Heinrich C. Mayr, Martin Pinzger (Hrsg.): INFORMATIK 2016,
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2016 519

Usability-Untersuchung eines Papierprototypen für eine mobile Online-Ausweisfunktion des Personalausweises

Sandra Kostic[1] Andreas Heinemann[2] Marian Margraf[3]

Abstract: Die Online-Ausweisfunktion des Personalausweises in Deutschland besitzt eine Reihe von Usability-Schwierigkeiten und somit eine geringe Akzeptanz bei den Bürgerinnen und Bürgern. Die Umsetzung des Personalausweises in Form einer App auf einem Smartphone könnte hier Abhilfe schaffen. Mithilfe eines Papierprototypen wurden erste Usabilty-Untersuchungen durchgeführt, die zeigen, dass zwar die Benutzbarkeit der App gegeben ist, das Vertrauen in die Sicherheitsfunktionen der App jedoch nicht.

Keywords: Personalausweis, Mobile Online-Ausweisfunktion, Usabilty, Smartphone

1 Einleitung

Reisepässe und Personalausweise werden nicht nur im hoheitlichen Bereich, z.B. im Rahmen einer Grenz- oder polizeilichen Kontrolle zur Identifikation des Ausweisinhabers eingesetzt, sondern regelmäßig auch im privatwirtschaftlichen Umfeld. Die Einsatzmöglichkeiten erstrecken sich hier von stark regulierten Bereichen in denen eine gesetzlich vorgeschriebene Identifikationspflicht besteht, wie z.B. dem Banken- und Versicherungswesen, über kommerzielle und behördliche Anwendungen, z.B. Bürgerdienste, bis hin zu Geschäften zwischen Privatpersonen, z.B. beim Kauf eines Gebrauchtwagens. Mit der in den seit 1.11.2010 ausgegebenen deutschen Personalausweisen enthaltenen Online-Ausweisfunktion kann die Authentifizierung des Ausweisinhabers nunmehr auch Online erfolgen.

So ist es schon heute möglich, ein Konto bei der Bank für Investments und Wertpapiere AG oder der Deutschen Kreditbank AG mit Hilfe der Online-Ausweisfunktion zu eröffnen. Zahlreiche Bundes-, Landes- und Kommunalbehörden bieten darüber hinaus ihre Bürgerdienste (Beantragung von Geburtsurkunden, Feinstaubplaketten, Führungszeugnis etc.) ebenfalls über diese Funktion an, siehe [BMI15] für eine Übersicht.

Die heute zur Verfügung gestellte Infrastruktur für die Online-Ausweisfunktion adressiert vornehmlich eine Nutzung mittels PC. So steht die von der Bundesregierung bereitgestellte notwendige Software nur für die Betriebssysteme Mac OS X und Windows zur Verfügung ([Gov15]), Open-Source-Projekte bieten Lösungen für Linux-Varianten an. Ein weiteres Problem für die Nutzung der Online-Ausweisfunktion mit mobilen Endgeräten ist die Notwendigkeit eines Kartenlesers, mit dem die kontaktlose Schnittstelle des Personalauswei-

[1] Freie Universität Berlin, Takustr. 9, 14195 Berlin, sandra.kostic@fu-berlin.de
[2] Hochschule Darmstadt, Haardtring 100, 64295 Darmstadt, andreas.heinemann@h-da.de
[3] Freie Universität Berlin, Takustr. 9,14195 Berlin, marian.margraf@fu-berlin.de

ses kommuniziert. Zwar stehen Lesegeräte, die z.B. über Bluetooth mit Smartphones oder Tablets verbunden werden können, zur Verfügung ([BMI15]), allerdings ist aus Sicht der Nutzerinnen und Nutzer die Verwendung von Kartenlesern für Smartphone- und Tablet-Anwendungen noch unüblicher als mit PCs.

Ziel der vorliegenden Arbeit ist es zu evaluieren, ob ein auf einem Smartphone oder Tablet virtualisierter Ausweis (d.h. die Umsetzung der Online-Ausweisfunktion über eine App) für nicht-hoheitliche Anwendungen von Nutzerinnen und Nutzern akzeptiert wird. Zwar zeigen die Nutzungszahlen von z.B. Apple Pay (siehe [BoA16]), dass virtualisierte Sicherheitschips (hier Kredit- und Debitkarten) grundsätzlich angenommen werden. Die Frage, ob ähnliche Umsetzungen auch für von staatlichen Stellen verantwortete Lösungen ähnliche Akzeptanzraten zeigen, wird dadurch aber nicht beantwortet (siehe auch die Diskussion in Abschnitt 6).

