Zur Benutzbarkeit der AusweisApp2

Jörg Willomitzer[1], Andreas Heinemann[2], Marian Margraf[3]

Institut für Informatik, AG ID Management, Freie Universität Berlin[1,3]
Fachbereich Informatik, AG User-Centered Security, Hochschule Darmstadt[2]

Zusammenfassung

Die Akzeptanz und Nutzung der Online-Ausweisfunktion des deutschen Personalausweises liegt hinter den Erwartungen zurück. Sie verlangte in der Vergangenheit vom Anwender den Einsatz der AusweisApp, die eine Reihe von Usability-Schwächen zeigt. Aus diesem Grund wurde bei der Neuentwicklung des Nachfolgers ─ der AusweisApp2 ─ auf den frühzeitigen und stetigen Einbezug des Anwenders geachtet. Im Rahmen von entwicklungsbegleitenden Usability-Untersuchungen konnten so frühzeitig Schwächen identifiziert und für die finale Version der AusweisApp2 eliminiert werden. Es zeigt sich jedoch auch, dass schwerwiegende Usability-Schwächen erst in der Interaktion des Gesamtsystems (Personalausweis, Kartenleser, AusweisApp2, Browser, Diensteanbieter) zum Vorschein treten und nicht durch die AusweisApp2 allein, sondern nur in der Betrachtung des Gesamtsystems zu lösen sind.

1 Einleitung

Mit der Einführung des neuen Personalausweises im November 2010 wurde auch eine kostenfreie Software (die sog. AusweisApp) zur Nutzung der Online-Ausweisfunktion bereitgestellt. Die Nutzung und Akzeptanz der Bevölkerung für diese Funktion blieb jedoch hinter den Erwartungen zurück. So betrug die Freischaltquote der Online-Ausweisfunktion auch drei Jahre nach Einführung ca. 28% (Fromm et al. 2013). Weniger als ein Drittel der Besitzer eines neuen Personalausweises ließ also die eID-Funktion des Ausweises freischalten, der prozentuale Anteil der tatsächlichen Nutzung dürfte noch weitaus niedriger liegen, da „nicht jede aktivierte Online-Ausweisfunktion auch zu deren Einsatz bei der Nutzung von Diensten [führt]“ (Fromm et al. 2013).

Eine Ursache für eine geringe Nachfrage von Sicherheitssoftware ist die Annahme der Nutzer, die erforderlichen Maßnahmen für ihre Sicherheit nicht durchführen und das Gefühl, die Konsequenzen von Handlungen nicht abschätzen zu können. Zieht man die Ergebnisse von Studien zu Vertrauen und Sicherheit im Internet heran (BitKom e. V. 2012, Deutsches Institut für Vertrauen und Sicherheit in der Informationstechnik 2012), so ist die Unsicherheit bei älteren Internetnutzern (65 Jahre und älter) besonders groß. Diese Gruppe hat aufgrund ihrer „geringen

Veröffentlicht durch die Gesellschaft für Informatik e.V. 2016 in
B. Weyers, A. Dittmar (Hrsg.):
Mensch und Computer 2016 – Workshopbeiträge, 4. - 7. September 2016, Aachen.

http://dx.doi.org/10.18420/muc2016-ws03-0002

Internet- und IT-Kompetenz ein starkes Bedürfnis nach mehr Sicherheit im Internet“, hält sich aber „aus Furcht, Fehler zu machen und für unsachgemäße Bedienung strafrechtlich zur Verantwortung gezogen zu werden“, sehr zurück (Deutsches Institut für Vertrauen und Sicherheit in der Informationstechnik 2012). An dieser Gruppe zeigt sich, dass nicht in erster Linie eine unzureichende Security Awareness, sondern eine mangelnde Benutzbarkeit anzuführen ist.

Projiziert man diese Erkenntnis auf die Software zur Nutzung der Online-Ausweisfunktion des Personalausweises, so liegt die Vermutung nahe, dass für eine Steigerung der Nutzungszahlen die Bedienfreundlichkeit ─ besonders für ältere oder technisch weniger versierte Personen ─ erhöht werden muss.

Mit dieser Erkenntnis wurde 2014 im Auftrag des Bundesamtes für Sicherheit in der Informationstechnik (BSI) mit der Entwicklung eines Nachfolgers, der sog. *AusweisApp2* begonnen. Hierbei sollten besonders der Nutzer, seine Fähigkeiten, Kenntnisse, Bedürfnisse und Erwartungen im Mittelpunkt stehen. Vorliegender Beitrag stellt das entwicklungsbegleitende Vorgehen und die gewonnenen Erkenntnisse zur Benutzbarkeit der AusweisApp2 vor.

