Hochschule Reutlingen
Reutlingen University

INF
Informatik

Uwe Kloos, Natividad Martínez, Gabriela Tullius (Hrsg.)

Informatics Inside
Digital Future

Informatik-Konferenz an der Hochschule Reutlingen
10. Mai 2017

ISBN 978-3-00-056455-0

Impressum

Anschrift:
Hochschule Reutlingen / Reutlingen University
Fakultät Informatik
Human-Centered Computing
Alteburgstraße 150
D-72762 Reutlingen

Telefon: +49 7121 / 271-4002
Telefax: +49 7121 / 271-4042

E-Mail: infoinside@reutlingen-university.de
Internet: http://www.infoinside.reutlingen-university.de

Organisationskomitee:
Prof. Dr. Gabriela Tullius, Hochschule Reutlingen
Prof. Dr. Natividad Martínez, Hochschule Reutlingen
Prof. Dr. Uwe Kloos, Hochschule Reutlingen

Lukas Brand
Heiko Brumme
Tobias Fleischer
Gamze Gök
Isabel Hagen
Denise Junger
Mücahit Karabulut
Dina Kurbanismailova
Arjana Mehmeti
Armin Müller
Iana Preuß
Marc Roswag
Anastasia Schmieder
David Schneider
Oliver Streicher
Benjamin Weinert

Hochschule Reutlingen
Reutlingen University

Herstellung und Verlag: Hochschule Reutlingen
ISBN 978-3-00-056455-0

Inhaltsverzeichnis

Longpaper

Zukunft des neuen elektronischen Personalausweises

David Schneider
Reutlingen University
David.Schneider@Student.Reutlingen-University.DE

Abstract

Diese Arbeit beschäftigt sich mit dem neuen elektronischen Personalausweis. Zum einen werden in diesem Paper die Sicherheitsziele des Personalausweises und die technische Umsetzung der Architektur und Protokolle erklärt. Es wird der Ablauf einer Online-Identifizierung für einen Nutzer mithilfe des Ausweises aufgezeigt. Risiken und Schwachstellen der Technologie im Software- oder Hardwarebereich werden diskutiert und die bereits erfolgten Hack-Angriffe aufgezeigt. Die Arbeit legt Möglichkeiten dar, wie sich der Nutzer vor Angriffen schützen kann. Es werden die Gründe genannt warum der neue Personalausweis online nur schwer Anklang findet und warum die Aufklärung, über die zur Verfügung stehenden Anwendungen, eine Preisreduzierung der Lesegeräte sowie die vom Europa Parlament und Europarat erlassene eIDAS-Verordnung nicht helfen werden um die Nutzung voranzutreiben. Ergebnisse hierfür liefert eine Nutzerstudie. Zum anderen werden Ideen genannt wie die Nutzung der elektronischen Funktionen des Ausweises stattdessen zu fördern ist.

Schlüsselwörter

RFID, Authentification Security, Hacking, Risks, German Identity Card.

CR-Kategorien

Algorithms, Design, Human Factors, Security, Standardization.

1 Einführung

Der neue elektronische Personalausweis (nPA) wurde am 1. November 2010 eingeführt und unterscheidet sich von seinem Vorgänger dadurch, dass er über einen integrierten Chip verfügt, welcher sich unsichtbar in der Plastikkarte verbirgt. Durch diesen Chip ist es möglich kontaktlos auf die Daten des nPA zuzugreifen. Die Funktechnik, die hierbei zum Einsatz kommt nennt sich RFID. Das Kürzel stammt aus dem Englischen und steht für *Radio Frequency Identification* zu Deutsch Identifizierung über Funkwellen. Die Technologie bietet die Möglichkeit, Daten auszulesen und auf einem Datenträger (hier: der integrierte Chip) zu speichern, ohne dass eine physische Verbindung oder direkter Sichtkontakt der Kommunikationspartner bestehen muss. Für die Verbindung wird ein Lesegerät benötigt.

1.1 Ziele dieser Arbeit

In dieser Arbeit wird sich ausschließlich mit dem neuen elektronischen Personalausweis

Betreuer Hochschule: Prof. Dr.-Ing. Marcus Schöller
Hochschule Reutlingen
Marcus.Schoeller@Reutlingen-University.de
Informatics Inside 2017
Wissenschaftliche Vertiefungskonferenz
10. Mai 2017, Hochschule Reutlingen

befasst, welcher seit dem 1. November 2010 an deutsche Staatsangehörige ausgegeben wird. Personalausweise die vor diesem Datum ausgestellt wurden, verfügen über keine Funktechnologie und werden daher in dieser Arbeit nicht betrachtet.

Die wesentlichen Neuerungen im Vergleich zum Vorgänger sind nachfolgend beschrieben. Der Ausweis wird nun im ID-1 Format ausgegeben. Es gibt einen Chip im Ausweis mit einer Online-Ausweisfunktion, Lichtbilder können auf dem Chip gespeichert werden, sowie die Fingerabdrücke, dies jedoch auf freiwilliger Basis. Es gibt eine Unterschriftsfunktion die es ermöglicht, rechtsverbindliche Verträge, Anträge, Urkunden etc. elektronisch zu unterschreiben.

