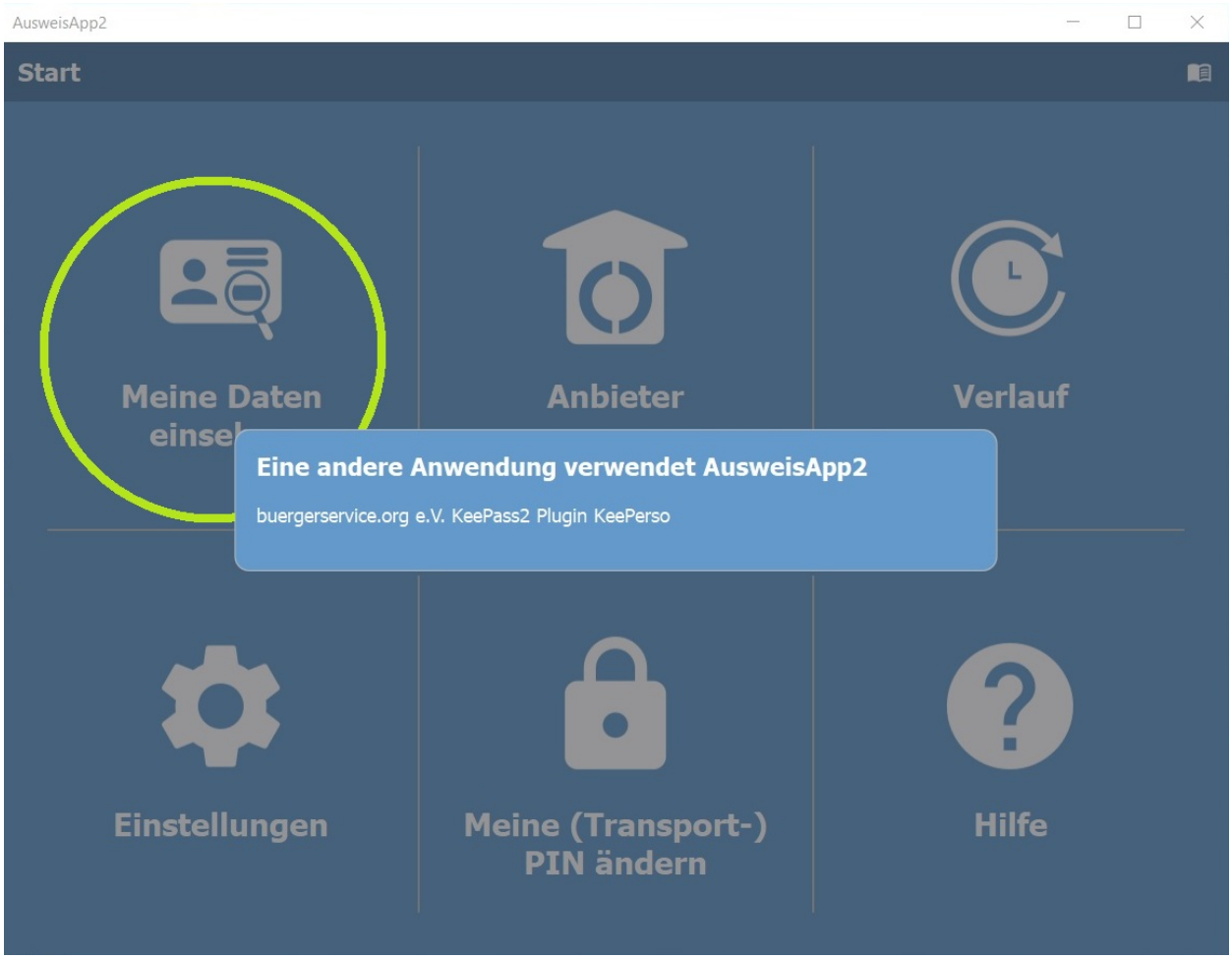
buergerservice.org e.V. -
Faktencheck Online-Ausweis (SdS)
Selbstschutz durch Selbstauskunft (SdS)



Der Faktencheck wird herausgegeben von

buergerservice.org e.V.

