschließend wird ein kurzes Fazit gegeben.

2. ALLGEMEIN

Schon im Mittelalter musste man sich mit Wappen, Orden oder Zunftzeichen ausweisen. In der Bundesrepublik gibt es seit 1951 einen Pass. Hingegen wurde in der damaligen DDR erst 1953 ein Ausweisdokument eingeführt. Der Personalausweis, den wir bis vor kurzem noch hatten und zum Teil noch haben, existiert seit dem 1. April 1987. Am 18. Dezember 2008 wurde der neue Personalausweis, auch nPA[1] genannt, vom Bundestag bewilligt und am 1. November 2010 eigeführt. Neben dem neuen Ausweis trat auch das „Gesetz über Personalausweise und den elektronischen Identitätsnachweis" (PersAuswG) in Kraft [12].

Der Ausweis wurde mit dem Hintergrund eingeführt, ein neues, sichereres Ausweisdokument zu schaffen. Durch die neuen Funktionen soll das Dokument viele Dienstleistungen der öffentlichen Verwaltung sowie Aktivitäten und Einkäufe des alltäglichen Lebens erleichtern. Einen standardisierten, elektronischen Identitätsnachweis gab es bislang noch nicht. So ist es fortan möglich sich gegenüber Behörden in Bereichen des E-Gouvernements auszuweisen. Dadurch kann sich der Bürger „lästige" Behördengänge ersparen. Des Weiteren ist das Ausweisen im Bereich des E-Business möglich und wird als schneller, einfacher und sicherer vom Bundesministerium des Inneren beschrieben. Folglich soll der Ausweis Internetgeschäfte sicherer machen und Cyberkriminalität wie Phishing und Identitätsdiebstahl verhindern.

Der neue deutsche Personalausweis ist fünf Gramm leicht, grün-blau unterlegt und wird aus Polykarbonat hergestellt. Er besitzt nicht mehr wie der Alte das ID-2

[1]Sollte erst „elektronischer Personalausweis" (ePA) genannt werden, jedoch führte Kritik an diesem Namen zur Umbenennung in „neuer Personalausweis" (nPA)

doi: 10.2313/NET-2011-07-2_07

Format sondern hat mit 8,6cm Länge und 5,4cm Breite die gleichen Abmessungen wie übliche Scheckkarten und ist somit im Besitz des ID-1 Formats. Wie schon der Vorgänger enthält dieser Ausweis zahlreiche Sicherheitsmerkmale, welche die Fälschungssicherheit erhöhen. Er verfügt über mehrfarbige Guillochen, Mikroschriften, UV-Aufdrucke, einen 3-D Bundesadler, Kontrastschriften, Melinfasern, ein Laserkippbild und viele weitere Merkmale [17]. Auf der Vorderseite ist der Familienname sowie der Geburtsname, der Vorname, ein gegebenenfalls vorhandener Doktorgrad, Tag und Ort der Geburt, die Staatsangehörigkeit, das Lichtbild, die Unterschrift, Gültigkeitsdatum, die Seriennummer und die Card Access Number (CAN) zu lesen. Die Card Access Number ist eine auf der Vorderseite des Personalausweises aufgedruckte sechsstellige dezimale zufällige Nummer. Die CAN lässt sich nicht aus personen- oder dokumentenbezogenen Daten berechnen. Die Card Access Number wird bei der hoheitlichen Biometriefunktion (siehe auch 3.1), der Änderung von Daten in den Ausweisbehöden sowie beim Verbindungsaufbau zur Signaturanwendung benötigt. Neben den Aufgedruckten Daten ist auf der Vorderseite, wie in Abbildung 1, das biometrische Passbild zu erkennen.

Abbildung 1: Ausweisansicht Vorderseite [16]

Auf der Rückseite des Ausweisdokumentes befinden sich die Augenfarbe, die Größe, die Anschrift, die Stadt mit Postleizahl der ausstellenden Behörde, Ausstelldatum, Ordens- bzw. Künstlername und das Logo sowie die maschinenlesbare Zone(MRZ). Die Ansicht auf die Rückseite des Ausweises ist in Abbildung 2 dargestellt.
Im Vergleich zum vorherigen Ausweis sind die CAN und die Postleizahl neu hinzugekommen. Das Ausweisdokument ist nach ISO 14443 mit einem kontaktlosen Chip ausgestattet. Auf dem Dokument sind nach §5 Abs. 5 PersAuswG Familienname, Geburtsname, Vorname, Doktorgrad, Tag und Ort der Geburt, Lichtbild, Anschrift, Staatsangehörigkeit, Seriennummer, Ordensname beziehungsweise Künstlername und die Daten der maschinenlesbaren Zone auf dem radio-frequency identification(RFID)-Chip gespeichert[12]. Neben den genannten Daten können auch freiwillig Fingerabdrücke, sowie die Qualität und Bezeichnung dieser gespeichert werden. Diese Daten dienen zur eindeutigen Zuordnung von Ausweis und Inhaber.

Abbildung 2: Ausweisansicht Rückseite [16]

Nach §1 Abs. 1 des PersAuswG ist jeder Bürger, der die deutsche Staatsangehörigkeit innehat und somit der Meldepflicht unterliegt, oder sich überwiegend in Deutschland aufhält, ab 16 Jahren dazu verpflichtet einen Ausweis zu besitzen. Kinder und Jugendliche unter 16 Jahren können ebenfalls einen Personalausweis beantragen, allerdings ohne den elektronischen Identitätsnachweis. Bei der Beantragung werden ein aktuelles, biometrisches Lichtbild und ein gültiges Identitätsdokument benötigt. Die eID kann jederzeit im Bürgeramt nachträglich ein- oder ausgeschaltet werden. Der Personalausweis kostet für Personen ab 24 Jahren 28,80 Euro und für Antragsteller unter 24 Jahren 22,80 Euro. Er ist mehr als 3,5 mal so teuer wie der alte Ausweis. Weitere Kosten sind in der „Gebührenverordnung für den neuen Personalausweis“ zu entnehmen[8].