Für die Untersuchung der vorliegenden Fragestellung wurde ein Prototyp entworfen (siehe Abschnitt 3) und einer Usability-Untersuchung unterzogen (Abschnitt 4). Eine sicherheitstechnische Evaluierung solch einer Umsetzung ist nicht Gegenstand dieser Arbeit. Eine mögliche Lösung wurde bereits in [Ot16] hinsichtlich einer sicheren Umsetzung untersucht.

Im Ergebnis (Abschnitt 5) wurde die App hinsichtlich ihrer Benutzbarkeit überwiegend positiv bewertet, es verbleiben aber Probleme, wie z.B. der aus Sicht der Nutzerinnen und Nutzer nicht bestehende Bedarf für die Nutzung und gefühlte Sicherheitsbedenken (siehe die Diskussion in Abschnitt 6).

2 Verwandte Arbeiten

Die Online-Ausweisfunktion des Personalausweises wird von Bürgerinnen und Bürgern nur sehr zögerlich eingesetzt [ID15]. So aktivieren lediglich ca. 30% der Besitzer des Personalausweises die Online-Ausweisfunktion. Die Gründe hierfür liegen nicht in sicherheits- oder datenschutzrechtlichen Problemen. Zahlreiche Untersuchungen haben gezeigt, dass die im Personalausweis zum Einsatz kommenden Verfahren sicher sind, vgl. [Be10a,Be10b, Be12]. Vielmehr zeigen Studien zur Online-Ausweisfunktion des deutschen Personalausweises, dass eine wesentliche Hürde zur Nutzung der Online-Ausweisfunktion die mangelhafte Verbreitung geeigneter Kartenleser in Haushalten ist, vgl. [As12]. Eine entwicklungsbegleitende Usability-Untersuchung der im Jahr 2014 veröffentlichten neuen Version der Software zur Nutzung der Online-Ausweisfunktion (AusweisApp2, [Gov15]) kam darüber hinaus zu dem Ergebnis, dass sich schwerwiegende Usability-Probleme aus der Gesamtinfrastruktur ergeben, die nicht allein durch die Anwendungssoftware gelöst werden können, [Wi16], siehe auch [As12]. So zeigt sich z.B., dass gerade die Verwendung von Kartenlesern zu einer sehr hohen Abbrecherquote bei bestimmten Nutzergruppen führt.

Ein weiteres Usability-Problem, das in [Wi16] aufgeführt wird, ergibt sich aus dem PIN-Management. Der Ausweis wird mit einer fünfstelligen Transport-PIN ausgeliefert. Vor der ersten Nutzung der Online-Ausweisfunktion muss diese in eine sechsstellige PIN um-

gewandelt werden. Da der Personalausweis keine Funktion vorsieht zu erfragen, ob die sechsstellige PIN bereits gesetzt wurde, kann die Software keine geeignete Nutzerführung umsetzen.

Die oben aufgeführten Usability-Probleme werden auch nicht über die Vorteile bei der Nutzung der Online-Ausweisfunktion kompensiert. Eine Vielzahl von Nutzerinnen und Nutzern sehen keinen Bedarf für diese Funktion, da ihnen geeignete Anwendungen nicht bekannt sind, vgl. [ZE16].

Eine wesentliche Voraussetzung für die Nutzung von Sicherheitsfunktionen ist die Benutzbarkeit, siehe z.B. [Wh99]. Benutzbarkeit kann aber nicht allein dadurch erreicht werden, dass Sicherheitsmechanismen ohne Nutzerinteraktion umgesetzt werden, da sonst das Vertrauen in die Sicherheitsfunktionen beim Nutzer nicht vorhanden ist, vgl. [Ru13].

3 Prototyp

Für die Untersuchung wurde ein Papierprototyp entwickelt, welcher jede einzelne Interaktion zwischen Benutzer und Software aufzeigt. Bei der Entwicklung des Prototypen wurden die Ergebnisse der in Abschnitt 2 erwähnten Studie [Wi16] berücksichtigt. Insbesondere konnten die dort aufgeführten Usability-Probleme durch das Konzept, die Online-Ausweisfunktion über eine App auf mobilen Endgeräten zu emulieren, gelöst werden (Wegfall eines Kartenlesers, bessere Umsetzung des PIN-Managements).