Vertreten durch:

Rudolf Philipeit (Vorstand)

rudolf.philipeit@buergerservice.org

Berliner Straße 5, 91522 Ansbach



Faktencheck Online-Ausweis: Selbstschutz durch Selbstauskunft (SdS)

Impressum

Herausgeber		
buergerservice.org e.V. Berliner Str. 5, D-91522 Ansbach		
Dateiname	**Dokumentennummer**	**Dokumentenbezeichnung**
20211103buergerservice.org_Faktencheck_Selbstschutz_durch_Selbstauskunft_SdS.docx	FC001	Faktencheck
Version	**Stand**	**Status**
1.4	03.11.2021	Abgestimmt
Autor	**Inhaltlich geprüft von**	**Freigegeben von**
Rudolf Philipeit	buergerservice.org unter Verwendung von Kommentaren der zuständigen Vertreter des Bundesverwaltungsamtes (BVA) und des Bundesamtes für Sicherheit in der Informationstechnologie (BSI)	buergerservice.org
Ansbach		
Ansprechpartner	**Telefon / Fax**	**E-Mail**
Rudolf Philipeit	Tel.: +49 (171) 3366669 Fax: +49 (981) 4815033	rudolf.philipeit@buergerservice.org
Kurzinfo		
Faktencheck Online-Ausweis: Selbstschutz durch Selbstauskunft (SdS)		

Copyright © 2021 buergerservice.org e.V., 91522 Ansbach

Alle Rechte, auch die des auszugsweisen Nachdrucks, der fotomechanischen Wiedergabe (einschließlich Mikrokopie) sowie der Auswertung durch Datenbanken oder ähnliche Einrichtungen, vorbehalten.



Inhaltsverzeichnis

Einleitung 1
Grundsätzliche Erläuterungen 2
Was ist Online-Ausweisen? 2
Was ist die Selbstauskunft beim Online-Ausweisen? 3
Was ist das Vertrauensniveau? 3
Selbstschutz durch Selbstauskunft (SdS) 4
Motivation 4
Einsatzfelder und Anwendungsmöglichkeiten 4
Pilotanwendungen - Einleitung 5
Pilotanwendung 1: KeePerso für KeePass2 5
Konzept 5
Umsetzung 5
Nutzen 6
Risiken und Gegenmaßnahmen 7
Pilotanwendung 2: PersonalausweisCredentialProvider (Win 10) 8
Konzept 8
Umsetzung 8
Nutzen 9
Risiken und Gegenmaßnahmen 9
Pilotanwendung 3: eID-Passwortgenerator PersoPassGen 11
Konzept 11
Umsetzung 11
Nutzen 12
Risiken und Gegenmaßnahmen 12
Pilotanwendung 4: eID-Türöffner MyPersoDoor 14
Konzept 14
Umsetzung 14
Nutzen 15
Demonstrator 16
Risiken und Gegenmaßnahmen 16

buergerservice.org



Faktencheck Online-Ausweis: Selbstschutz durch Selbstauskunft (SdS)

Faktencheck 18

Recht 18

Sicherheit 18

Allgemein 18

Darstellung der Beteiligten und Ansprechpartner 20

Abkürzungsverzeichnis 23

Anhang 24

buergerservice.org



Abbildungsverzeichnis

Abbildung 1: Auswahl KeePerso KeyProvider 5
Abbildung 2: Login-Seite von Windows 10 8
Abbildung 3: Anwendung PersoPassGen 11
Abbildung 4: Anwendung MyPersoDoor 14
Abbildung 5: Demonstrator MyPersoDoor 16

buergerservice.org



Faktencheck Online-Ausweis: Selbstschutz durch Selbstauskunft (SdS)

Einleitung

Nach über 25 Jahren Internet als Massenmedium muss man sich bis heute weltweit mit vielen Gefahren im Netz nahezu hilflos abfinden. In Deutschland haben alle Bürgerinnen und Bürger allerdings ein wirksames Gegenmittel verfügbar, welches im globalen Internet bisher noch gänzlich unbekannt ist. Es handelt sich um den Personalausweis mit Online-Ausweisfunktion (eID), welcher nach dem 10-jährigen Roll-Out seit dem 1.11.2020 bei nahezu allen deutschen Staatsbürgern im Portemonnaie steckt und so, wie auch das Smartphone, ständig mitgenommen wird. Deutschland befindet sich mit der Art der technologischen, organisatorischen, prozessualen, rechtlichen und benutzerfreundlichen Umsetzung beim Online Ausweisen im internationalen Vergleich in einer Pole-Position bzgl. sicherer digitaler Identitäten (SDI) und selbstbestimmter Identität (Self-Sovereign Identity (SSI)).