Bei Verlust oder Diebstahl des Ausweises ist der Inhaber dazu verpflichtet, den Verlust der Personalausweisbehörde zu melden. Hat der Ausweis die eID Funktion, muss diese mit Hilfe des Sperrkennworts gesperrt werden. Dies sollte schnellstmöglich im Bürgeramt oder über den 24-Stundensperrnotruf 0180-1-33 33 33[2] geschehen. Falls auch die Qualifizierte Elektronische Signatur genutzt wird, muss das Signaturzertifikat beim jeweiligen Anbieter gesperrt werden.

3. FUNKTIONEN

Das Ausweisdokument dient weiterhin als Sichtausweis, wurde jedoch um zusätzliche Funktionen ergänzt. Die hoheitliche Biometriefunktion soll das Ausweisen an Grenzkontrollen erleichtern und den Ausweis sicherer machen. Zusätzlich kann der elektronische Identitätsnachweis und die qualifizierte elektronische Signatur beantragt werden. Um diese freiwilligen Funktionen zu nutzen, wird eine Software, welche als Schnittstelle zwischen Ausweis, Kartenlesegerät und der einzelnen Funktion fungiert, benötigt. Diese Software wird

[2]3,9 Ct/Min. aus dem dt. Festnetz, aus dem Mobilfunknetz maximal 42 Ct/Min.. Auch aus dem Ausland erreichbar

doi: 10.2313/NET-2011-07-2_07

vom Bundesamt für Sicherheit in der Informationstechnik (BSI) für Windows, Linux und MacOS zur Verfügung gestellt und trägt den Namen „AusweisApp“[3]. Im Folgenden werden die einzelnen Funktionen betrachtet. Es wird besonders auf den elektronischen Identitätsnachweis eingegangen.

3.1 Die Hoheitliche Biometriefunktion

Mit dem Terrorismusbekämpfungsgesetz vom 9. Januar 2002 wurden die biometrischen Merkmale mit in den deutschen Personalausweis aufgenommen. Der nPA ist weiterhin als Sichtausweis verwendbar und als Passersatz innerhalb der Europäischen Union gültig. Die elektronisch gespeicherten Daten sind nur mit einem hoheitlichen Berechtigungszertifikat auslesbar. Biometrische Daten dürfen nur von Polizeivollzug, Zoll, Steuerfahndung der Länder, sowie der Pass-, Personalausweis- und Meldebehörden ausgelesen werden. Um die biometrischen Daten auszulesen, muss die auf dem Ausweis aufgedruckte Card Access Number eingegeben werden. Um Grenzkontrollen zu beschleunigen kann statt der CAN das Basic Access Control (BAC) Verfahren verwendet werden. Bei diesem Verfahren liest das Durchzugslesegerät der Behörden die optischen Daten aus der MRZ und erstellt einen SHA-1-Hashwert aus der 9 stelligen Seriennummer, dem Geburtsdatum und dem Ablaufdatum. Die ersten 16 Byte des Hashwertes bilden einen Schlüssel. Der Ausweischip hat ebenfalls anhand der eigenen Daten einen Schlüssel berechnet. Sind diese Schlüssel gleich, wird ein gemeinsamer Schlüssel zwischen Chip und Lesegerät bestimmt. Darauffolgend gibt der Chip die Daten für das Lesegerät frei.[9]

3.2 Der elektronische Identitätsnachweis

Die wohl größte Innovation des neuen Personalausweises ist der elektronische Identitätsnachweis, welcher als Online-Authentifizierung am PC dient. Mit den auf dem Ausweis gespeicherten Datenfeldern kann sich der Ausweisinhaber im elektronischen Rechts- und Geschäftsverkehr eindeutig identifizieren. Der Inhaber legitimiert sich über den Personalausweis und seine eID-PIN. Die Dienstanbieter weisen sich mit einem staatlichen Berechtigungszertifikat aus. Das Zertifikat gestattet nur das Auslesen der im Berechtigungszertifikat aufgeführten Datenfelder und die Gültigkeit des Ausweises. Um dies zu ermöglichen wurde eine neue Infrastruktur realisiert.

3.2.1 aus der Sicht des Anwenders

Möchte der Ausweisnutzer die elektronische Identifikation auf einer Website nutzen, klickt er auf den eID-Button. Folglich öffnet sich die AusweisApp lokal auf seinem Rechner. Für den Nutzer gibt es vier sichtbare Schritte in der Applikation. Im ersten Schritt erfährt der Benutzer, wer auf seinen Ausweis zugreifen will, wie lange dessen Berechtigungszertifikat gültig ist und von wem das Zertifikat ausgestellt wurde. Im nächsten Schritt zeigt die Anwendung eine Übersicht, der von dem Dienstanbieter angeforderten Datenfelder. Daraufhin kann der Benutzer Datenfelder hinzufügen oder entfernen. Im dritten Schritt muss der Nutzer seine eID-PIN eingeben um die Daten freizugeben. Im letzten Abschnitt werden die PIN, sowie die Gültigkeit des Personalausweises und die Anbieterberechtigung geprüft. Wenn die Überprüfung erfolgreich war, werden die Daten übertragen. Infolgedessen schließt sich die Applikation und das Ergebnis wird im Browser dargestellt.