Auf die physischen Sicherheitsmerkmale [1], wie Guillochen, Mikroschriften, UV-Aufdruck, optisch variable Farben, holografische Porträts, 3D-Bundesadler, kinematische Bewegungstrukturen etc., wird in dieser Arbeit nicht näher eingegangen, da sich diese Arbeit ausschließlich mit den elektronischen Funktionen des nPAs beschäftigt. Der Grund, warum dem nPA eine Chipkarte eingebettet wurde, liegt neben der Speicherung der Daten darin die Fälschungssicherheit zu erhöhen und neue Funktionalitäten zu unterstützen. Dies wird noch näher in den folgenden Kapiteln erläutert. Am Ende der Arbeit wird sich mit der Fragestellung auseinandergesetzt, inwiefern der nPA bei den Verbrauchern Anklang findet und ob durch die neue eIDAS-Verordnung der EU-Kommission die Nutzung des nPA vorangetrieben werden kann. Dazu wird eine Nutzerstudie durchgeführt.

2 Technologie und Sicherheit des Personalausweises

Der neue Personalausweis enthält zahlreiche Sicherheitsmerkmale, die bestmöglichen Schutz vor Fälschung und Missbrauch bieten; diese Merkmale machen den Ausweis zu einem der sichersten der Welt [1]. Durch den integrierten Chip im nPA kann der Ausweisinhaber sich via Online-Authentisierungsfunktion (engl. electronic identity, kurz eID) bei Anwendungen und Webseiten anmelden. Eine Auflistung der aktuellen Anwendungsmöglichkeiten findet sich auf dem Personalausweisportal [2]. Diese erhalten nach Zustimmung des Inhabers Zugriff auf personen- und dokumentenbezogene Daten. Nicht auf dem Chip abgelegt sind eigenhändige Unterschrift, Körpergröße und Augenfarbe [3]. Mithilfe der Qualifizierten elektronischen Signatur (QES) kann der Nutzer Verträge rechtskräftig unterschreiben. Durch die eIDAS-Verordnung [4] wird das ab 2018 europaweit der Fall sein.

Die Vorteile der eID Funktion liegen auf der Hand, es gibt einen vollkommen digitalen, öffnungszeitenunabhängigen und medienbruchfreien (nur bei QES) Vorgang, bei dem zusätzlich Wartezeiten entfallen und Papier und Porto gespart werden.

2.1 Lesegeräte für den nPA

Für das Auslesen des nPA ist neben Treibern und Software ein spezielles Lesegerät notwendig. Es gibt verschiedene Modelle, die dafür zu verwenden sind. Der Kunde hat die Möglichkeit sich auf dem freien Markt ein Gerät zu besorgen. Das einzige Kriterium, das an das Lesegerät gestellt wird, ist, dass es von Bundesamt für Sicherheit in der Informationstechnik (BSI) anhand der Technischen Richtlinie TR-03119 zertifiziert ist [5]. Solche Geräte sind auch am nPA Logo zu erkennen [6]. Die Lesegeräte gibt es in drei Ausführungen: Basisleser, Standardleser und Komfortleser. Der Basisleser unterstützt die Onlineausweisfunktion und stellt damit einen Sicherheitsgewinn dar. Der Standardleser besitzt zusätzlich eine eigene Tastatur und optional ein eigenes Display. Der Komfortleser hat grundsätzlich ein eigenes Display und alle Funktionen der beiden anderen Geräte. Er beinhaltet damit die Vollausstattung und unterstützt darüber hinaus noch die elektronische Unterschriftsfunktion (QES).

2.2 Sicherheitsziele

Neben einem schnellen Sperrvorgang durch ein persönliches Sperrkennwort nach einem Diebstahl des Ausweises ist es in erster Linie für den Ausweisinhaber wichtig, dass die Daten während des Auslesevorgangs nicht abgefangen oder verfälscht werden. Dies dient dem Sicherheitsziel der Authentizität und Integrität. Daher ist es erforderlich, die Kommunikation durch einen Mechanismus zu verschlüsseln. Des Weiteren muss auch die Kommunikation des Lesegerätes zum Server im Internet verschlüsselt ablaufen. Außerdem soll es dem Ausweisinhaber möglich sein auszuwählen, welche Daten an welches Unternehmen gesendet werden. Dies geschieht im Dialog mit dem Lesegerät (falls Display und Tastatur vorhanden) oder mit der Anwendersoftware.

Daneben gibt es verschiedene Ziele für den Datenschutz wie Aufenthaltsort des Inhabers, Wiedererkennen eines Nutzers (Tracking) auf die in dieser Arbeit nicht näher eingegangen wird.

2.3 Auslesevorgang

Das Protokoll [11] für den Auslesevorgang ist vom Bundesamt für Sicherheit in der Informationstechnik (BSI) entwickelt und in der Technischen Richtlinie TR-03127 festgehalten.