Das Online-Ausweisen ermöglicht den rechtsgültigen gegenseitigen elektronischen Identitätsnachweis, wie er nur durch Staaten für die Einwohner realisiert werden kann[1]. Das ist der Grund dafür, dass es im globalen Internet eine derartige Funktion nicht allgemeingültig gibt. Was das globale Internet nicht anbieten kann, können auch die Nutzer des Netzes nicht kennen. Und so fühlt sich das Online-Ausweisen im weltweiten Internet zunächst wie ein Fremdkörper an und wird ignoriert. An diesem Punkt ist Aufklärungsarbeit erforderlich, damit die Bürgerinnen und Bürger die Rolle des Staates bei der Herstellung sicherer digitaler Identitäten für mehr Sicherheit im Netz erkennen und mittragen.

buergerservice.or e.V. ist als gemeinnütziger Verein angetreten, um das Wissen um das Online-Ausweisen für mehr Akzeptanz und Nutzung der Funktion zu verbreiten. Aus Sicht von buergerservice.org ist es damit möglich, das digitale Gemeinwohl in unserem Land deutlich zu verbessern.

Das Wissen rund um die Online-Ausweisfunktion ist in nahezu allen Bereichen der Gesellschaft noch nicht vorhanden. So kommt es häufig zu Fehlinterpretationen bei ersten Berührungen mit den unterschiedlichen Varianten und den vielfältigen Funktionen beim Online-Ausweisen und den zugehörigen Diensten.

Mit diesem Faktencheck wird die Funktion Selbstauskunft herausgegriffen. Es wird aufgezeigt, wie die Funktion Selbstauskunft beim Deutschen Personalausweis für einen besseren Selbstschutz zum Einsatz gebracht werden kann und welche Fakten dabei eine Rolle spielen.

Der Faktencheck trägt den Titel:

Selbstschutz durch Selbstauskunft

Über weitere Werkzeuge und Modelle, wie die Akzeptanz und Nutzung für das Online-Ausweisen gesteigert werden kann, informiert buergerservice.org auf der Webseite www.buergerservice.org.

[1] Staaten verwalten die Identitäten ihrer Einwohner und organisieren das Rechtswesen zur Ahndung jeglicher Vergehen.



Grundsätzliche Erläuterungen

Für ein besseres Verständnis der Ausführungen im Dokument sollen zunächst das Ausweisen mit dem Personalausweis und die Eigenprüfung des Personalausweises in der analogen Welt den zugehörigen Online-Varianten gegenübergestellt werden. Dies ist deshalb von Bedeutung, da die rechtlichen Aspekte für beide Varianten prinzipiell gleich zu bewerten sind. So soll es dem Leser gelingen, das vorhandene Wissen aus der analogen Welt für die Online-Varianten beim Ausweisen zu interpretieren.

Was ist Online-Ausweisen?

Wir kennen alle das Ausweisen mit unserem Personalausweis in der analogen Welt. Vom Staat erhalten wir mit dem Deutschen Personalausweis ein mit vielen Sicherheitsmerkmalen ausgestattetes Dokument, mit welchem wir uns gegenüber einem Dritten ausweisen können (unsere Identität nachweisen können). Der Dritte, z.B. ein Kundenberater in der Bank, vergleicht dabei das Foto auf dem Ausweis mit der zugehörigen Person und nimmt die Sicherheitsmerkmale in Augenschein. Nach dieser Prüfung kann in diesem Beispiel der Kundenberater die Namen, das Geburtsdatum und die Adressdaten vom Ausweis im Rahmen seiner Geschäftstätigkeit und unter den in diesem Zusammenhang stehenden datenschutzrechtlichen Rahmenbedingungen verwenden (z.B. für die Eröffnung eines Bankkontos für den Kunden).