[3]Download auf www.ausweisapp.bund.de

3.2.2 eID-PIN

Nach Beantragung eines Ausweises mit eID wird ein PIN-Brief per Post, welcher eine 5-stellige zufällige Transport-PIN, die PUK Nummer und ein Sperrkennwort beinhaltet, zugestellt. Diese 5-stellige Nummer, muss durch einen 6-stellige, dezimale persönliche eID-PIN beim Bürgeramt oder an einem passenden Lesegerät ersetzt werden. Ohne eigene eID-PIN ist die eID Funktion nicht nutzbar. Um das Erraten der eID-PIN durch Ausprobieren zu verhindern enthält der Chip einen Fehlbedienungszähler (FBZ), welcher die die Karte nach drei falschen Eingaben sperrt. Der dritte Eingabeversuch ist erst nach Eingabe der CAN möglich um einen Denial of Service-Angriff zu verhindern. Das PIN-Schema ist in Abbildung 3 dargestellt.

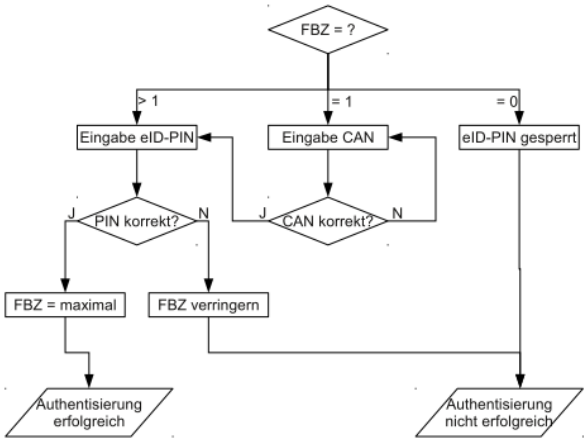

Abbildung 3: Eingabe der eID-PIN [5]

3.2.3 Pseudonym

Der Personalausweisinhaber hat die Möglichkeit sich bei Internetdiensten mit Pseudonymen anzumelden. Dieses Pseudonym wird bei jeder späteren Anmeldung vom Dienstanbieter wiedererkannt und ohne personenbezogene Daten wie zum Beispiel Name und Adresse weitergegeben. Diese Funktion ist karten- und dienstspezifisch, dies bedeutet, dass für jedes Pseudonym ein Schlüssel aus einem Ausweis-Chipschlüssel und Schlüssel des Betreibers berechnet wird. Somit ist das Abgleichen der Datenbanken von Dienstanbietern, um personenbezogene Daten zu bekommen, nutzlos.

3.2.4 Infrastruktur

Auf der Seite des Bürgers ist der Kartenleser an den PC angeschlossen. Auf diesem PC ist die AusweisApp installiert. Ein Plug-in im Browser startet diese Applikation bei dem Aufruf der eID Funktion. Auf Seiten des Dienstanbieters, wie in Abbildung 3 zu erkennen, arbeitet ein Webserver als Frontend, welcher über einen eID-Connector mit dem eID-Server kommuniziert. Der eID-Server, der entweder vom Betreiber der Website oder einem weiteren Dienstanbieter unterhalten wird, übernimmt die Kommunikation mit der AusweisApp, den Abruf von Berechtigungszertifikaten und der Sperrliste. Die Sperrliste ist eine Liste, welche die gesperrten Ausweise beinhaltet. Als Schnittstelle wird