Für den Zugriff auf die Chip-Daten kommen folgende Anwendungsfälle infrage [11]:

1. eine auf dem Kartenkörper aufgedruckte sechsstellige Nummer (CAN – Card Access Number);
2. Hash über Dokumentennummer, Geburtsdatum und Ablaufdatum aus der maschinenlesbaren Zone (MRZ);
3. die eID-PIN: dies ist entweder eine dem Karteninhaber im PIN-Brief mitgeteilte fünfstellige eID-Transport-PIN oder eine nur dem Karteninhaber bekannte operationelle sechsstellige eID-PIN;
4. ein dem Karteninhaber im PIN-Brief mitgeteilter zehnstelliger PUK

In dieser Arbeit wird sich ausschließlich mit dem dritten Anwendungsfall beschäftigt, da dieser der Hauptanwendungsfall, insbesondere für die Ausweisinhaber selbst, ist.

Voraussetzung für den Lesevorgang am Computer ist die Installation der „AusweisApp“ des BSIs sowie der Treiber des Lesegerätes.

Die AusweisApp ist für Windows, Macintosh und Linux erhältlich. Das Lesegerät empfängt vom Diensteanbieter das Berechtigungszertifikat. Der Ausweisinhaber gibt nun seine persönliche Benutzer-PIN ein und erteilt hierdurch die Einwilligung zum Zugriff auf seine Ausweisdaten.

Der Vorgang wird im nachfolgenden Kapitel auf Protokollebene erläutert.

2.3.1 PACE

Nachdem der Chip im Personalausweis das die PIN überprüft hat startet das *Password Authenticated Connection Establishment* (PACE) Protokoll und erstellt einen verschlüsselten und integritätssicheren Kanal zwischen Terminal und Chip [11] (siehe Abbildung 1). Das PACE-Verfahren besteht im Kern aus einem Diffie-Hellman-Schlüsselaustausch-protokoll, wobei die ausgetauschten Schlüssel mittels (einfachen) Passwörtern (PINs) abgesichert werden; bei der PACE-Authentisierung generieren sowohl der Chip als auch das Lesegerät dynamisch flüchtige (ephemeral) DH-Schlüsselpaare, basierend auf den auf dem Chip abgelegten DH-Parametern, den sogenannten Domänen-Parametern [15].

Die Authentizität der öffentlichen DH-Schlüssel wird über den Nachweis der Kenntnis des gemeinsamen Geheimnisses, der 6-stelligen PIN, sichergestellt [15]. Beim nPA kommen zur Abwicklung des PACE-Protokolls die elliptischen Verfahren *Elliptic curve Diffie–Hellman* (ECDH) und *Elliptic Curve Digital Signature Algorithm*

(ECDSA) mit 224 Bit-Schlüsseln zum Einsatz [15].

Nachfolgend eine Vergröberung des Protokolls nach Eckert [15]:

1. Der Chip wählt eine Zufallszahl *s* und verschlüsselt diese mit einem aus der PIN π abgeleiteten Schlüssel $K\pi$: $C = E(s, K\pi)$.
2. Der Chip überträgt den Kryptotext *C* und seine DH-Parameter zum Lesegerät.
3. Das Lesegerät erhält die PIN π durch die Eingabe über den Benutzer.
4. Das Lesegerät leitet seinerseits den Schlüssel $K\pi$ aus der PIN ab und entschlüsselt den erhaltenen Kryptotext: $s = D(C, K\pi)$.
5. Chip und Lesegerät erzeugen jeweils flüchtige DH-Schlüsselpaare basierend auf den neu berechneten DH-Parametern. Dazu wenden sie jeweils eine Abbildungsfunktion an, die als Eingabe die ursprünglichen Domänen-Parameter des Chips sowie die verschlüsselt ausgetauschte Zufallszahl *s* verwendet.
6. Beide Partner tauschen ihre jeweiligen öffentlichen DH-Schlüssel aus.
7. Beide Partner berechnen den gemeinsamen, geheimen DH-Schlüssel *K* und leiten davon einen gemeinsamen Integritäts- K_{MAC} und Sitzungsschlüssel K_{Enc} ab.
8. Beide Partner erzeugen jeweils ein Authentisierungstoken. Dies ist ein MAC über den Integritätsschlüssel K_{MAC} und den öffentlichen DH Schlüssel des Partners.
9. Beide prüfen den MAC und verwenden danach die neuen Schlüssel für das nachfolgende Secure Messaging zwischen dem Chip und dem Lesegerät.

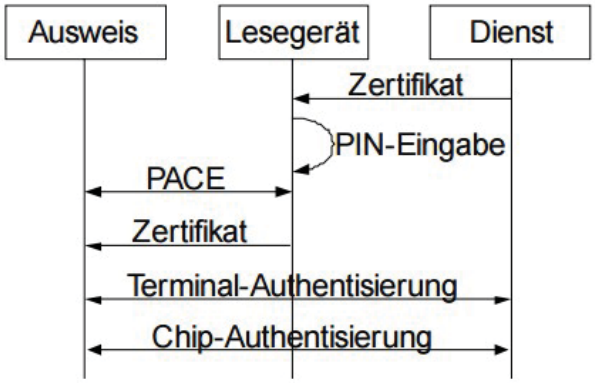

Abbildung 1 – Schema PACE-Protokoll [17]

Das PACE zählt, wie die nachfolgendene Terminal- und Chip-Authentisierung, zum *Extended-Access-Control* (EAC) Protokoll, welches speziell für den nPA entwickelt wurde. Nachdem über PACE gemeinsame Sitzungsschlüssel ausgehandelt wurden, überträgt das Lesegerät das Berechtigungszertifikat des Diensteanbieters zum Ausweis [15]. Nun folgt die Terminal-Authentisierung.