Das Online-Ausweisen ist dem dargestellten Prinzip aus der analogen Welt entsprechend als elektronischer Identitätsnachweis umgesetzt worden. Da die Sichtprüfung bei einem Diensteangebot auf einem Webserver nicht möglich ist[2], mussten zusätzliche Funktionen in und an den Personalausweis angebracht werden. Es handelt sich um einen berührungslos lesbaren Computer-Chip im Ausweis und einen zertifizierten eID-Server im Internet. Bei jedem Auslesevorgang wird ein Dreieck zwischen diesen beiden Elementen und dem Webserver des Diensteanbieters gebildet. Der eID-Server steht unter hoheitlicher Kontrolle des Staates und trifft Aussagen darüber, ob die Verwendung von Ausweisdaten in der jeweiligen Situation grundsätzlich erlaubt ist und ob der Ausweis gültig ist. Die Sicherheit wird insgesamt durch das Zusammenspiel mit der staatlichen Berechtigung (Berechtigungszertifkat), dem eID-Server und der Karte geschaffen. Der Ausweisinhaber muss das Auslesen durch Eingabe seiner PIN freigeben. Ist alles ok, erhält der Diensteanbieter die Daten aus dem Ausweis, um Sie wie im obigen Beispiel zu verwenden. Die direkte Verbindung des IT-Systems des Diensteanbieters mit dem eID-Server ist dabei der Garant dafür, dass es sich um echte Ausweisdaten handelt. Jegliche Manipulation des geschlossenen Dreiecks wird von der im Einsatz befindlichen Technik erkannt. So kann kein technologischer[3] Missbrauch des elektronischen Identitätsnachweises stattfinden.

---

[2] Mit VideoIdent-Verfahren oder Nect Selfie-Ident werden die Instrumente der analogen Sichtprüfung benutzt. Damit zählen derartige Verfahren nicht als elektronischer Identitätsnachweis.

[3] Ein Missbrauch aufgrund Fehlverhalten der Nutzer wird bei der technischen Betrachtung nicht behandelt.

buergerservice.org



Was ist die Selbstauskunft beim Online-Ausweisen?

Auch hier wieder der Vergleich mit der analogen Welt. Selbstauskunft ist mit der Eigenprüfung vergleichbar. Der Ausweisinhaber schaut auf seinen Personalausweis, prüft die Sicherheitsmerkmale und kann die aufgedruckten Daten ablesen und auf Richtigkeit prüfen. Die meisten Menschen machen eine derartige Kontrolle nachdem sie einen neuen Personalausweis von ihrem Meldeamt erhalten haben. Es handelt sich in diesem Fall also nur um den Inhaber des Ausweises, der seinen Ausweis selbst prüft. Keine weitere Person ist bei dieser Eigenprüfung beteiligt. Datenschutzrechtlich ist für den Ausweisinhaber keinerlei Relevanz gegeben, da der Ausweisinhaber nur seine eigenen Daten sieht.

Bei der Selbstauskunft (online) wird wieder die gleiche Technik, wie beim Online-Ausweisen dargestellt, als Ersatz für die online nicht einsehbaren physischen Sicherheitsmerkmale beim Personalausweis genutzt. Auch hier wird wieder ein Dreieck zwischen dem Ausweis, dem „hoheitlichen“ eID-Server und dem IT-Systems des Diensteanbieters für die Selbstauskunft geschlossen. Als Besonderheit ist hierbei zu werten, dass das IT-System des Diensteanbieters keinem Dritten zur weiteren Verarbeitung personenbezogener Daten gehört, sondern dieses nur die ausgelesenen Daten an den Ausweisinhaber zurücksendet und danach sofort wieder löscht. Damit ist der Vorgang datenschutzrechtlich wie bei der analogen Eigenprüfung anzusehen..

Was ist das Vertrauensniveau?

Das Vertrauensniveau gibt an, wie sicher bzw. wie vertrauenswürdig übermittelte Daten sind[4].

Das Vertrauensniveau für Identitätsdaten kann eine von drei Stufen annehmen:

- Ein "niedriges" Vertrauensniveau mindert die Gefahr des Identitätsdiebstahls (Beispiel: Facebook-Account).
- Ein "substanzielles" Vertrauensniveau reduziert die Gefahr des Identitätsmissbrauchs erheblich (Beispiel: Homebanking-Account).
- Das Vertrauensniveau "hoch" erfordert eine Verhinderung des Identitätsdiebstahls (nur die Online-Ausweisfunktion erfüllt dieses Niveau)

[4] Grundlegende Festlegungen der eIDAS-Verordnung: die Durchführungsverordnung (EU) 2015/1502 regelt die technischen Mindestanforderungen an die Vertrauensniveaus (in den Texten der Verordnung auch „Sicherheitsniveau“). Es existieren die Vertrauensniveaus: niedrig, substanziell und hoch (low, substantial, high). Die BSI TR-03107-1 überträgt und detailliert die Anforderungen der eIDAS-Verordnung.