doi: 10.2313/NET-2011-07-2_07

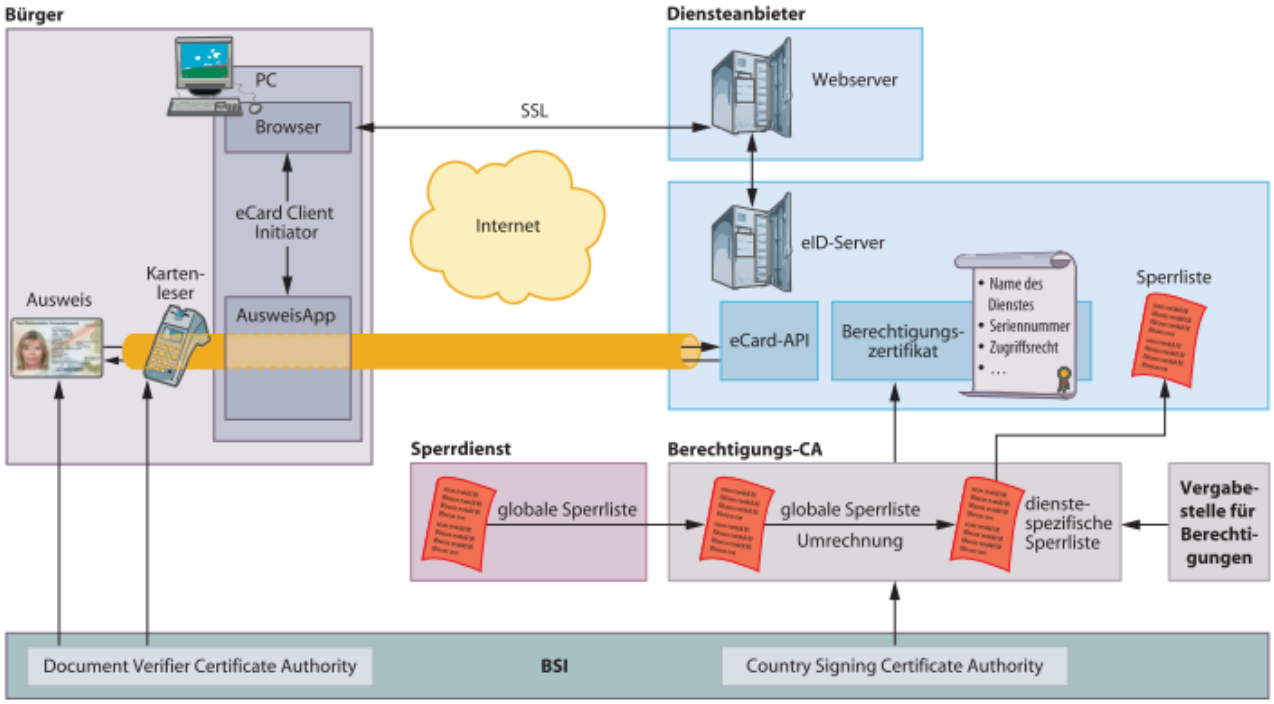

Abbildung 4: Infrastruktur [1]

die eCard-API verwendet. Die Daten werden zwischen eID-Server und Webserver, bei einem offenen Netz, verschlüsselt und signiert übertragen. Klickt nun der Ausweisinhaber auf die eID-Funktion auf einer Website eines Dienstanbieters, öffnet sich lokal die Applikation. Diese erhält die notwendigen Parameter wie zum Beispiel die Adresse des zuständigen eID-Servers. Mit dem Erhalt der Parameter wird der sichere Verbindungsaufbau zwischen Chip des Ausweises und dem eID-Server veranlasst. Diese Verbindung ist in Abbildung 4 zu erkennen. Die Zugriffskontrolle übernimmt das PACE-Protokoll (siehe 5.1) um die Verbindung abzusichern. Der eID-Server muss seine Leseberechtigung mit einem Zertifikat nachweisen.

3.3 Die qualifizierte elektronische Signatur

Neben dem elektronischen Identitätsnachweis wurde die qualifizierte elektronische Signatur, auch Unterschriftsfunktion genannt, eingeführt. Diese ermöglicht dem Auswisinhaber das digitale Signieren von Dokumenten.

3.3.1 Allgemein

Der Ausweisinhaber kann freiwillig, je nach Bedarf die Unterschriftfunktion auf seinem Ausweis aktivieren. Für die Nutzung der Funktion wird ein Signaturzertifikat benötigt. Dieses verursacht jährliche Zusatzkosten in Höhe von ungefähr 60 bis 80 Euro. Die Signatur wird von verschiedenen Anbietern angeboten, hierdurch entsteht der Unterschied in den Kosten. Wie bei der eID-Funktion ist eine Geheimnummer, die Signatur-PIN erforderlich. Zum Auslieferungszeitpunkt des Ausweises ist keine Signatur-PIN gesetzt, das heißt der Inhaber muss diese PIN selbst bestimmen. Die Signatur ist der eigenhändigen Unterschrift rechtlich gleichgestellt und es können somit rechtsverbindliche Willenserklärungen abgegeben werden. Aus diesem Grund sind die Anforderungen an die Sicherheit größer als bei der eID. Die QES kann nur mit einem Komfortlesegerät (siehe 4.1) genutzt werden.

3.3.2 aus der Sicht des Anwenders

Möchte der Bürger ein Dokument signieren, öffnet er die AusweisApp. Zunächst muss die zu signierende Datei ausgewählt werden. Daraufhin wird der Ausweisinhaber nach der auf dem Ausweis aufgedruckten CAN gefragt. Infolgedessen kann der TrustedViewer[4] den Inhalt des zu unterzeichnenden Dokuments anzeigen und warnt vor unsichtbaren Inhalten. Mit der Eingabe der Signatur-PIN ist das Dokument unterschrieben. Nachträgliche Veränderungen des Dokuments werden angezeigt.

4. KOMPONENTEN ZUR NUTZUNG

Um Funktionen wie eID oder QES zu nutzen, wird gewisses Zubehör benötigt. Was benötigt wird und welche Kosten dabei für Nutzer und Unternehmen anfallen wird in diesem Abschnitt genauer dargestellt. Es wird auf die Komponenten sowie auf die entstehenden Kosten näher eingegangen.

4.1 Für Ausweisinhaber

Für die Nutzung der elektronischen Identifikation und der qualifizierten elektronischen Signatur wird neben der AusweisApp auch ein kontaktloses Kartenlesegerät benötigt. Es gibt drei verschiedene Arten von Lesegeräten: den Basisleser für 10 bis 25 Euro, den Standardleser für 30 bis 80 Euro und den Komfortleser für 90 bis 160 Euro. Lesegeräte sind im freien Handel zu erwerben. Somit ist der Preisunterschied zu erklären. Für die eID-Funktion reicht ein Basislesegerät aus,

[4]Der TrustedViewer ist ein Programm welches das Dokument vor der Unterzeichnung auf versteckte Inhalte überprüft

doi: 10.2313/NET-2011-07-2_07

bei welchem die PIN über den Computer eingegeben werden muss. Das Standardlesegerät hat ein seperates Tastenfeld sowie ein Display. Das Komfortlesegerät hat ebenfalls einPIN-Pad und ein Display. Das Komfortlesegerät ist jedoch mit dem EAL4+ Modul ausgestattet, welches zur Nutzung der QES notwendig ist. Es ist darauf zu achten, dass nur vom BSI zertifizierte Lesegeräte verwendet werden, welche an einem aufgedruckten Personalausweis-Logo zu erkennen sind. Auf der Internetseite der AusweisApp sind die von der Applikation unterstützten Lesegeräte gelistet.