2.3.2 Terminal-Authentisierung

Die Terminal-Authentisierung (TA) dient der Autorisierung der Leserechte, sowohl für das Terminal selbst, als auch für den Dienstanbieter, welcher bei einer Online-Authentisierung die Daten benötigt [11]. Der Ausweisinhaber muss dieser Abfrage zustimmen. Somit behält er neben der Zugriffskontrolle auf seinen Ausweis, geschützt durch seine PIN, auch die Kontrolle über die Daten, die abgefragt werden. Durch das Challenge-Response-Protokoll weist der Diensteanbieter durch die Erstellung einer Signatur die Kenntnis seines privaten Schlüssels nach, der zu dem öffentlichen Schlüssel passen muss, der im Berechtigungszertifikat enthalten ist [15]. Der Chip prüft die Signatur, jedoch ist er nicht in der Lage Sperrlisten abzufragen, um zu prüfen, ob das Berechtigungszertifikat noch gültig ist; deshalb haben derartige Zertifikate nur eine sehr kurze Gültigkeit von max. 3 Tagen [15].

Bei der TA kommt für das EAC-Protokoll eine Public-Key-Infrastruktur (PKI) zum Einsatz. Die PKI besteht aus der Wurzelinstanz Country-Verifying-Certification-Authority (CVCA) und Document-Verifiers (DV) (siehe Abbildung 2). Diese DVs haben die Aufgabe die Schlüsselpaare der einzelnen Lesegeräte oder Dienstanbieter zu signieren.

Die Terminal-Authentisierung unterbindet das unbefugte Auslesen der Daten. Die Leserechte können detailliert via Zertifikat festgelegt werden. Zudem ist es möglich die Rechte vor dem Auslesevorgang weiter einzuschränken. Die Leserechte sind hierbei an die Sitzungsschlüssel gebunden, die im nachfolgenden Schritt ausgehandelt werden; dadurch ist sichergestellt, dass die Daten nur in einem stark gesicherten Ende-zu-Ende-Kanal zwischen Chip und Dienstanbieter übertragen werden, der nur durch den authentisierten Dienstanbieter aufgebaut werden kann [17].

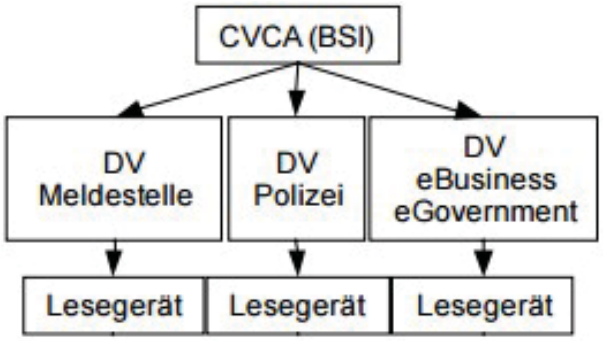

Abbildung 2 - EAC-PKI [17]

Um ein Erraten der eID-PIN durch Ausprobieren zu verhindern, enthält die Karte einen Fehlbedienungszähler (FBZ), der nach drei falschen PIN-Eingaben die eID-PIN sperrt; dadurch bestünde die Gefahr eines Denial of Service Angriffs (DoS) über die kontaktlose Schnittstelle auf die eID-PIN durch mehrmaliges Falscheingeben der eID-PIN ohne Kenntnis des Inhabers; um dies zu verhindern, wird der dritte Eingabeversuch erst nach erfolgreicher Eingabe der auf der Karte aufgedruckten CAN ermöglicht [11].

Nun folgt die Chip-Authentisierung.

2.3.3 Chip-Authentisierung

Die Chip-Authentisierung (CA) hat den Zweck einen sicheren Kanal zwischen Terminal bzw. Dienstanbieter und Chip aufzubauen. Sie prüft, ob der Chip in Besitz des privaten Schlüssels ist, der zum gespeicherten öffentlichen Schlüssel gehört und sorgt hierbei für Integrität und Authentizität [11].

Basierend auf den ausgetauschten DH-Werten berechnen Chip und Diensteanbieter ein gemeinsames MAC-Geheimnis sowie einen gemeinsamen, geheimen Sitzungsschlüssel *K* [15]. Der Dienste-anbieter kann anhand des vom Personalausweisaussteller (Bundesdrucker-ei) signierten, im Chip abgelegten, öffentlichen Schlüssels des Chips dessen Authentizität prüfen [15]. Der Chip verschlüsselt die zu übertragenen Daten mit dem Sitzungsschlüssel *K* und überträgt sie zum Diensteanbieter [15].

2.4 Angriffe auf den nPA

Bisher wurde gezeigt, dass der nPA bekannte und häufige Schwachstellen durch die Implementierung des PACE-Protokolls und der Zwei-Faktor-Authentifizierung vermeidet. Das BSI hat PACE entwickelt und patentieren lassen; es gilt bis heute (Februar 2017) als sicher. Es gibt jedoch weitere Angriffsmöglich-keiten auf die in diesem Abschnitt näher eingegangen wird.