Selbstschutz durch Selbstauskunft (SdS)

Motivation

Bei der Eigenprüfung des Sichtdokuments Personalausweis (analog) ist nur ein einziger Selbstschutz bekannt. Der Selbstschutz besteht darin, dass der Ausweisinhaber selbst seine Daten kontrolliert und fehlerhafte Daten feststellen kann. So schützt sich der Ausweisinhaber vor einem Verstoß gegen § 27 des Personalausweisgesetzes[5] .

Bei der Online-Ausweisfunktion Selbstauskunft kommt hingegen zusätzliche Technik auf einem Endgerät zum Einsatz, womit sich neben der Kontrolle korrekter Daten beim Online-Ausweisen zusätzliche Selbstschutzmaßnahmen im persönlichen Umfeld des Ausweisinhabers realisieren lassen.

buergerservice.org möchte mit Anwendungen für den persönlichen Bereich die Bevölkerung einladen, die Selbstauskunft für den Selbstschutz zu nutzen und so das Handling mit dem eigenen Personalausweis kennenzulernen und einzuüben. Durch die wiederkehrende Nutzung soll vor allem die PIN zum Personalausweis dauerhaft erlernt werden.

Einsatzfelder und Anwendungsmöglichkeiten

Anwendungen sind überall dort möglich, wo das Endgerät inkl. Diensteangebot zur Hoheit des Ausweisinhabers gezählt werden kann. Nur in dieser Situation kann neben dem Anspruch auf Selbstauskunft i.S.d. Art 15 DSGVO zusätzlich ein tatsächlicher Nutzen durch die Selbstauskunft generiert werden. Zwei Aspekte schränken weitergehende mögliche Einsatzfelder auf dieses konkrete Umfeld ein:

1. Die datenschutzrechtlichen Aspekte zur Selbstauskunft erlauben nur dem Ausweisinhaber seine Daten einzusehen. Kein Dritter darf die Daten weiterverwenden.
2. Die ausgelesenen Daten verlieren das Vertrauensniveau hoch in dem Moment, wo sie aus dem eingangs beschriebenen Dreieck (s. Was ist Online-Ausweisen?) am Endgerät des Ausweisinhabers herausgenommen werden. Danach haben diese Daten jegliches Vertrauensniveau verloren[6].

Unter diesen Rahmenbedingungen wurden von buergerservice.org erste Pilotanwendungen entwickelt (s.u.). Alle Anwendungen nutzen eine einfache Library. Sämtliche Quellcodes sind auf Github veröffentlicht. Interessierte Programmierer können so relativ einfach die Selbstauskunft in weitere Anwendungen für den persönlichen Bereich des Ausweisinhabers verfügbar machen.

---

[5] § 27 Pflichten des Ausweisinhabers: Der Ausweisinhaber ist verpflichtet, der Personalausweisbehörde unverzüglich den Ausweis vorzulegen, wenn eine Eintragung unrichtig ist

[6] Mit sehr aufwändiger Technik (z.B. OPTIMOS 2) könnte man ein Vertrauensniveau an dieser Stelle bewahren, jedoch soll der erforderliche Aufwand für SdS nicht weiter betrachtet werden.

buergerservice.org

Pilotanwendungen - Einleitung

Die AusweisApp2 verfügt über die Funktion "Meine Daten einsehen". Mit dieser Funktion können die auf dem Deutschen Personalausweis für deutsche Staatsangehörige, dem elektronischen Aufenthaltstitel für EU-Ausländer oder der eID-Karte für Unionsbürger gespeicherten Daten ausgelesen und angezeigt werden. Hierbei handelt es sich um die sogenannten Selbstauskunft. Diese Funktion steht allen Ausweisinhabern kostenfrei über die AusweisApp2 zur Verfügung und hat sich deshalb für die Pilotanwendungen bestens geeignet. Die AusweisApp2 steht als Open Source Quellcode bereit. Mit dem SDK zur AusweisApp2 ist auch eine Programmierschnittstelle (API) mit festgelegtem Protokoll (Commands/Messages) vorhanden.