Die weitere Arbeit ist wie folgt gegliedert: In Abschnitt 2 werden zunächst Vorarbeiten und verwandte Arbeiten diskutiert. Abschnitt 3 beschreibt das Vorgehen bei der angewendeten begleitenden nutzer-zentrierten Softwareentwicklung der AusweisApp2. Die Erkenntnisse und welche Ergebnisse hiervon bei der Umsetzung berücksichtigt werden konnten, werden in Abschnitt 4 vorgestellt. Die Arbeit schließt mit einer Zusammenfassung und einem Ausblick.

2 Vorarbeiten und verwandte Arbeiten

Für das Konzept, den Nutzer beim Design und der Umsetzung von Sicherheitssoftware stärker in den Mittelpunkt zu setzen, prägten Zurko und Simon (1996) den Begriff *User-Centered Security*. Mit Ausrichtung auf den Nutzer ist eine Berücksichtigung seiner Bedürfnisse und Fähigkeiten sowie seines Wissensstandes gemeint. Zurko und Simon beschränken sich hierbei nicht nur auf Software, sondern verweisen mit dem Begriff auf Sicherheitsmodelle, Sicherheitssysteme und Sicherheitssoftware, die Usability/Nutzerfreundlichkeit als Hauptziel haben. Sie stellen die These auf, Privatpersonen erwerben oder setzen keine Sicherheitssoftware ein, die sie nicht verstehen. Sie beschreiben ein generelles Desinteresse der Endbenutzer an Sicherheitssoftware, was nach ihnen in der fehlenden Verschmelzung mit (bekannten) Aspekten von Nutzerfreundlichkeit begründet liegt.

Ein Lösungsansatz könnte darin bestehen, den Nutzer möglichst alle Schritte abzunehmen und ihn mit dem Sicherheitskonzept nicht zu behelligen. Dies kann jedoch zum einen den Nutzer verunsichern und ist zum anderen auch kein Garant für das Ausbleiben von Fehlern bei der Bedienung und dadurch entstehenden Sicherheitslücken (Ruoti et al. 2013).

Es soll also weder Sicherheit zugunsten von Benutzbarkeit geopfert werden, noch soll die Software aufgrund komplizierter Bedienung Laien und ungeübte Personengruppen von einem Einsatz abhalten. Ziel der sog. *Usable Security* ist es nun ein angemessenes Sicherheitsniveau zu bieten und zugleich einfach und komfortabel in der Bedienung zu sein. Dies gelingt nur,

wenn der Nutzer das zugrundeliegende Konzept versteht und so in der Lage ist, die von ihm zu tätigen Handlungen in richtiger Reihenfolge und fehlerfrei ausführen zu können.

Ein weiterer, bedeutender Aspekt bei der Betrachtung von Sicherheitssoftware ist das ihr entgegengebrachte Vertrauen. Ohne ein hinreichendes Maß an Vertrauen wird sie nicht zum Einsatz kommen. Laut Patrick et al. (2005) führt unzureichendes Vertrauen zu falschen oder dem Ausbleiben von Entscheidungen und damit zu einer Gefährdung der Sicherheit eines Systems.

Das weitere Vorgehen berücksichtigt die eben genannten Aspekte, indem alle relevanten Nutzergruppen analysiert werden und schon in den ersten Empfehlungen die Ergebnisse dieser Analyse und vertrauensbildende Maßnahmen einbezogen werden.

3 Vorgehen

Wie in Abschnitt 1 und 2 motiviert, wird der Nutzer bei allen Überlegungen in den Mittelpunkt gestellt. Zudem soll er von Anfang an in einem iterativen Entwicklungsprozess involviert werden. Hiervon ausgehend gliedert sich das Vorgehen in drei Phasen:

Phase 1: Zuerst wurden in einer Voruntersuchung Studien zur aktuellen AusweisApp gesichtet und ausgewertet. Darüber hinaus wurde abgesteckt, was die Charakteristika von potentiellen Nutzern sind, und welche Fähigkeiten und Bedürfnisse diese mitbringen. Die Erkenntnisse aus den Recherchen bildeten die Grundlage für erste Empfehlungen hinsichtlich des Funktionsumfangs, der allgemeinen Gestaltung und der Dialoggestaltung der AusweisApp2.

Die Eigenschaften der potentiellen Nutzer ergaben sich aus Erkenntnissen einer im Auftrag des Deutschen Instituts für Vertrauen und Sicherheit vom SINUS-Instituts Heidelberg durchgeführten Grundlagenstudie zu Vertrauen und Sicherheit im Internet (Deutsches Institut für Vertrauen und Sicherheit im Internet 2012). Hier werden sieben Internet-Milieus identifiziert, die unterschiedliche Einstellungen gegenüber Sicherheit und Datenschutz haben. Die Haltung der einzelnen Milieus wird u. a. maßgeblich durch ihr technisches Verständnis und der Häufigkeit der Nutzung von digitalen Systemen (vornehmlich Heimcomputer) bestimmt.