2.4.1 PIN Phishing

Wie bei gängigen Passwort-Phishings ist es auch beim nPA möglich die PIN zu stehlen, z.B. durch ein gefälschtes Online-Plugin der AusweisApp oder der AusweisApp selbst. Durch eine optisch ähnliche Eingabemaske könnte der Nutzer seine PIN dem Angreifer unbeabsichtigterweise übermitteln.

Wird dieser Angriff mit einem Trojaner auf dem Rechner des Opfers kombiniert, könnte der Angreifer den Ausweis direkt online für seine Zwecke benutzen.

2.4.2 PIN Diebstahl

Die PIN kann auch durch Ablauschen eines Basislesegeräts gestohlen werden [19]. Hierbei wird über E-Mail ein Tool installiert, dass den Bildschirm zum Angreifer spiegelt und dadurch persönliche Daten, welche von Nutzer eingegeben werden, im Klartext einsehbar sind. Dieser Angriff ist nur möglich beim Basis-Lesegerät, da dieses nicht über eine integrierte Tastatur verfügt. Auch die optionale Bildschirmtastatur der AusweisApp ist keine Verbesserung, da das Tastenfeld nicht randomisiert ist. Von diesem Angriff sind Standard- und Komfortleser ausgeschlossen, da sie über eine eigene Tastatur verfügen.

Der Ausweis kann nur dann vom Angreifer verwendet werden, solange er auf dem Lesegerät liegt. Da die Adressdaten des Opfers nach dem Angriff bekannt sind sollte der Diebstahl des physischen Ausweises ebenfalls möglich sein.

2.4.3 Manipulierte AusweisApp

In der Vergangenheit ist es einem Angreifer gelungen, die Update-Funktion der AusweisApp (erhältlich für Windows, Linux, Mac) zu manipulieren [12]. Dies war möglich, da das Programm nicht prüfte ob das SSL-Zertifikat zum Servernamen passt. Daher bedurfte es keinem gültigen Zertifikat für den Updateserver, sondern es genügte ein gefälschtes SSL-Zertifikat. Der Updatefunktion kann auf diesem Weg eine manipulierte Antwort untergeschoben werden, um etwa einen Trojaner von einer beliebigen URL herunterzuladen und zu installieren.

2.4.4 Skimming

Beim Skimming besteht das Risiko der Nutzung eines infizierten oder gar falschen Lesegerätes. Die AusweisApp auf dem Nutzer-Computer prüft die Zertifizierung der Lesegeräte. Da die Bezeichnung des Lesers vom Betriebssystem stammt, sollte es nicht zu schwierig sein sie zu fälschen [20]. Wie auch bei Bankautomaten können die öffentlichen Lesegeräte z.B. in Behörden etwa durch zusätzliche Hardware gefälscht werden.

2.5 Zusammenfassung und Bewertung der Ergebnisse

Mit der Anwendung des PACE-Protokolls ist eine sichere Möglichkeit gegeben die Daten des nPAs vor unbefugtem Auslesen zu schützen. Der Beweis ist von Bender et al. bestätigt [14]. Viele bekannte Schwachstellen sind bei der Entwicklung von PACE bereits eliminiert vermieden worden z.B. in dem es einen verschlüsselten, integritätssicheren Kanal zwischen Karte und Lesegerät aufbaut. Es ist praktisch sehr unwahrscheinlich, dass durch Brute-Force die Benutzer-Pin gebrochen wird, da nur drei Versuche zur Verfügung stehen. Die Benutzer-PIN besteht im Vergleich zu Bankkarten aus sechs Ziffern anstatt nur vier.

Gängige Social-Engineering-Angriffe, wie Erraten des Passworts, Phishing aber auch Skimming Angriffe, sind möglich. Im Vergleich zu RFID Kreditkarten, welche über Funk nachweislich über größere Distanzen als angegeben im Klartext ihre Daten senden, findet die Kommunikation zwischen nPA und Terminal verschlüsselt statt. Zusätzlich ist eine beidseitige Authentifizierung integriert und der Diensteanbieter muss eine Berechtigung zum Auslesen der Daten vorweisen. Die auszulesenden Daten gibt der Ausweisinhaber im nächsten Schritt manuell frei.

Die Kritik an dem nPA ist somit verglichen mit anderen Funkkarten auf hohem Niveau. Vielfach wird auch der Datenschutz respektiert und für Anfragen, in denen kein Name erforderlich ist, nur ein Pseudonym gesendet. Ähnlich verhält es sich bei Altersabfragen, wobei nur ein Ü18 Signal gesendet wird und nicht das Alter selbst.

Einige der aufgezeigten Hackangriffe wies das BSI zurück, da es für unwahrscheinlich empfunden wird, dass ein Trojaner auf dem PC des Opfers ist [7]. Sie beziehen sich darauf, dass die Endanwender verpflichtet

sind ihre PCs zu schützen. Hier geben sie Vorgaben, wie den Einsatz einer Firewall, Virenscanners und die Einspielung regelmäßiger Software-Updates. Der Ausweis soll nach der Verwendung sofort vom Lesegerät entfernt werden. Da ein Trojaner permanent auf dem infizierten Rechner aktiv ist, spielt es keine Rolle wann der Ausweis auf das Lesegerät gelegt wird. Die Argumentation des BSI ist somit sehr schwach und es schiebt die Verantwortung auf den Bürger ab.