4.2 Für Unternehmen

Damit Unternehmen die eID Funktion nutzen und auf Daten zugreifen können, müssen sie über ein Berechtigungszertifikat verfügen. Diese kann bei der Vergabestelle für Berechtigungszertifikate, welches dem Bundesverwaltungsamt unterliegt, beantragt werden. Laut Detlef Borchers von „C't“ kostet die Beantragung 105 Euro [1]. Zur Beantragung muss das Unternehmen glaubhaft nachweisen, weshalb sie die Datenfelder nutzen möchte. Die Vergabestelle prüft, welche Daten das Unternehmen für seine Zwecke wirklich braucht und ob es ein vertrauenswürdiges Unternehmen ist. Derzeit werden nach Borchers nur zwei Gründe akzeptiert, ein gesetzlicher Grund wie zum Beispiel die Altersverifikation oder, wenn ein erhebliches „kreditorisches Risiko“ angenommen werden muss. Die Zertifikate sind in der Regel drei Jahre gültig, können jedoch auch jederzeit entzogen werden. Um die eID zu nutzen müssen zusätzlich zu dem Zertifikat noch ein eID-Server und Hardware Security Module angeschafft werden. Die Server kosten schätzungsweise 200.000 bis 300.000 Euro, ohne die laufenden Kosten. Für Unternehmen mit geringen Anfragen ist ein eID-Service-Provider die bessere Alternative. Der Provider „]init[“ bietet zwei unterschiedliche Services an. Für die Nutzung von einem Zertifikat bietet „]init[“ den „Trusted eID-Service Premium“ für 250 Euro im Monat plus 750 Euro Einrichtungsgebühr an. Der „Trusted eID-Service Enterprise“ welcher bis zu 16 Berechtigungszertifikate verwalten kann, kostet 2750 Euro im Monat zuzüglich 7500 Euro Einrichtungsgebühr [18]. Der Service, das Hardware Security Modul, von D-Trust, einer Tochterfirma der Bundesdruckerei kostet 250 Euro pro Monat und jedes weitere Modul 150 Euro. Die Einrichtungsgebühr hierfür liegt bei 750 Euro. Zur Beantragungsgebühr, dem Server und dem Modul kommen noch die Zertifikatgebühren hinzu. Das erste Zertifikat kostet 2000 Euro pro Jahr und jedes weitere jeweils 500 Euro pro Jahr. Für Behörden der Bundesländer und Kommunen sind die eID-Server kostenlos. Jedoch muss die Kommune mindestens 5700 Euro im Jahr für das Berechtigungszertifikat bezahlen [1].

5. SICHERHEITSMECHANISMEN

Zur Sicherung der personenbezogenen Daten, welche auf dem kontaktlosen Chip gespeichert sind, wurden neue Sicherheitsmechanismen entwickelt. Unter anderem das Password Authenticated Connection Establishment, das Extended Access Control, die Passive Authentication, sowie die Public Key Infrastructures.

5.1 Password Authenticated Connection Establishment (PACE)

Password Authenticated Connection Establishment, kurz PACE, ist ein kryptografisches Protokoll für den gegenseitigen Authentisierungsmechanismus zwischen Terminal und Chip. PACE wurde vom Bundesamt für Sicherheit in der Informationstechnik für den neuen Personalausweis entwickelt und wird in der Technischen Richtlinie TR-03110 [4] beschrieben. Das PACE-Protokoll sorgt für die verschlüsselte und integritätsgesicherten Kanal zwischen Kartenleser und Chip. Welches Passwort für die Generierung eines Verschlüsslungspassworts benutzt wird hängt vom Lesegerät und Nutzen des Ausweises ab. Zur Nutzer-Authentifikation beim Verwenden der eID-Funktion wird die 6-stellige eID-PIN verwendet. Bei hoheitliche Kontrollen wird die auf dem Kartenkörper aufgedruckte Card Access Number oder die Hashnummer aus der Basic Access Control verwendet[5]. Der Chip generiert eine Zufallszahl, welche er mit dem Passwort über eine Hashfunktion verschlüsselt. Das Lesegerät muss zur Entschlüsselung ebenfalls die Hashfunktion sowie das Passwort kennen. Hat das Lesegerät die geheime Zufallszahl herausgefunden wird ein gemeinsamer symmetrischer AES-Schlüssel für Secure Messaging zwischen Chip und Lesegerät abgeleitet[9]. Kern des Verfahrens ist der Diffie-Hellman-Schlüsseltausch. Das Protokoll soll vor dem unbefugten Auslesen des Chips aus der Entfernung schützen.

5.2 Extended Access Control (EAC)

Extended Access Control, kurz EAC, ist eine erweiterte Zugangskontrolle zwischen Lesegerät oder Dienstanbieter und Chip. EAC besteht aus zwei Unterprotokollen, der Chip Authentication (CA) und der Terminal Authentication (TA). Es wird ebenfalls in den Technischen Richtlinien TR-03110 [4] des BSI beschrieben.

5.2.1 Chip Authentication

Die Chip Authentication dient zur Überprüfung der Echtheit des Chips, sowie dem sicheren Verbindungsaufbau zwischen Chip und Lesegerät, beziehungsweise den Dienstanbietern bei der Nutzung der eID-Funktion. Die CA basiert auf dem Diffie-Hellmann-Schlüsselaustausch. Das Lesegerät nutzt ein flüchtiges Schlüsselpaar und der Chip ein statisches Paar. Der Schlüssel des Ausweischips wird während der Herstellung signiert. Dadurch wird die Echtheit des Chips und damit auch der auf dem Chip gespeicherten Daten nachgewiesen. Weiter dient die Authentifizierung zum Aufbau eines sicheren Kanals zwischen Kartenlesegerät oder Dienstanbierter und RFID-Chip.