Um das Vertrauen in die Lösung zu erhöhen, müssen Nutzer bewusst Sicherheitsfunktionen anstoßen (Eingabe einer PIN), sind also Teil des Sicherheitsprozesses (siehe Abschnitt 2.

Die Teilnehmer des Tests haben positiv auf den Papierprototypen reagiert. Durch die Möglichkeit, direkt in den einzelnen Seiten des Prototypen Anmerkungen und Verbesserungen zu notieren, haben sich die Teilnehmer als Teil des Prozesses empfunden, ein noch konzeptionelles Produkt zu verbessern. Darüber hinaus zeigen z.B. [Sn03] und [Ri13], dass viele Nutzerinnen und Nutzer bei Einsatz von professionell wirkenden Prototypen (z.B. Prototypen, die mittels Mock-up-Tools entwickelt wurden), eine große Hemmschwelle haben, Kritik zu äußern, da gerade für technisch nicht versierte Nutzerinnen und Nutzer diese Lösungen bereits vollständig aussehen.

Gleichwohl haben die Teilnehmer den Prototypen als eine komplexe, funktionierende App wahrgenommen. In Situationen in denen der Papierprototyp eine Tätigkeit von ihnen erwartete, haben sie intuitiv richtig interagiert. Die Teilnehmer hielten zum Beispiel den Prototypen wie ein funktionierendes mobiles Gerät, um ein Foto zu machen oder verwendeten den Ziffernblock, um die für die Online-Ausweisfunktion notwendige PIN einzugeben.

So bietet er zum Beispiel ein Navigationsmenü (siehe Abb. 1) oder auch Untermenüs (siehe Abb. 2), um hier in einer Funktion *Verlauf* die ausgegeben Liste zu sortieren. Beispielhafte Anmerkungen der Testpersonen waren zu ergänzende Bedienelemente (siehe Abb. 3) oder erweiterte Funktionalitäten (siehe Abb. 4)

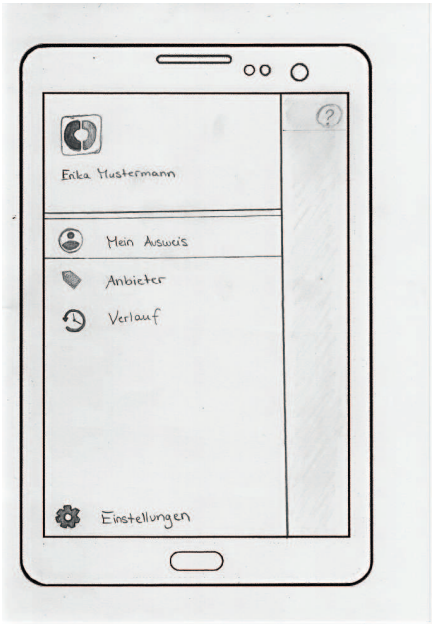

Abb. 1: Hauptmenü

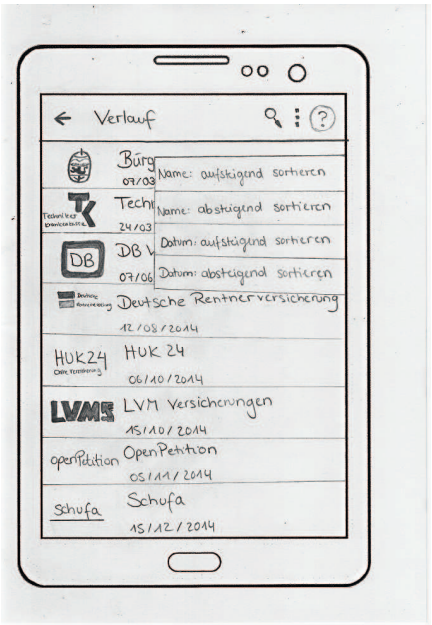

Abb. 2: Untermenü innerhalb der Funktion *Verlauf*

Die hier vorgestellten Oberflächen des entwickelten Prototypen sind ausgewählte Beispiele.[4]

4 Durchführung der Usability-Studie

An der Usability-Untersuchung haben insgesamt fünf Testpersonen teilgenommen. Nach [Ri13] ist diese Anzahl ausreichend, um im Rahmen von Usability-Tests schwerwiegende Usability-Probleme einer zu untersuchenden Lösung zu erkennen.