Für den nPA gibt es ein Sperrkennwort, mit welchem die Benutzer den Ausweis sofort selbst sperren können.

2.5.1 Handlungsempfehlungen

Neben den vom BSI empfohlenen Handlungen, wie Einsatz von Firewall, Virenscanner und Einspielung regelmäßiger Software-Updates sowie das sofortige Entfernen des Ausweises von Lesegerät nach Gebrauch, sollte auf jedenfall nur der Komfortleser verwendet werden, da dieser viele Angriffe durch die integrierte Tastatur vermeiden kann. Beim Kauf eines Lesers sollte darauf geachtet werden, das Lesegerät nur vom Hersteller direkt zu kaufen um Fälschungen zu vermeiden. Auch sollte die AusweisApp nur von Herausgeber selbst heruntergeladen werden. Öffentliche Terminals sollten aufgrund von Skimming-Attacken vermieden werden.

3 Nutzerstudie

Weil diese Arbeit eine Vorarbeit für die Master-Thesis ist, wird anhand einer Nutzerstudie evaluiert, wie es um die Nutzung des Personalausweises zukünftig steht. In der darauffolgenden Thesis werden verschiedene Möglichkeiten zur Identifizierung und zum Vertragsabschluss im Internet geprüft, wobei auch der nPA im Mittelpunkt stehen wird. Daher kam die Frage auf, inwiefern die eIDAS-Verordnung dabei helfen kann.

Wie in Kapitel 2 erwähnt, bietet eIDAS die Möglichkeit rechtssichere Verträge mithilfe der QES europaweit abzuschließen, da sie einen einheitlichen rechtlichen und organisatorischen Rahmen bietet [13].

Im Jahr 2010 begrüßten 52% der teilnehmenden Internet-Nutzer die Einführung des neuen Personalausweises [16].

Bei einer Umfrage zur geplanten Nutzung der Funktionen des nPA antworteten 52,2%, dass sie den Ausweis als Internetausweis und 45% für die elektronische Signatur möchten benutzen [10].

Fünf Jahre später (2015) hat das Marktforschungsunternehmens GFK festgestellt, dass nur ca. 30% die Onlinefunktion des nPA aktivieren ließen und nur ca. 5% die Onlinefunktion tatsächlich nutzen [9].

Vermutlich ist auch der Preis für ein teures Endgerät, wie den Komfortleser mit ca. 160€ (Stand Februar 2017), ein starkes Problem, wurden anfangs sogar Basis-Lesegeräte von den Bundesländern verschenkt, um die Nutzung voranzutreiben.

In einer Bitkom-Studie wurde 14+-jährigen Internet-Nutzern folgende Frage gestellt: „Wie viel Geld wären Sie bereit, für ein Personalausweis-Kartenlesegerät auszugeben, damit Sie Internet-Dienste nutzen können?“. Darauf antworteten 30%, mit „gratis“, 57%, „weniger als 50 Euro“ und gerade mal 5% mit „mehr als 50 Euro“ [18]. Allgemein gesehen betrachtet beginnt die Zahlungsbereitschaft für ein Lesegerät, bei Personen die älter als 30 Jahre sind.

3.1 Hypothesen

Die Nutzerzahlen zeigen ein ernüchterndes Ergebnis und es stellt sich die Frage, weshalb die Nutzer den Personalausweis so selten nutzen und wie die Nutzerzahlen verbessert werden können. Interessant ist auch, ob die neue eIDAS-Verordnung hilft, die Online-Funktion des Personalausweises bei den Bürgern beliebter zu machen. Dies führt zu folgenden Hypothesen.

3.1.1 Hypothese 1

„Wären die aktuellen Funktionen des elektronischen Personalausweises den Nutzern bekannt, würden Sie den Ausweis häufiger online verwenden."

3.1.2 Hypothese 2

„Durch die eIDAS-Gesetzesänderung wird der neue elektronische Personalausweis zukünftig häufiger online verwendet"

3.1.3 Hypothese 3

„Der sichere Komfortleser ist zu teuer, da die Nutzer wenig oder gar kein Geld für ein Lesegerät ausgeben möchten."

3.1.4 Hypothese 4

„Durch vielfach erweiterbare Anwendungsmöglichkeiten würden mehr Nutzer den Komfortleser verwenden."