Phase 2: In dieser Phase wurden erste Prototypen der AusweisApp2 von Usability-Experten evaluiert. In einer heuristischen Evaluation wurde die Software auf Verstöße gegen die in der Grundsatznorm DIN EN ISO 9241-110 formulierten Grundsätze der Dialoggestaltung untersucht. Bei einem Verstoß gegen eine gewünschte Eigenschaft liegt ein potenzielles Usability-Problem vor, wobei aber durch den Kontext der Nutzung keine Kausalität zwischen beiden besteht.

Im anschließenden Cognitive Walkthrough versetzten sich Usability-Experten in die Nutzerrolle, wodurch eine „Verbindung der allgemeinen Usability-Expertise mit Wissen über die Anwendungsdomäne und die Zielgruppe angestrebt“ wird (Sarodnick und Brau 2006). Bei der Simulation von typischen Arbeitsschritte bei der Verwendung der Software, wurden potentiellen Usability-Schwächen dokumentiert und darauf aufbauend Empfehlungen für die Gestaltung erarbeitet.

Phase 3: Hier wurde die Software von Testnutzern evaluiert und so tatsächlich auftretende Usability-Probleme identifiziert. Für die Nutzertests wurden 30 Testpersonen zu gleichen prozentualen Teilen aus sechs der sieben Milieus der eingangs erwähnten Milieu-Studie (Deutsches Institut für Vertrauen und Sicherheit im Internet (2012)) akquiriert. Die Gruppe *Internetferne Verunsicherte* wurde aufgrund ihrer Charakteristika („Fast zwei Drittel (63 Prozent) nutzen nie das Internet […], auch das verbleibende Drittel geht nur selten online. Dieses Verhalten steht im Einklang mit einer generellen Distanz zu modernen Technologien“) als nicht potentielle Nutzergruppe eingestuft und fand somit keine Berücksichtigung.

In gewohnter Arbeitsumgebung sollten die Probanden ihnen gestellte Aufgabe lösen. Dabei sollten sie ihre Gedanken und Überlegungen laut äußern (Thinking-Aloud-Test (Sarodnick und Brau 2006). Für eine spätere Auswertung wurden Bildschirm und Ton aufgezeichnet. Hilfestellung wurde nur gegeben, wenn der Teilnehmer in dieser Situation auch sonst Hilfe von Dritten (z.B. Freunden) in Anspruch genommen hätte (z. B. bei der Installation von Software (AusweisApp2 oder PDF-Reader für das Handbuch) oder Treibern für das Kartenlesegerät).

4 Ergebnisse

4.1 Voruntersuchung

In den gesichteten Studien (Fromm et al. 2013, Hasso-Plattner-Institut 2013) wurden in erster Linie die Bedienung der Software kritisiert und zusätzliche Funktionen gewünscht. Einige Befragte gaben an, wegen Sicherheitsbedenken die Online-Ausweisfunktion des Personalausweises nicht haben freischalten lassen. Diese Bedenken beruhen aber nicht auf Kenntnis von Schwachstellen der aktuellen Lösung, sondern auf Misstrauen gegenüber Technik (im Allgemeinen) bzw. den dahinterstehenden staatlichen Einrichtungen. Es wird also nicht berechtigterweise die existierende Umsetzung als ungenügend eingestuft, sondern aufgrund fehlender Kenntnisse über eingesetzte Technologie und zugrundeliegender Sicherheitskonzepte auf einen Einsatz vorsichtshalber verzichtet.

Ein weiterer Kritikpunkt war die, aufgrund der geringen Anzahl an verfügbaren Diensten, fehlende Einsatzmöglichkeit. Dieses ist das typische Henne-Ei Problem: Bedingt durch geringe Nutzerzahlen wird der Dienst nur von wenigen Anbietern offeriert, gleichzeitig interessieren sich nur wenige Nutzer für die neue Möglichkeit, solange nicht mehr Dienste angeboten werden.

Die Studie des Hasso-Plattner-Instituts kommt zu dem Fazit: „Die Usability der Software ist verbesserungswürdig und die Hürden der Nutzbarkeit werden auf die Technologie ‚Online-Ausweisfunktion’ projiziert.“ Neben einer geringen Nutzerfreundlichkeit wird vor allem die Vertrauenswürdigkeit der Online-Ausweisfunktion als gering eingestuft. Dies lag nicht an tatsächlichen Sicherheitslücken, sondern an der Summe von „Kleinigkeiten“ wie unterschiedliche Designs verschiedener offizieller Webseiten zur AusweisApp oder fehlenden Informationen zur Nutzung der Anwendung.