5.2.2 Terminal Authentication

Der Zweck der Terminal Authentication ist die Authentisierung des Lesegeräts oder eines Dienstanbieters zum Auslesen von Daten. Hierzu verschickt das Lesegerät oder der Dienstanbieter seine Leseberechtigung in Form des Terminal-Zertifikats an den Chip. Des Weiteren wird das Country Verifying Certificate Authority (CVCA) sowie die Zertifikate in der Zertifikat-Hierarchie zwischen Terminal-Zertifikat und CVCA mitgeschickt. Darauf prüft der Chip die Echtheit und Unverfälschtheit des Terminals. Es müssen alle Zertifikate mit dem geheimen Schlüssel des Vorgängers signiert worden sein beginnend mit dem CVCA-Zertifikat um ein positives Ergebnis zu erhalten. Das CVCA-Zertifikat wurde bei der Herstellung des Chips auf dem Chip gespeichert. Wenn die Echtheit und Unverfälschtheit des Terminal-Zertifikates erfolgreich festgestellt wurde, muss geprüft werden ob dieses Zertifikat auch wirklich für dieses Lesegerät ausgestellt wurde. Hierzu schickt der Chip eine Zufallszahl an das Lesegerät.

doi: 10.2313/NET-2011-07-2_07

Die Zahl wird mit dem geheimen Schlüssel des Terminal-Zertifikats signiert und an den Chip zurückgesand. Durch den öffentlichen Schlüssel des Lesegeräts, kann der Chip die Signatur der Zahl überprüfen und feststellen, ob das Lesegerät den passenden Schlüssel besitzt[3].

5.3 Passive Authentication (PA)

Die Passive Authentication, kurz PA, dient zur Überprüfung der Echtheit und Unverfälschtheit der Daten auf dem Chip. Bei der Herstellung des Ausweisdokuments werden die elektronischen Daten mit dem Document Signing-Zertifikat digital signiert. Dieses Zertifikat ist wiederum mit dem Country Signing Certificate Authority (CSCA), welches nur dem Ausweishersteller zur Verfügung steht, signiert. Beim Lesen eines Ausweises wird anhand der passiven Authentisierung die Signatur der Daten geprüft und bis zum CSCA zurückverfolgt. So kann festgestellt werden, ob die Daten vom offiziellen Passhersteller im Chip gespeichert wurden und ob diese unverfälscht sind.

5.4 Public Key Infrastructures (PKI)

Die Public Key Infrastructures, kurz PKI, ist die Hierarchie von digitalen Zertifikaten. Für den Ausweis werden zwei PKI benötigt, die Country Signing Certificate Authority und die Country Verifying Certificate Authority. Diese Infrastrukturen werden in den Technischen Richtlinien TR-03128 [6] beschrieben. Das CSCA ist laut BSI die Hierarchie von digitalen Zertifikaten zur Signierung von Daten in elektronischen Ausweisdokumenten. Dagegen ist das CVCA die Hierarchie von digitalen Zertifikaten zur Leseberechtigung bei elektronischen Ausweisdokumenten[3].

6. SICHERHEITSLÜCKEN UND WEITERE PROBLEME

In der Presse und anderen Medien wird immer wieder Kritik zum Personalausweis ausgeübt. Es heißt, Betrügern sei es problemlos möglich sensible Daten sowie die geheime PIN abzufangen. Die Bundesregierung behauptet hingegen, der Ausweis sei sicher. In der Kritik stehen auch die Umsetzung und die daraus resultierenden Probleme für die Kommunen und den Bürger. Diese Kritik wird im folgenden Abschnitt genauer dargelegt.

6.1 Sicherheitslücke

Der neue Personalausweis geriet wegen Sicherheitsmängel unter heftigen Beschuss in den Medien. So auch vom Westdeutschen Rundfunk (WDR). Dieser thematisierte im „Bericht aus Brüssel“ vom 22. September 2010, 21:55 Uhr, den Ausweis und dessen festgestellte Sicherheitsmängel. Mittelpunkt des geschilderten Angriffsszenarios ist ein mit einem Trojanischen Pferd infizierter Rechner. Die Schadsoftware wurde mithilfe eines Hackerangriffs unbefugt platziert. Der Hacker sieht darauffolgend alle Tastatureingaben oder kann Bildschirmanzeigen mitlesen. Mit Hilfe eines Keyloggers können diese Daten aufgezeichnet werden. Im Beispiel wurde so die PIN herausgefunden und konnte vom Angreifer geändert werden. Im schlimmsten Fall könnte der Hacker online einkaufen oder ein Konto eröffnen. Das BSI nimmt in einer Pressemitteilung [2] Stellung zum „Bericht aus Brüssel“ und weist die Sicherheitsbedenken erneut zurück. So heißt es in dieser, der Angreifer könne zwar die PIN erspähen und ändern, aber dies würde zur Entdeckung des Angriffs und somit zur Sperrung des Ausweises führen. Darüber hinaus zählt das BSI grundlegende Sicherheitsmaßnahmen im Umgang mit dem Ausweis auf. Peter Schaar, der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, äußerte sich in einer Pressemitteilung [13] zum Personalausweis am 29.Oktober 2010: „Wer die Gefahr des Ausspähens der PIN mittels einer Schadsoftware umgehen will, sollte lieber ein höherwertiges Lesegerät einsetzen“. Das Ausspähen der PIN ist ausschließlich bei der Nutzung eines Basislesers möglich. Grund hierfür ist, dass Basisleser nicht über eine PC externe Hardware zum Eingeben der PIN verfügen. Des Weiteren ist ein Angriff nur möglich, wenn der Ausweis auf dem Lesegerät liegt. Der Ausweis sollte daher laut BSI immer sicher verwahrt werden und nur bei Nutzung auf das Lesegerät gelegt werden. Aufgrund dieser Tatsachen gilt der neue Personalausweis als sichere Alternative zu den ursprünglich Benutzerdaten im E-Business. Jedoch belegen Banking-Trojaner, dass Betrüger sicher bereit sind, vergleichbaren Aufwand zu betreiben, wenn die Gewinnerwartung hoch genug ist. Für die Nutzer der eID und der QES ist die Nutzung und ständige Aktualisierung von Firewall, Antivirensoftware und Systemupdates im eigenen Interesse Pflicht.