Voraussetzung für die Auswahl der Testpersonen war, dass sie ein Smartphone besitzen und dieses nicht nur für Telefonate nutzen, sondern mit der Nutzung von Apps auf Smartphones vertraut sind (siehe Zeile vier in Tabelle 1). Weiter wurden Testpersonen aus unterschiedlichen Altersgruppen, Geschlechtern, verschiedenem technischen Vorwissen (allgemein und Kenntnisse über die Online-Ausweisfunktion) ausgewählt. Die Online-Ausweisfunktion selbst hatte keine der Testpersonen zuvor benutzt. Die Informationen wurden im Rahmen von Interviews erhoben. Tabelle 1 fasst die Angaben zu den ausgewählten Testpersonen zusammen.

Der Usability-Untersuchung gliederte sich in zwei Teile:

[4] Der vollständige Prototyp ist unter `https://ucs.fbi.h-da.de/wordpress/wp-content/uploads/2016/05/AusweisApp-Prototyp.pdf` einsehbar.

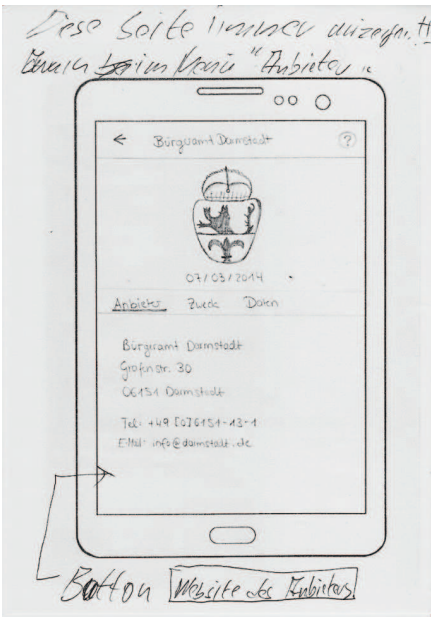

Abb. 3: Anmerkung eines Teilnehmers zur Ergänzung zum Reiter *Anbieter*

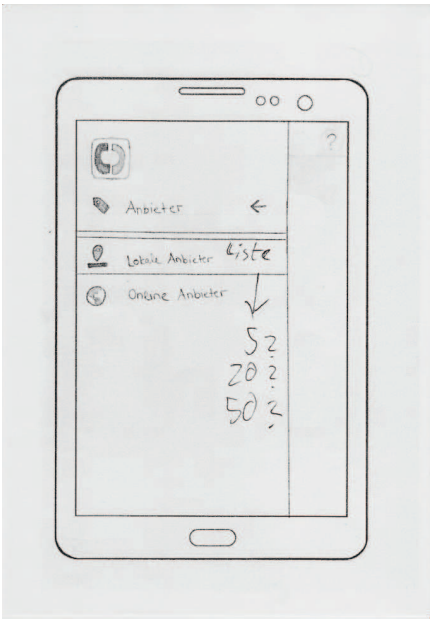

Abb. 4: Anmerkung eines Teilnehmers für die Karte der lokalen Anbieter

Geschlecht	P2, P3, P4 männlich, P1, P5 weiblich
Alter	P1: 33J., P2: 55J., P3: 56J., P4: 47J., P5: 45J., ∅ 47 Jahre
technisches Wissen	stark: P2, P3, mittel: P4, gering: P1, P5
Nutzung von Smartphone-Apps	häufig: P1, P3, P4, mittel: P2, P5, gering: 0
Wissen über Online-Ausweisfunktion	stark: 0, mittel: P3, gering: P4, P5, kein: P1, P2
Nutzung der Online-Ausweisfunktion	keiner der Teilnehmer