Es wurde deutlich, dass die neue Version der AusweisApp für eine bessere Akzeptanz besonders zwei der problematischen Eigenschaften von Sicherheit adressieren muss:

- Zum einen ist der Nutzer unmotiviert die Software einzusetzen, wenn sie nur das Sicherheitsniveau anhebt, ohne für ihn einen anderen ersichtlichen Vorteil zu bieten. Stellt z. B. ein Dienst der Online-Ausweisfunktion lediglich eine Alternative für einen bisher gewohnten Login da, ist der Nutzer höchst wahrscheinlich unmotiviert die bisher gewohnte Methode zu Gunsten der Neuen zu verwerfen.
- Zum anderen wird von einem Nutzer gefordert, sich mit Sicherheitsstrategien zu befassen. Gerade das Konzept der Zwei-Faktor-Authentisierung oder der Sinn und Zweck des Zertifikats des Dienstanbieters erschlossen sich ihm nicht.

Obwohl Nutzer mit dem Konzept der Zwei-Faktor-Authentisierung eigentlich hinlänglich vertraut sind (EC-Karte, SIM-Karte), ist ihnen die verfolgte Strategie dahinter und der dadurch erzielte Sicherheitsgewinn unklar. Da die vorhandenen Broschüren oftmals keine Beachtung finden, sollte dies ihm in kurzweiliger Form (beispielsweise ein mit der Software ausgeliefertes Einführungsvideo) vermittelt werden.

Für den ersten Prototypen der AusweisApp2 wurden ─ den Empfehlungen von Patrick et al. (2005) folgend ─ vertrauensbildende Maßnahmen berücksichtigt. So orientiert sich das Erscheinungsbild an den Design-Guidelines des jeweiligen Betriebssystems, bekannte Elemente wie die von Geldscheinen bekannte Guilloche (ineinander verwickelte und überlappende Linienzüge, die eine Fälschung erschweren sollen) werden beim Zertifikat angezeigt und Hintergrundinformationen über den Anbieter oder das angebotene Produkt werden zur Verfügung gestellt. Abbildung 1 zeigt die Vorgängersoftware, Abbildung 2 den Prototypen, der zum Start der Expertentests vorlag[1].

4.2 Analytische Evaluation

Bei heuristische Evaluation wurden 81 Normverletzungen[2] identifiziert, wobei hier anzumerken ist, dass diese sehr unterschiedliche Auswirkungen auf die Nutzerfreundlichkeit haben.

Die Erkenntnisse aus dem Cognitive Walkthrough zeigten, welche Auswirkung es haben kann, wenn das Sicherheitsmodell (hier durch den Ausweis) schon vorgegeben ist, statt auf Grundlage des Nutzungskontextes gewählt zu werden. Hier weicht das zugrunde liegende Konzept von PIN und PUK (PIN unlock key) von den dem Nutzer bekannten Konzepten ab. Bei Neubeantragung des Ausweises erhält der Nutzer einen Brief mit einer 5-stelligen Transport-PIN und einer PUK. Diese Transport-PIN muss vor der ersten Authentifizierung durch eine persönliche 6-stellige PIN ersetzt werden, welche fortan beim eigentlichen Ausweis-Prozess oder beim Ändern der PIN eingegeben werden muss.

[1] Alle referenzierten Abbildungen finden sich im Anhang.

[2] Bericht kann bei der Governikus GmbH & Co. KG angefragt werden.

Der Ausweis sieht keine Möglichkeit vor, um zu erfragen, ob die persönliche PIN bereits gesetzt wurde. Somit kann die Software als Schnittstelle nicht darüber informieren und das initiale Setzen der 6-stelligen PIN wird oftmals vergessen bzw. (unbewusst) übergangen. Dies hat zur Folge, dass die Transport-PIN beim Ausweisvorgang eingegeben wird, was zu einem Fehler führt.

Anders als sonst üblich kann auch mit der PUK die PIN nicht neu gesetzt werden, sondern bei gesperrtem Ausweis (infolge dreimaliger Falscheingabe der aktuellen PIN) die PIN ein weiteres Mal eingegeben werden. Beim Durchspielen des Szenarios „Nutzer hat PIN vergessen und möchte diese neu setzen" stießen die Experten daher gleich auf mehrere potentielle Probleme. So war zum einen die Rückmeldung nicht objektiv/konstruktiv formuliert. Zum anderen musste aufgrund der ungewohnten Funktion der PUK zwischen Anzeige und externen Informationen (Brief der Bundesdruckerei) gewechselt werden.