6.2 Weitere Probleme

Neben den Sicherheitslücken im technischen Bereich sind auch zusätzliche Probleme entstanden. Probleme wie die Schlüsselfunktion des Staates, die Belastung für die Verwaltung und die Akzeptanz des Ausweises. Desweiteren ist die Haftung bei Angriffen zu nennen. Auf diese Schwachstellen wird in den folgenden Abschnitten näher eingegangen.

6.2.1 Einführung durch den Staat

Die technische Sicherheit und die Sicherheitslücken sind die eine Seite. Auf der anderen Seite hingegen steht die Kritik an der politischen Sicherheit. Peter Schaar kritisierte in seinem Vortrag auf dem Chipkarten-Kongress Omnicard 2011, dass der Staat nun „ein neue Schlüsselfunktion“ zwischen Konsumenten und Dienstanbietern einnimmt. Dies geschieht durch die Zertifikatausteilung und -entziehung.

6.2.2 Belastung für Verwaltung

Ein weiteres Problem bei der Einführung des Ausweisdokuments ist die zusätzliche Belastung für Kommunen und Ordnungsämter. So schrieb die Hessische/Niedersächsische Allgemeine Zeitung am 23.07.2010: „Der neue Ausweis, der ab dem 1. November beantragt werden kann, soll 28,80 Euro kosten. Die sechs Euro, die davon bei den Städten und Gemeinden bleiben sollen, reichten nicht, um deren Kosten zu decken. 22,70 Euro gehen an den Hersteller, zehn Cent fließen in die notwendigen Computerprogramme. Grund für die Mehrkosten bei den Städten ist vor allem eine längere Bearbeitungszeit: Bisher kalkulieren sie mit siebeneinhalb Minuten Bearbeitungszeit für einen Ausweis“ [15]. Das Hamburger Abendblatt datierte den Personalaufwand auf bis zu dreimal so hoch wie bisher [14]. Darüber hinaus müssen die Mitarbeiter auf den neuen Ausweis geschult werden. Anton Hanfstengl, Leiter des Bürgerbüros München berichtet davon, dass sich die Änderungsterminals der Bundesdruckerei für PIN und PUK oft aufhängen und sich somit die Ausweisausgabe verzögert [11]. Jedoch ist das größte Bedenken der Bürgerämter, dass die Bürger bei technischen Problemen mit Kartenlesern oder Software die Bürgerbüros aufsuchen.

doi: 10.2313/NET-2011-07-2_07

6.2.3 Basisleser und Haftung bei Angriffen

Im Rahmen des IT-Investitionsprogramms des Konjunkturpakets II stellt der Bund 24 Millionen Euro für die Förderung von Lesegeräten zur Verfügung. Durch diese Unterstützung können rund 1,5 Millionen IT-Sicherheitskits kostenfrei oder verbilligt ausgegeben werden. Diese Kits enthalten einen Basiskartenleser und Informationsbroschüren zur Nutzung mit Chipkarten. Die Verteilung dieser Kits wird jedoch kritisiert, da die Basisleser als unsicher gelten. Der Staat haftet nicht bei Hackerangriffen, so Ex-Bundesinnenminister de Maizière in einem Interview mit Plusminus vom 24. August 2010. Somit bleibt den Nutzern bei Angriffen nur die Hoffnung auf Kulanz bei Dienstanbietern.

6.2.4 Akzeptanz des Ausweises

Das Bundesministerium des Innern hat eine Studie von der Universität Potsdam durchführen lassen, um die Akzeptanz des neuen Personalausweises zu prüfen [10]. Untersucht wurden drei Zielgruppen, die Bürger, die Verwaltung und die Unternehmen. Die Studie zeigte, dass es bei den Bürgern Skepsis aber auch Begeisterung gibt. So weiß ein Drittel noch gar nicht über den neuen Personalausweis Bescheid. Jedoch will jeder zehnte Bürger noch vor Ablauf seines alten Ausweises den Neuen beantragen. Auf Seiten der Unternehmer sind die Funktionen des Ausweisdokumentes weitestgehend unbekannt. So gibt es derzeit erst wenige Unternehmen die die Nutzung der eID-Funktion anbieten[5]. Die großen Internationalen Unternehmen wie Google, Amazon, PayPal oder eBay werden nach eigenen Aussagen die Entwicklung des neuen Personalausweises beobachten.