Tab. 1: Zusammenfassung der Angaben zu den Testpersonen

- *Der erste Teil* bestand aus der Durchführung von Thinking Aloud Tests an Hand des vorliegenden Papierprototypen. Dabei wurde die Installation der App auf einem Smartphone, die Hauptfunktion der App über einen beispielhaften Authentisierungsvorgang und die Deinstallation vorgestellt. Durch Nachfragen wurden die Testpersonen zusätzlich dazu angeregt, Verbesserungsvorschläge zu unterbreiten, aber auch Sicherheitsbedenken zu äußern. Anmerkungen und Verbesserungsvorschläge zum Prototypen wurden vom Teilnehmer selbst auf dem Prototypen notiert oder skizziert und in einem parallel geführten Protokoll festgehalten.
- *Der zweite Teil* bestand aus der Beantwortung eines Fragebogens basierend auf der ISO-Norm 9241/110 (Grundsätze der Dialoggestaltung), [Pr09]. Auch wenn die meisten Fragen schon im Rahmen des zweiten Teils erhoben wurden, diente der Fragebogen dazu, die Ergebnisse der Usability-Untersuchung standardisiert zu präsentieren (siehe Abbildung 5).

5 Ergebnisse

Im Folgenden werden die Ergebnisse der beiden durchgeführten Usability-Tests vorgestellt. Eine Diskussion der Ergebnisse findet sich in Abschnitt 6.

5.1 Ergebnisse der Thinking Aloud Tests

Die Usability wurde durchweg positiv bewertet, siehe auch Abschnitt 5.2. Die Testteilnehmer haben insgesamt 54 Verbesserungsvorschläge unterbreitet. Diese betreffen insb. sicherheitsrelevante Fragestellungen (34 von 54). So wurde z.B. gefordert, dass die PIN nicht nur beim eigentlichen Authentisierungsvorgang eingegeben werden soll, sondern schon beim Öffnen der App (P2, P4). P2 sagte dazu:

> „In der App ist mein Ausweis enthalten und damit meine Daten. Ohne die PIN hier eingeben zu müssen können ja Angreifer meine Daten sehen. “

Bemerkenswert ist die Tatsache, dass zwei der fünf Teilnehmer immer wieder von der eigentlichen Usability-Untersuchung abwichen und sicherheitsrelevante Fragen stellten (P2, P3).

Beispielhaft sei hier die Anmerkung von P4 wiedergegeben:

> „Wenn aus Gründen der Bequemlichkeit bei der App darauf verzichtet wird, die Deinstallation vom Smartphone komplexer als üblich zu gestalten, besteht das Risiko, dass eines meiner Kinder diese App einfach so in den Papierkorb verschiebt! Was mache ich dann? Denn dann sind ja alle meine Daten weg.“

Oder die Anmerkung von P2:

> „Der Benutzer-PIN genügt doch nicht als Sicherheitskriterium, genauso wie biometrische Daten. Das Medium Internet ist nicht dafür gedacht die Realität und Personen zu ersetzten.“

5.2 Auswertung des Fragebogens

Der im zweiten Teil genutzte Fragebogen basierend auf der ISO-Norm 9241/110 (Grundsätze der Dialoggestaltung) ist in sieben Kategorien unterteilt:

- Aufgabenangemessenheit
- Selbstbeschreibungsfähigkeit
- Erwartungskonformität

- Lernförderlichkeit
- Steuerbarkeit
- Fehlertoleranz
- Individualisierbarkeit

Die Kategorien Fehlertoleranz kann mittels eines Papierprototypen nicht sinnvoll getestet werden und wurde daher aus der Untersuchung herausgenommen. Fragen aus der Kategorie Individualisierbarkeit, wie z.B. ob sich die App für unterschiedliche Aufgaben anpassen lässt, waren nicht relevant, da ja nur eine Aufgabe (sichere Authentisierung) umgesetzt wird. Hier wurde lediglich die Frage, ob sich die App sowohl für Anfänger und Experten gleich gut eignet, untersucht. Diese wurde durchgängig positiv beantwortet.