4.3 Empirische Evaluation

Bei der Evaluierung durch Nutzer wurde deutlich, welchen großen Einfluss Vorkenntnisse über PC-Systeme auf die Evaluationsergebnisse haben. Bei der Gruppe *Ordnungsfordernde Internet-Laien* (Deutsches Institut für Vertrauen und Sicherheit im Internet (2012)), also der Nutzergruppe mit dem geringsten Wissen und Übung im Umgang mit digitalen Geräten, lag die Abbruchquote bei 100% (über alle Nutzer im Durchschnitt bei 75%). Die Nutzer aus diesem Milieu hatten große Schwierigkeiten mit der Installation der benötigten Hardware („Ich könnte das nie alleine. Da müsste ich meinen Sohn anrufen."). Daraus resultierte ein enormer Zeitaufwand von bis zu 2,5 Stunden für die Bearbeitung der Testaufgaben.

Ohne eine umfangreiche Hilfestellung zur Einrichtung von Kartenlesegeräten durch die AusweisApp2 ist ein Großteil dieser Gruppe nicht in der Lage die Online-Ausweisfunktion zu nutzen. Durch die Bereitstellung eines Einrichtungs-Assistenten, der bei der Installation des benötigten Treibers unterstützt, soll diese Einstiegshürde abgebaut werden.

Dieses Problem stellt eines der drei schwerwiegenden Usability-Probleme dar, die in bei der Verwendung der Online-Ausweisfunktion aufgetreten sind. Die zwei weiteren sind/waren:

- Der Zustand der Karte war dem Nutzer unklar. Es wurde ihm nicht mitgeteilt, ob er schon seine persönliche 6-stellige PIN gesetzt hat, bzw. ob die Ausweisfunktion bei seinem Ausweis überhaupt aktiviert ist.
- Die Interaktion mit Display-Kartenlesern ist höchst problematisch, da Benutzer die Anzeige des Lesegerätes nicht wahrnehmen und daher häufig Timeouts in der Kommunikation zwischen PC und Lesegerät auftreten, die sie sich nicht erklären können („Bei dem Dialog PIN-Änderung gibt es im Kartenlesegerät […] keinen Hinweis darauf, dass die PIN-Eingabe wiederholt werden soll. Könnten die einen ja mal ruhig sagen", „Warum muss ich die jetzt 2mal eingeben? Das hab ich doch eben schon gemacht").

Zudem ist das Konzept der Zwei-Faktor-Authentisierung dem Nutzer unklar und der Mehrwert wird nicht gesehen. Obwohl dies keine Usability-Schwäche im eigentlichen Sinne darstellt, ist es für die Nutzung der Online-Ausweisfunktion doch essentiell, dass die AusweisApp2 sich

diesem Problem annimmt. Die Software steht quasi stellvertretend für die Online-Ausweisfunktion und ist oftmals erste Anlaufstelle, wenn ein neuer Besitzer des Ausweises zu Hause sich über die Möglichkeiten und Vorteile informieren möchte.

Bei technisch versierte Personen war das Feedback zur neuen Version durchweg positiv („Die Anwendung ist auch viel komfortabler und schneller als die Nutzung der AusweisApp“, „Insgesamt finde ich die App ansprechend und im Unterschied zur Ausweis-App von Openlimit funktioniert sie auch.“). Besonders Nutzer, die bereits die Vorgängerversion genutzt haben, erwähnten die Verbesserung bezüglich der Usability und die sinnvolle Erweiterung des Funktionsumfangs. Insbesondere die genaue Beschreibung des Systemzustandes und Informationen über durchzuführende Schritte wurden positiv bewertet (siehe Abbildung 3 und den überarbeiteten Dialog in Abbildung 4).

5 Zusammenfassung und Ausblick

Durch das im Rahmen dieser Arbeit vorgestellte Vorgehen und die Ergebnisse konnten insgesamt gute Verbesserungen hinsichtlich der Nutzerfreundlichkeit der AusweisApp2 erzielt werden, insbesondere durch Überarbeitung der Dialoge, genaue Beschreibung des Systemzustands und durchzuführender Aktionen (siehe Abbildung 5). Neue Features wie eine Übersicht über getätigte Ausweisvorgänge (Abbildung 6) und Einsatzmöglichkeiten (Abbildung 7) werden geschätzt und sorgen dafür, dass die Software als Anlaufstelle für die Online-Ausweisfunktion genutzt wird.