Pilotanwendung 1: KeePerso für KeePass2

SdS Lane
Selbstschutz durch Selbstauskunft mit Online-Ausweis

KeePass

Konzept

Der Passwortmanager KeePass2 soll durch die Selbstauskunft eine zusätzliche Absicherung erhalten. Beim Passwortmanager wurde für das Pilotvorhaben das kostenfreie Programm KeePass2 ausgewählt, da hier neben der hohen Verbreitung eine einfache Einbindung von Softwarekomponenten über Plugin-Technologien gegeben ist.

Umsetzung

Die Durchführung bestand in der Entwicklung eines Plugins für den Passwortmanager KeePass2.

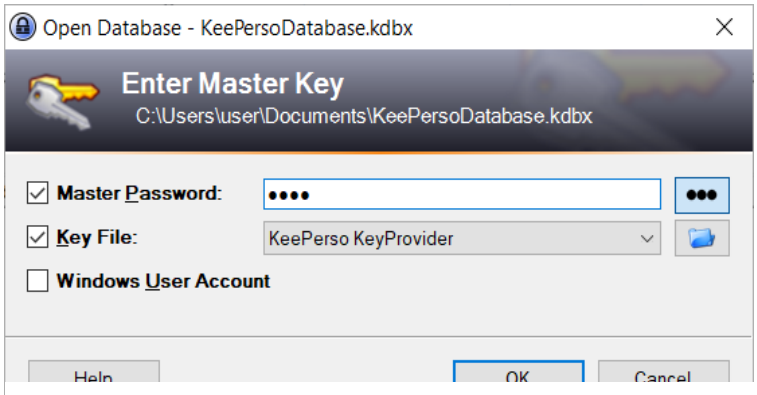


Abbildung 1: Auswahl KeePerso KeyProvider



Das Plugin für KeePass2 kommt bei folgenden Situationen innerhalb der KeePass2-Anwendung zum Einsatz:

- beim Anlegen einer neuen Passwort-Datenbank und
- beim späteren Aufrufen dieser Datenbank mit KeePass2

In beiden Situationen werden folgende Aufgaben von KeePerso durchgeführt:

- Hinweis auf die Voraussetzungen (AusweisApp2 gestartet, Kartenleser angeschlossen und Ausweis aufgelegt)
- Abfrage der PIN (nur bei Basiskartenlesegeräten durch das Plugin, bei Kartenlesegeräten mit eigener Tastatur erfolgt die Eingabe am Kartenleser)
- Übergabe der Befehlsfolge an die AusweisApp2
- Überschreiben der im Programmspeicher befindlichen PIN mit einer Zufallszahl zur Missbrauchsvermeidung (nur bei Basiskartenlesegeräten, s.o.)
- Hinweisfenster auf den Auslesevorgang einblenden, bis die Selbstauskunft abgeschlossen wurde (Anzeige der Informationen nach §18 (4) PAuswG vulgo das Berechtigungszertifikat und die zu übermittelnden Daten)
- Übernahme bestimmter Ausweisdaten von der AusweisApp2. Es werden diejenigen Daten verwendet, welche relativ selten eine Änderung erfahren (Vorname, Nachname oder wenn vorh. Geburtsname, Geburtsdatum und Geburtsort)
- Bilden eines Hash-Wertes aus den verwendeten Ausweisdaten
- Löschen der im Programmspeicher befindlichen Ausweisdaten (die für die Ausweisdaten im Programmcode verwendeten Variablen werden mit Zufallszahlen überschrieben). D. h. sämtliche ausgelesenen Ausweisdaten sind an dieser Stelle im Programmablauf nicht mehr vorhanden und können auch nicht wieder hergestellt werden
- Übergabe des Hash-Wertes als zusätzlichen Schlüssel an die Anwendung KeePass2

Nutzen

Für den Nutzer entsteht eine höhere Sicherheit für die Passwortdatei, da jetzt zum Öffnen der Datei neben dem Masterpasswort von KeePass2 zusätzlich der Hash-Wert aus den Ausweisdaten des Personalausweises zur Verschlüsselung zum Einsatz gebracht wird.

Auf einem nicht kompromittierten Rechner erreicht man damit einen besonders benutzerfreundlichen und trotzdem hohen Schutz für seine Passwortdatei. Der gestaltete Hash-Wert ist bereits ein sehr kompliziertes Passwort, so dass beim Masterpasswort ein einfaches und leicht zu merkendes Passwort ausreicht. So ist es durch KeePerso auch möglich, die KeePass2-Datenbank mit einem relativ einfachen Masterpasswort in der Cloud abzulegen.

buergerservice.org



Die Notwendigkeit der Verwendung des eigenen Personalausweises schütz davor, dass andere Personen bei Kenntnis des Masterpasswortes Zugang erhalten.