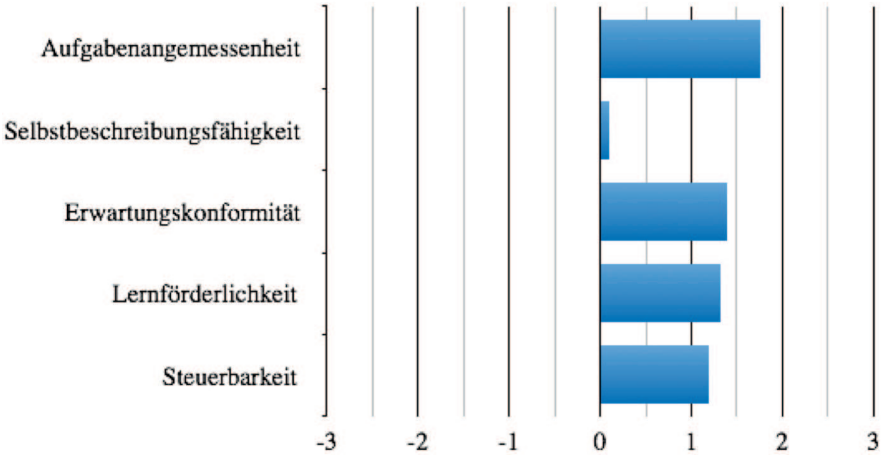

Abb. 5: Auswertung des Fragebogens (ISO 9241/110), Skala von −3 (sehr schlecht) bis 3 (sehr gut)

6 Fazit und Ausblick

Ziel dieser Arbeit war es festzustellen, ob ein auf dem Smartphone emulierter Ausweis von Nutzerinnen und Nutzern angenommen würde. Dabei wurde zunächst nur die Verwendung der Online-Ausweisfunktion für E-Business- und E-Government-Anwendungen untersucht. Die hoheitliche Ausweisfunktion, die z.B. im Rahmen einer polizeilichen Kontrolle verwendet wird, war nicht Gegenstand der Untersuchung.

Die Benutzbarkeit des untersuchten Prototypen wurde durchgängig positiv bewertet. Aus den Antworten der Testteilnehmer (siehe Abschnitt 5.1) lässt sich aber ableiten, dass das Vertrauen in die Anwendung eher gering ist. Dies hat mehrere Gründe:

- Selbst technisch nicht versierte Nutzer kennen die Gefahren, die von Schadsoftware auf Smartphones verursacht werden können. Auf der anderen Seite soll die

Online-Ausweisfunktion für Anwendungen eingesetzt werden, die ein hohes bis sehr hohes Sicherheitsniveau umsetzen müssen (z.B. Eröffnung eines Bankkontos, Abschluss eines Versicherungsvertrages, Abgabe der Steuererklärung). Dies empfanden die Testteilnehmer als Widerspruch. Hier müssen in weiteren Arbeiten Methoden (z.B. geeignete Visualisierung von Sicherheitsmechanismen) gefunden und untersucht werden, die diesen gefühlten Widerspruch auflösen.

- Die App wurde von Seiten der Testteilnehmer als Teil des Personalausweises verstanden. Insbesondere nahmen sie an, dass die App vom Staat bereitgestellt wird. An staatliche Einrichtungen wird aber mehr hinsichtlich der Umsetzung von Schutzmaßnahmen für IT-Sicherheit und Datenschutz erwartet. Zum einen, weil er als deutlich mächtiger empfunden wird als private Institutionen, zum anderen, weil staatlichen Stellen im Allgemeinen IT-Kompetenz nicht zugetraut wird. Auch hier müssen geeignete Methoden erarbeitet und untersucht werden, die Vertrauen in staatliche IT-Lösungen erzeugen.

Ein Problem verbleibt: Die Testpersonen sahen keinen Bedarf in der Verwendung der Online-Ausweisfunktion. Auch hierfür konnten mehrere Gründe aus den Antworten der geführten Tiefeninterviews abgeleitet werden:

Das Ergebnis aus Tabelle 1 zeigt, dass die Testpersonen sehr geringes Wissen bezüglich der Online-Ausweisfunktion haben. Dies liegt u.a. daran, dass das zuständige Ministerium die Online-Ausweisfunktion nur sehr wenig bewirbt (derzeit lediglich über die Internetplattform `http://www.personalausweisportal.de` und `http://www.ausweisapp.bund.de`).

Zwar gibt es bereits eine Vielzahl von Anwendungsfällen für die Online-Ausweisfunktion (siehe [BMI15]), für den durchschnittlichen Nutzer ergeben sich daraus aber lediglich ca. zwei Anwendungen jährlich (siehe [Ko16]). Umso wichtiger ist es, die Lösung so zu gestalten, dass sie benutzbar ist, also insbesondere ohne komplizierte Initialisierung auskommt und die Sicherheitsmechanismen, die eine Nutzerinteraktion benötigen, ohne Vorwissen genutzt werden können (bspw. Nutzung von biometrischen Merkmalen anstelle einer PIN).