Die noch existierenden schwerwiegenden Usability-Probleme fallen jedoch, obwohl kein direkter Zusammenhang zu der Usability der AusweisApp2 besteht, auf die Software und somit auch auf die Online-Ausweisfunktion des Personalausweises zurück. Hier zeigt sich, wie wichtig es ist, den Nutzungskontext und gesamten Lebenszyklus einer Software zu berücksichtigen. So wären bei einer Einschränkung des Probandenkreises auf technisch versierte Nutzer oder der Vorkonfiguration der Testumgebung die Schwächen nicht identifiziert oder nicht als schwerwiegend eingestuft worden.

In der Weiterentwicklung und Pflege der AusweisApp2 sollte der Gewinn an Sicherheit durch die Zwei-Faktor-Authentisierung der Online-Ausweisfunktion dem Nutzer einfach verständlich (z.B. in Form von Einführungsvideos) näher gebracht werden.

Der Untersuchungsfokus lag auf der Evaluation der Nutzerfreundlichkeit. Die im Design der AusweisApp2 berücksichtigten Richtlinien zum Herstellen von Vertrauen wurden aktuell nicht evaluiert. Hier sind weitere Arbeiten geplant.

Literaturverzeichnis

BitKom e. V. (2012). Vertrauen und Sicherheit im Netz. https://www.bitkom.org/Publikationen/2012/Studie/Vertrauen-und-Sicherheit-im-Netz/Vertrauen-und-Sicherheit-im-Netz.pdf. Abruf am 19.05.2016.

Bundesamt für Sicherheit in der Informationstechnik (2012). Leitfaden Informationssicherheit: IT-Grundschutz kompakt. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Leitfaden/GS-Leitfadenpdf.html. Abruf am 26.05.2016.

Deutsches Institut für Vertrauen und Sicherheit im Internet (2012). DIVSI Milieu-Studie zu Vertrauen und Sicherheit im Internet. https://www.divsi.de/sites/default/files/presse/docs/DIVSI-Milieu-Studie_Gesamtfassung.pdf. Abruf am 26.05.2016.

Fromm, J., Heptner, P., Pattberg, J., und Welzel, C. (2013). 3 Jahre Online-Ausweisfunktion - Lessons Learned. http://publica.fraunhofer.de/documents/N-265058.html. Abruf am 20.05.2016.

Hasso-Plattner-Institut (2013). Akzeptanz und Nutzerfreundlichkeit der AusweisApp: Eine qualitative Untersuchung. http://opus.kobv.de/ubp/volltexte/2013/6397/pdf/tbhpi69.pdf. Abruf am 25.05.2016.

Patrick, A., Marsh, S., und Briggs, P. (2005). Designing Systems that People will Trust. L. Cranor & S. Garfinkel (Eds.), Security and Usability: Designing Secure Systems That People Can Use. O'Reilly & Associates.

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

Sarodnick, Florian; Brau, H. (2006). Methoden der Usability Evaluation: Wissenschaftliche Grundlagen und praktische Anwendung. Verlag Hans Huber.

Zurko, M. E. und Simon, R. T. (1996). User-centered Security. In Proceedings of the 1996 Workshop on New Security Paradigms, New York, NY, USA. ACM.

Anhang

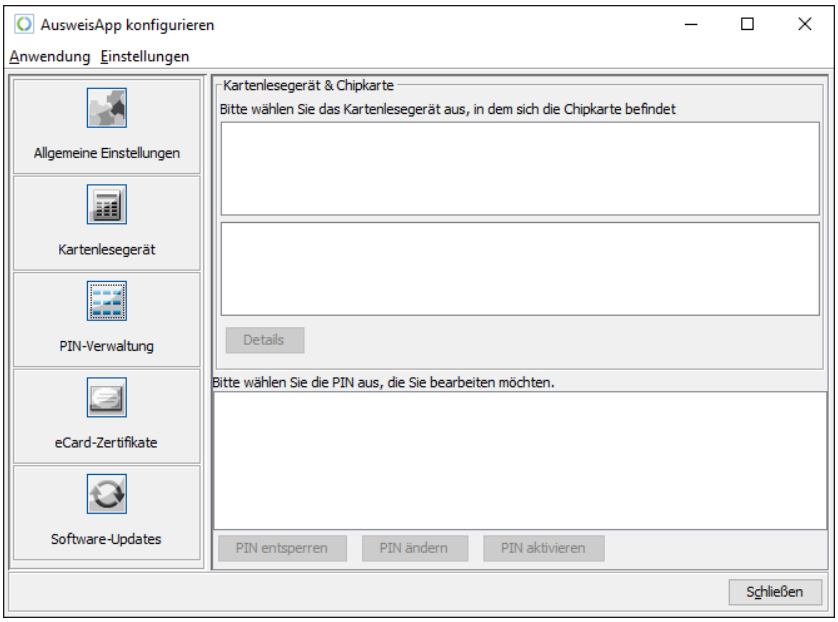

Abbildung 1: AusweisApp (Version 1.11) - Dialog PIN-Verwaltung bei nicht angeschlossenem Kartenleser