Bei einem kompromittierten Rechner ist hingegen der Schutz durch KeePerso nur in geringem Umfang erhöht (s. Risiken).

Risiken und Gegenmaßnahmen

Veränderung der Daten auf dem Ausweis oder beim Selbstauskunftsdienst

Eine Veränderung der verwendeten Daten auf dem Personalausweis (Vorname, Nachname oder wenn vorh. Geburtsname, Geburtsdatum und Geburtsort) bedeutet, dass der Zugang zur Passwortdatei nicht mehr direkt mit dem Personalausweis möglich ist. Ebenso können Ausfälle, Änderungen oder Anpassungen am Selbstauskunftsdienst dazu führen, dass die KeePass2-Datenbank nicht mehr entsperrt werden kann. Für diese Fälle ist ein Backup ohne die Zusatzverschlüsselung mit KeePerso vorzuhalten.

Kompromittierter Rechner

Auf einem kompromittierten Rechner sind umfangreiche Risiken gegeben. An dieser Stelle soll nur der Bezug zu KeePerso erläutert werden.

Die Verwendung von Basiskartenlesegeräten birgt die Gefahr, dass auf kompromittierten Rechnern die PIN zum Ausweis einem Angreifer in die Hände fallen kann. Bei Verwendung eines Kartenlesegerätes mit eigenem Tastaturfeld ist dieses Risiko nicht gegeben.

Ein Angreifer kann nach „Übernahme“ eines Rechners die Passwortdatei, das zugehörige Masterpasswort und den Hashwert von KeePerso stehlen und kann sich so Zugang zu den Passwörtern verschaffen.

Bei einem kompromittierten Rechner ist eine Neuinstallation des Betriebssystems die beste Lösung.

buergerservice.org

Pilotanwendung 2: PersonalausweisCredentialProvider (Win 10)

SdS Lane
Selbstschutz durch Selbstauskunft mit Online-Ausweis
Windows Login

Konzept

Der Login auf einem Windows-10 Rechner soll durch die Selbstauskunft einen hohen Zugangsschutz erhalten.

Das von Microsoft vorgesehene Konstrukt „Custom credential provider für Windows 10“ erlaubt die Verwendung von kundeneigenen Zugangsverfahren zum Windows 10 -Rechner.

Umsetzung

Die Durchführung bestand in der Entwicklung einer DLL-Datei für das Windows 10 Betriebssystem.

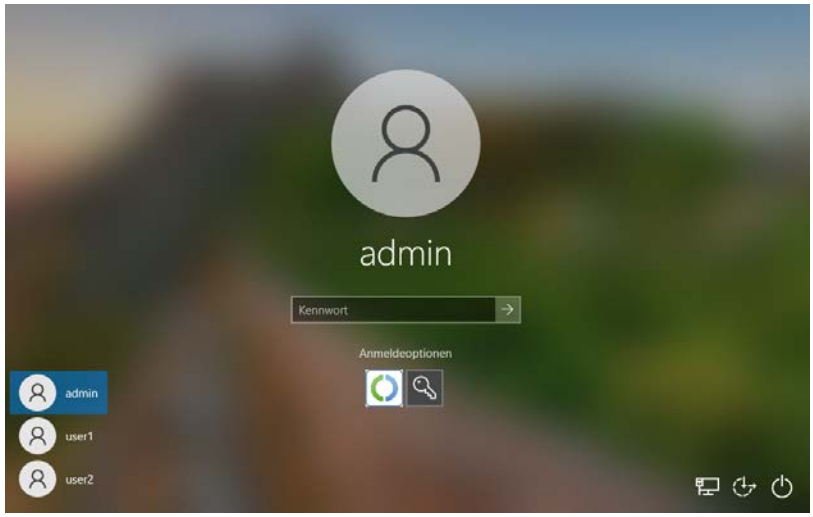


Abbildung 2: Login-Seite von Windows 10

Der PersonalausweisCredentialProvider kommt während der Anmeldung am Windows 10-PC zum Einsatz:

Es werden folgende Aufgaben von PersonalausweisCredentialProvider durchgeführt:

- Starten der AusweisApp2 im Hintergrund, bereits vor der Anmeldung am Windows 10-PC