Literaturverzeichnis

[As12] S. Asheuer, J. Belgassem, W. Eichhorn, R. Leipold, L. Licht, Ch. Meinel, A. Schanz und M. Schnjakin. Akzeptanz und Nutzerfreundlichkeit der AusweisApp: Eine qualitative Untersuchung. Technische Berichte Nr. 69 des Hasso-Plattner-Instituts für Softwaresystemtechnik an der Universität Potsdam, 2012.

[BoA16] Bank of America Newsroom. Bank of America Reports Fourth-quarter 2014 Net Income of $3.1 Billion, or $0.25 per Diluted Share. `http://newsroom.bankofamerica.com/press-releases/corporate-and-financial-news/bank-america-reports-fourth-quarter-2014-net-income-31-b`, Zugriff: 23.05.2016.

[Be10a] J. Bender, D. Kügler, M. Margraf und I. Naumann. Privacy-Friendly Revocation Management without unique Chip Identifiers for the German National ID Card. . In: Computer Fraud & Security. Vol. 2010, No. 9. (September 2010), pp. 14-17.

[Be10b] J. Bender, D. Kügler, M. Margraf und I. Naumann. Das Sperrmanagement im neuen deutschen Personalausweis. : Erschienen in: DuD-Datenschutz und Datensicherheit, Mai 2010.

[Be12] J. Bender, Ö. Dagdelen, M. Fischlin und D. Kügler: The PACE|AA Protocol for Machine Readable Travel Documents, and its Security. Financial Cryptography 2012: 344-358 (2012).

[BMI15] Bundesministerium des Innern (BMI). http://www.personalausweisportal.de/DE/Buergerinnen-und-Buerger/Online-Ausweisen/Online-Ausweisen_node.html, Zugriff: 25.05.2016.

[Gov15] Governikus GmbH & Co. KG. http://www.ausweisapp.bund.de, Zugriff: 5.12.2015.

[ID15] Initiative D21. 2015. eGovernment Monitor 2015: Nutzung und Akzeptanz von elektronischen Bürgerdiensten im internationalen Vergleich. Initiative D21 e.V., 2015, pp. 19-20.

[Ko16] S. Kostic, A. Heinemann, M. Margraf. Nutzungspotential der Online-Ausweisfunktion aus Sicht der Bürgerinnen und Bürger. Preprint 2016.

[Ot16] F. Otterbein, T. Ohlendorf und M. Margraf. Mobile Authentication with German eID. Extended Abstract for Presentation at the 2016 IFIP Summer School on Privacy and Identity Management, 2016.

[Pr09] J. Prümper und M. Anft. Beurteilung von Software auf Grundlage der Internationalen Ergonomie-Norm DIN EN ISO 9241-110 (Langfassung) http://people.f3.htw-berlin.de/Professoren/Pruemper/instrumente/ISONORM%209241-110-L.pdf, Zugriff: 25.05.2016.

[Ri13] M. Richter and M.D. Flückiger. Usability Engineering kompakt – Benutzbare Produkte gezielt entwickeln. Springer-Verlag, Berlin Heidelberg New York, 3. Auflage 2013.

[Ru13] S. Ruoti, N. Kim, B. Burgon, T. van der Horst und K. Seamons. 2013. Confused Johnny: When Automatic Encryption Leads to Confusion and Mistakes. In: Proceedings of the Ninth Symposium on Usable Privacy and Security (SOUPS 13). ACM, New York.

[Sn03] C. Snyder. Paper Prototyping - The Fast and Easy Way to Design and Refine User Interfaces. : Morgan Kaufmann, San Francisco, California, 2003.

[Wh99] A. Whitten and J. D. Tygar. 1999. Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0. In: Proceedings of the 8th conference on USENIX Security Symposium - Volume 8 (SSYM'99), Vol. 8. USENIX Association.

[Wi16] J. Willomitzer, A. Heinemann und M. Margraf. Zur Benutzbarkeit der AusweisApp2. In: Mensch und Computer 2016. Workshop Usable Security and Privacy: Ansätze und Lösungen zur nutzerzentrierten Entwicklung und Ausgestaltung von digitalen Schutzmechanismen. 2016.

[ZE16] DIE ZEIT. Wo Deutschland bei der Digitalisierung lahmt. http://www.zeit.de/digital/internet/2016-05/e-government-digitalisierung-deutschland-fortschrittsbericht, Zugriff: 25.05.2016.