Abbildung 2: Prototyp der AusweisApp2 in der Version 0.6 - Startbildschirm mit bekannten Elementen wie Personalausweis und Logo der Online-Ausweisfunktion

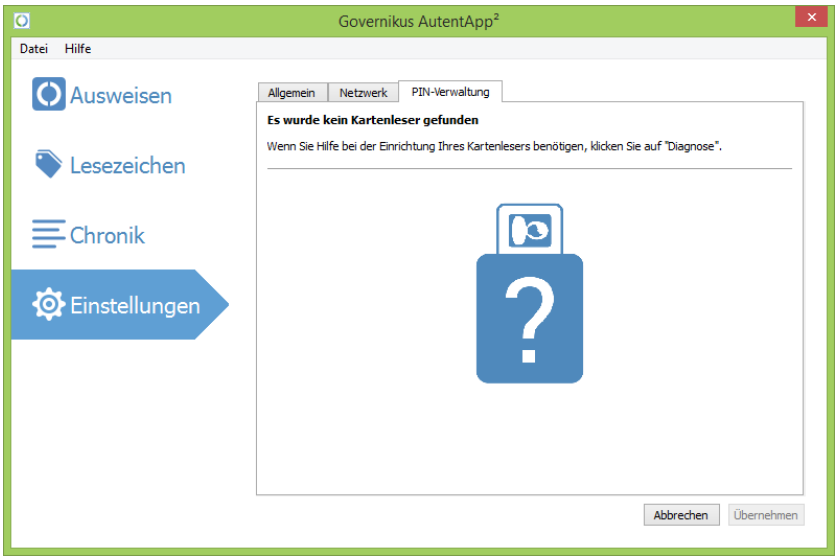

Abbildung 3: AusweisApp2 (Version 0.8.1) zum Start der empirischen Evaluation – Dialog PIN-Verwaltung bei nicht angeschlossenem Kartenleser

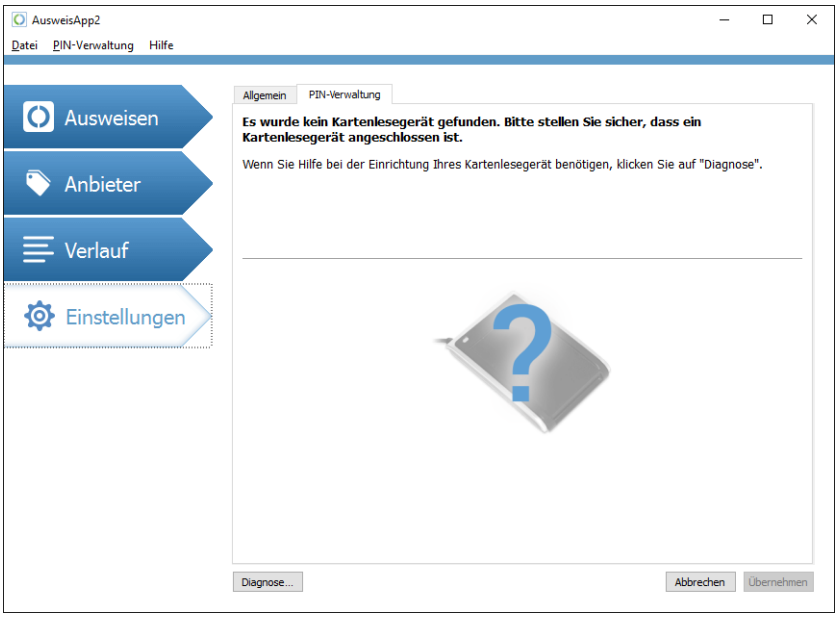

Abbildung 4: AusweisApp2 (Version 1.8.0) vom 26. Mai 2016 - Dialog PIN-Verwaltung