3.2 Durchführung

Als Zielgruppe wird, wie bei vergleichbaren Studien, eine Stichprobe aus der Bevölkerung Deutschlands genommen. Größere Studien benutzen den Mikrozensus (Stichprobe mit ca. 1% der Bevölkerung), welchem die Daten des Statistischen Bundesamts zugrunde liegen. Die Stichprobe dieser Arbeit umfasst 60 Personen, aus unterschiedlichen Altersklassen und mit verschiedenem technischem Hintergrundwissen. Für 60 Teilnehmer entspricht die Verteilung der Bevölkerung, gemessen im Jahr 2015 [8], zwischen 14-29 Jahren 12,6 Personen (21,31%), 30-49 Jahren 20,4 Personen (34,06%), 50-64 Jahren 12,6 Personen (21,31%) und 65+ Jahren 13,8 Personen (23,31%). Natürlich kann diese Nutzerstudie nicht repräsentativ für alle Bundesbürger gelten aufgrund der begrenzten Teilnehmerzahl. Die Fragen der Nutzerstudie waren in vier Bereiche eingeteilt: allgemein, nPA, eIDAS + Kosten, Sicherheit und Mehrwert. Die Einteilung ist wichtig für den Umfrageverlauf da zum Einstieg einfache Fragen und zum Schluss sicherheitskritische Fragen gestellt wurden. Die Nutzerstudie hat sowohl in persönlichen Interviews als auch in einer Online-Befragung stattgefunden.

3.3 Ergebnis und Diskussion

70% der Befragten besitzen den neuen Personalausweis wovon 20% die Online-Funktion aktivieren ließen. Die Hauptgründe hierfür waren Neugierde, Kostenvermeidung durch nachträgliches Aktivieren und die Annahme, dass die Funktionen oft zu verwenden seien. Dies deckt sich nicht mit dem generellen Interesse der Bevölkerung gemessen im Einführungsjahr 2010 in der Befragung von Statista. 80% haben sich dagegen entschieden, da sie entweder kein Interesse hatten (30%), Sicherheitsbedenken äußerten (55%) oder die Funktionen nicht kannten (77%). Daher muss über die Funktionen deutlich besser aufgeklärt werden sofern die Nutzung der eID Funktionen vorangetrieben werden möchten. Jedoch konnten eine Aufklärung und ein konkretes Nachfragen in dieser Nutzerstudie kein gesteigertes Interesse aufzeigen. Daher konnte die erste Hypothese nicht eindeutig belegt werden.

Die Möglichkeit der Nutzung innerhalb der gesamten EU hat nur einen geringen Einfluss auf das zukünftige Verhalten. 29% würden dadurch die Online-Funktion häufiger nutzen und 77% entschieden sich dagegen. Daher konnte die zweite Hypothese ebenfalls nicht eindeutig belegt werden.

97% würden den Kauf des Komfortlesers ablehnen auch wenn sie durch eIDAS europaweit Verträge abschließen könnten. Hypothese drei wurde dadurch bestätigt und bekräftigt damit die Ergebnisse der Bitkom-Umfrage von 2010 zur Zahlungsbereitschaft der Kartenlesegeräte. Insbesondere junge Menschen, welche sich vorwiegend mit den neuen Technologien auseinandersetzen, möchten keinen oder nur einen geringen zusätzlichen Geldbetrag für ein Lesegerät aufbringen. Auch der Sicherheitsvorteil gegenüber günstigen Lesegeräten spielt hier keine Rolle.

Die vielfach erweiterbaren Nutzungsmöglichkeiten wie Datenabfrage der elektronischen Gesundheitskarte (Krankenkasse), Nutzung beim Online-Banking, Aufladung der Geldkarte und Personalausweis als Personennahverkehr-Ticket würden 67% der Teilnehmer nicht dazu überzeugen einen Komfortleser zu kaufen. Damit konnte Hypothese vier nicht bestätigt werden.

Allgemein ist festzuhalten, dass die Teilnehmer den Kosten-Nutzen-Faktor des teureren Komfortlesers schlecht einschätzen, insbesondere wenn im privaten Bereich die Online-Funktion sehr selten genutzt werden. Einige Teilnehmer schrieben, dass sie die zusätzliche Hardware wie das Lesegerät als unkomfortabel empfinden. Sie favorisieren eher eine Möglichkeit ohne zusätzliche Hardware.

Wenn die Nutzung des nPA vorangetrieben werden soll, müssen jedenfalls die Lesegeräte billiger werden, aber besser noch durch eine andere Technologie ersetzt werden, welche keine Lesegeräte voraussetzt, da die Nutzer die Verwendung zu unkomfortabel finden. Die eIDAS-Verordnung schafft hierbei die Voraussetzung in dem es die gesetzliche Grundlage dafür bietet. Zusätzlich könnten die Bürger mit Bonussen oder Rabatten gelockt werden falls die Verträge digital abgeschlossen würden.

Mitunter haben Hackangriffe auch eine gewisse Furcht oder Ablehnung bei den Bürgern verursacht. So wurde in einigen Ämtern der BRD den Nutzern empfohlen die Ausweisfunktion nicht freizuschalten nach Bekanntwerden diverser Gefahren für den Nutzer durch die einfachen Lesegeräte und einer Sicherheitslücke in der AusweisApp. Dies veranlasste die BSI dazu die AusweisApp für einige Zeit zur Verbesserung vom Download-Portal zu entfernen.

Dazu kommt das Problem, dass das Interesse der Wirtschaft gering bleibt, solange sich die Nutzerzahlen gering halten. Daher kommt die Entwicklung von Anwendungen für den nPA erst allmählich in die Gänge.