7. FAZIT

Zusammenfassend kann festgestellt werden, dass der neue Personalausweis ein sicheres Ausweisdokument darstellt. Wer den elektronischen Identitätsnachweis nutzen möchte, kann das Vertrauensverhältnis zwischen Verbrauchern und Dienstanbietern im Internet durch mehr Sicherheit verbessern. Der Ausweisinhaber kann mit der qualifizierten elektronischen Signatur fortan rechtsgeschäftliche Abschlüsse elektronisch tätigen, was den Geschäftsverkehr erleichtert und beschleunigt. Dadurch setzt Deutschland neue Maßstäbe im Identitätsmanagement. Doch den Ausweis neben Erfindungen, wie den Buchdruck oder das Auto zu stellen ist vom Bundesministerium des Inneren übertrieben. Weiterhin ist die Belastung in der Verwaltung kritisch zu betrachten, denn die Bürgerämter sind jetzt schon überfordert. Ebenso zeigt die Studie, dass die Bürger und vorallem die Unternehmen der Bundesrepublik Deutschland bisher wenig über den neuen Personalausweis Informiert sind. Die frühe Einführung zeigt die Dringlichkeit mit welcher der Staat dieses Dokument herbeiführen wollte. Trotz der neu entwickelten Sicherheitsmechanismen ist aufgrund der aufgezeigten Sicherheitslücke das Nutzen eines Basislesers nicht zu empfehlen. Ein Standardleser oder Komfortleser ist daher zu bevorzugen. Letztendlich bleibt abzuwarten, inwieweit die neuen Funktionen des Personalausweises von den Bürgern und Unternehmen akzeptiert und zu einem festen Bestandteil des Internets werden.

[5]Eine Liste von Unternehmen ist unter www.npa-in-aktion.de zu finden

8. LITERATUR

[1] Detlef Borchers: *Digitale Identität: Anwendungszenarien für den elektronischen Personalausweis*, Report, C't, Heise Zeritschriften Verlag, Oktober 2010

[2] Bundesamt für Sicherheit in der Informationstechnik: *BSI weist Sicherheitsbedenken zum neuen Personalausweis erneut zurück*, Pressemitteilung, Bonn, September 2010

[3] Bundesamt für Sicherheit in der Informationstechnik: *Innovationen für eine eID-Architektur in Deutschland*, Broschüre, Bonn, September 2010

[4] Bundesamt für Sicherheit in der Informationstechnik: *Technical Guideline TR-03110: Advanced Security Mechanisms for Machine Readable Travel Documents*, Version 2.05, Technische Richtlinie, Bonn, Oktober 2010

[5] Bundesamt für Sicherheit in der Informationstechnik: *Technische Richtlinie TR-03127: Architektur elektronischer Personalausweis und elektronischer Aufenthaltstitel*, Version 1.13, Technische Richtlinie, Bonn, Oktober 2010

[6] Bundesamt für Sicherheit in der Informationstechnik: *Technische Richtlinie TR-03128: EAC-PKI'n für den elektronischen Personalausweis*, Version 1.1, Technische Richtlinie, Bonn, Oktober 2010

[7] Bundesministerium des Inneren: *Der elektronische Personalausweis*, Broschüre, Berlin, Februar 2009

[8] Bundesministerium des Inneren: *Gebührenverordnung für den neuen Personalausweis*, Gebührenverordnung, Berlin, August 2010

[9] Prof. Dr. Claudia Eckert: *Vorlesung IT-Sicherheit, WS 10/11*, Vorlesung, München, Januar 2011

[10] Jasper Hugo Grote, Daniela Keizer, Dominik Kenzler, Patrick Kenzler, Prof. Dr. Christoph Meinel, Maxim Schnjakin, Lisa Zoth: *Vom Client zur App: Ideenkatalog zur Gestaltung der Software zum Einsatz des neuen Personalausweises*, Universität Potsdam, Studie, Potsdam, September 2010

[11] Kolja Kröger: *Computer-Probleme mit dem neuen Personalausweis*, Artikel, merkur-online, München, Dezember 2010

[12] Horst Köhler, Dr. Angela Merkel, Dr. Wolfgang Schäuble: *Gesetz über Personalausweise und den elektronischen Identitätsnachweis sowie zur Änderung weiterer Vorschriften*, Gesetz, Bundesanzeiger Verlag, Berlin, Juni 2009

[13] Peter Schaar: *Neuer Personalausweis: Sie haben die Wahl!*, Pressemitteilung, Bonn / Berlin, Oktober 2010

[14] Fabian Schindler: *Neuer Ausweis - Kommunen fürchten hohe Kosten*, Zeitungsartikel, Hamburger Abendblatt, Hamburg, Juli 2010

[15] Olaf Weiß: *Neuer Personalausweis: Hohe Kosten für Städte und Gemeinden*, Zeitungsartikel, Hessische Allgemeine, Northeim, Juli 2010

[16] *Aufbau Personalausweis*, `http://www.personalausweisportal.de/SharedDocs/Bilder/DE/Ausweisansicht.jpg?__blob=poster&v=7,(26.03.2011,17.34Uhr)`

[17] *Sicherheitsmerkmale des neuen Personalausweises*, `http://www.personalausweisportal.de/`

doi: 10.2313/NET-2011-07-2_07

SharedDocs/Downloads/DE/Flyer_Bundesdruckerei_
Sicherheitsmerkmale_nPA.pdf?__blob=
publicationFile,(30.03.2011,12.37Uhr)
[18] *Trusted eID-Services*, http://www.init.de/sites/
default/files/downloads/Trusted_eID-Services_
print.pdf,(04.04.2011,15.00Uhr)

doi: 10.2313/NET-2011-07-2_07