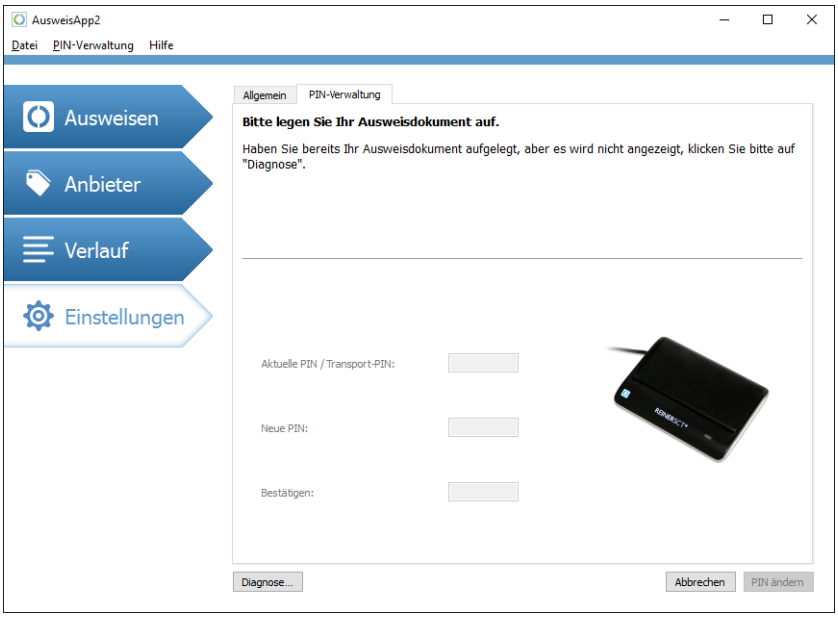

Abbildung 5: AusweisApp2 (Version 1.8.0) - Dialog PIN-Verwaltung

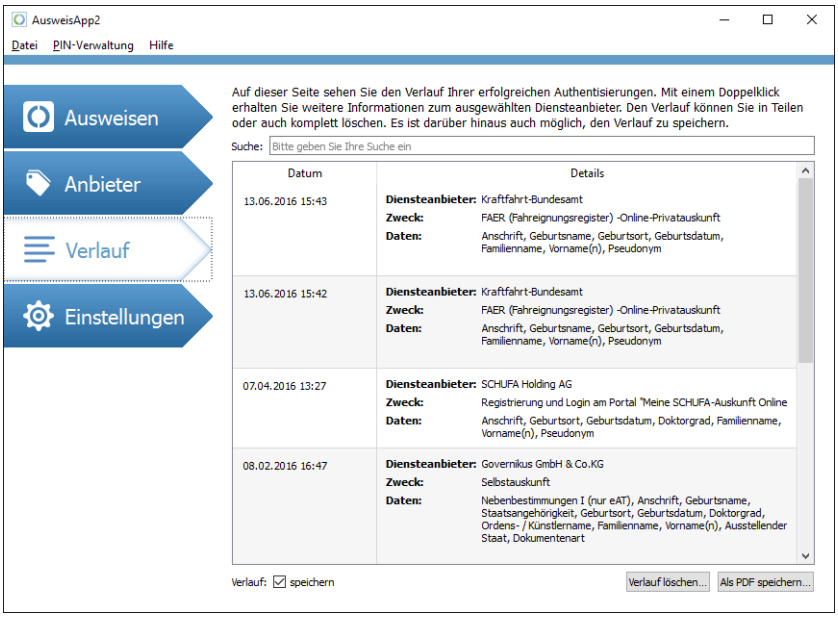

Abbildung 6: AusweisApp2 (Version 1.8.0) - Dialog Verlauf

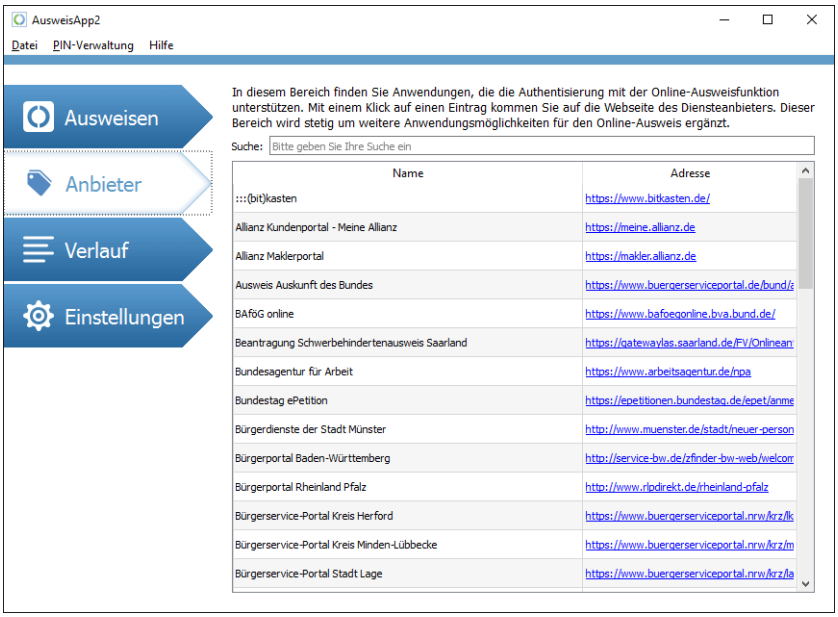

Abbildung 7: AusweisApp2 (Version 1.8.0) - Dialog Anbieter