Den Mehrwert, den sich die Nutzer vom nPA wünschen sind: Integration anderer Ausweise wie Führerschein, Schwerbeschädigtenausweis, Zug- oder Busticket, Reisepass, Kreditkartenfunktion, Punkte in Flensburg abfragen, vereinfachte Altersverifizierung E-Mail Signaturen abseits von der DE-Mail, Gesundheitskarte, Bankkarte, Kreditkarte, Büchereiausweis, Jahreskarten für Freizeitaktivitäten.

Der Konsens lautet, dass solange nicht deutlich mehr elektronische Medien in einem Identifikationsmedium zusammengeführt werden, sind Teillösungen relativ unbedeutend. Hierbei ist Estland ein Vorreiter, welche als erste die eID-Funktion mit vielen weiteren Funktionen wie Online-Banking kombinierte und bereits seit 2005 Wahlen über das Internet ermöglicht.

Andere Nutzer möchten den nPA nur als Sichtausweis nutzen und wünschen daher eine Kostenreduzierung.

4 Literaturverzeichnis

[1] Sicherheitsmerkmale elektronsicher Personalausweis. Bundesdruckerei GmbH in Kooperation mit Bundesministerium des Innern, Berlin, 2014.

[2] Hier können Sie die Online-Ausweisfunktion nutzen. Webseite, 2017. https://www.personalausweisportal.de/DE/Buergerinnen- und-Buerger/Anwendungen/Anwendungen_node.html; abgerufen am 13.3.2017.

[3] Daten im Chip. Webseite, 2017. https://www.personalausweisportal.de/DE/Buergerinnen-und-Buerger/Sicherheit-und-Datenschutz/Sicherheit-und-Datenschutz-node.html; Besucht am 8.3.2017.

[4] eIDAS-Verordnung Nr. 910/2014 des europäischen Parlaments und des EU-Rates. EU-Kommission. http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32014R0910; abgerufen am 13.3.2017.

[5] Bundesministerium des Innern - Chipkarten-Lesegeräte. Website, 2017. Online verfügbar unter https://www.personalausweisportal.de/DE/Buergerinnen-und-Buerger/Online-Ausweisen/das-brauchen-Sie/Kartenlesegeraete/Kartenlesegeraete_node.html; Besucht am 28.2.2017.

[6] Bundesministerium des Innern – Daten auf dem Ausweis. Webseite, 2017. https://www.personalausweisportal.de/DE/Buergerinnen-und-Buerger/Der-Personalausweis/Details/DatenAusweis/datenAusweis_node.html; Besucht am 28.2.2017.

[7] Bundesministerium des Innern – Sicherheitsbedenken Personalausweis. Webseite, 2010. https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2010/Sicherheitsbedenken_ Personalausweis_240810.html; abgerufen am 13.3.2017.

[8] Statista. Bevölkerung - Verteilung der Einwohner in Deutschland. Studie, 2015.

[9] K. Hilbinger, Frage des Monats Mai – Elektronischer Personalausweis - GFK Studie im Auftrag der WeltN24 GmbH, Nürnberg, 2015.

[10] Geplante Nutzung von Funktionen des neuen Personalausweises in Deutschland 2010; Webseite, 2010 https://de.statista.com/statistik/daten/studie/167117/umfrage/geplante-nutzung-von-funktionen-des-neuen-personalausweises/; Besucht am 28.2.2017.

[11] Bundesamt für Sicherheit in der Informationstechnik. Technische Richtlinie TR-03127 - eID-Karten mit eID- und eSign-Anwendung basierend auf Extended Access Control - Elektronischer Personalausweis und elektronischer Aufenthaltstitel. Bonn, Version 1.16, 2015.

[12] J. Schejbal. AusweisApp gehackt (Malware über Autoupdate). Webseite, 2010. https://janschejbal.wordpress.com/2010/11/09/ausweisapp-gehackt-malware-uber-autoupdate/; abgerufen am 13.3.2017.

[13] eIDAS-Verordnung über elektronische Identifizierung und Vertrauensdienste ,Bundesamt für Sicherheit in der Informationstechnik, Webseite, 2017. https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/eIDAS/eIDAS_node.html, abgerufen am 12.3.2017.

[14] J. Bender, M. Fischlin, D. Kügler. Security analysis of the pace key - agreement protocol. Bundesamt für Sicherheit in der Informationstechnik, Darmstadt, 2009.

[15] C. Eckert. IT-Sicherheit - Konzepte – Verfahren – Protokolle, Oldenbourg Wissenschaftsverlag GmbH, München, 2014.

[16] Statista. Begrüßen Sie die Einführung des neuen elektronischen Personalausweises?, Studie, 2010.

[17] J. Bender, D. Kügler, M. Margraf, I. Naumann. Sicherheitsmechanismen für kontaktlose Chips im deutschen elektronischen Personalausweis. Datenschutz und Datensicherheit, Gabler Verlag, Wiesbaden, Ausgabe 03.2008.

[18] Bitkom. Zahlungsbereitschaft für Kartenlesegeräte. Studie, 2010.

[19] N. Kohnert und R. Stumpf. CCC Plusminus. WDR, Fernsehmagazin, Sendezeit: 24. August 2010 21:50–22:15. 2010.

[20] D. Oepen, F. Morgner. Die gesamte Technik ist sicher - Besitz und Wissen: Relay-Angriffe auf den neuen Personalausweis, Humboldt-Universität, Berlin, 2010.