- Hinweis auf die Voraussetzungen (Internetverbindung gegeben, AusweisApp2 gestartet, Kartenleser angeschlossen und Ausweis aufgelegt)
- Abfrage der PIN (nur bei Basiskartenlesegeräten durch das Plugin, bei Kartenlesegeräten mit eigener Tastatur erfolgt die Eingabe am Kartenleser)
- Übergabe der Befehlsfolge an die AusweisApp2
- Überschreiben der im Programmspeicher befindlichen PIN mit einer Zufallszahl zur Missbrauchsvermeidung (nur bei Basiskartenlesegeräten, s.o.)
- Hinweisfenster auf den Auslesevorgang einblenden, bis die Selbstauskunft abgeschlossen wurde (Anzeige der Informationen nach §18 (4) PAuswG vulgo das Berechtigungszertifikat und die zu übermittelnden Daten)
- Übernahme bestimmter Ausweisdaten von der AusweisApp2. Es werden diejenigen Daten verwendet, welche relativ selten eine Änderung erfahren (Vorname, Nachname oder wenn vorh. Geburtsname, Geburtsdatum und Geburtsort)
- Bilden eines Hash-Wertes aus den verwendeten Ausweisdaten
- Löschen der im Programmspeicher befindlichen Ausweisdaten (die für die Ausweisdaten im Programmcode verendeten Variablen werden mit Zufallszahlen überschrieben). D. h. sämtliche ausgelesenen Ausweisdaten sind an dieser Stelle im Programmablauf nicht mehr vorhanden und können auch nicht wieder hergestellt werden
- Verwendung des Hash-Wertes als Schlüssel für den Zugang zum Windows 10-PC

Nutzen

Für den Nutzer entsteht eine höhere Sicherheit für seinen Windows-PC, da jetzt für den Zugang zum PC die Selbstauskunft mit seinem Personalausweis zum Einsatz gebracht wird. Das System kann vom Administrator so konfiguriert werden, dass der Zugang für einen User nur mit dem Personalausweis erfolgen kann.

Auf einem nicht kompromittierten Rechner erreicht man damit einen besonders benutzerfreundlichen und trotzdem hohen Schutz für seine PC.

Die Notwendigkeit der Verwendung des eigenen Personalausweises schütz davor, dass andere Personen Zugang zum PC, z.B. durch Ausspähen von Benutzername und Passwort, erhalten könnten.

Risiken und Gegenmaßnahmen

Veränderung der Daten auf dem Ausweis oder beim Selbstauskunftsdienst

Eine Veränderung der verwendeten Daten auf dem Personalausweis (Vorname, Nachname oder wenn vorh. Geburtsname, Geburtsdatum, Geburtsort) bedeutet,



dass der Zugang zum Windows-Rechner nicht mehr direkt mit dem Personalausweis möglich ist. Ebenso können Ausfälle, Änderungen oder Anpassungen am Selbstauskunftsdienst dazu führen, dass der Zugang zum PC für den jeweiligen Benutzer nicht mehr möglich ist. Für diese Fälle muss der Administrator des PCs über seinen Zugang einen neuen Personalausweis für den betreffenden Benutzer einrichten oder vorübergehend eine andere Zugangsart aktivieren..

Kompromittierter Rechner

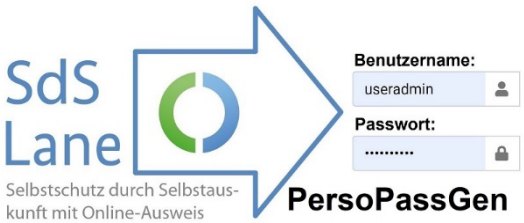
Auf einem kompromittierten Rechner sind umfangreiche Risiken gegeben. An dieser Stelle soll nur der Bezug zu PersonalausweisCredentialProvider erläutert werden.

Die Verwendung von Basiskartenlesegeräten birgt die Gefahr, dass auf kompromittierten Rechnern die PIN zum Ausweis einem Angreifer in die Hände fallen kann. Bei Verwendung eines Kartenlesegerätes mit eigenem Tastaturfeld ist dieses Risiko nicht gegeben.

Bei einem kompromittierten Rechner ist eine Neuinstallation des Betriebssystems die beste Lösung.

buergerservice.org

Pilotanwendung 3: eID-Passwortgenerator PersoPassGen



Konzept

Mit Hilfe der Selbstauskunft und einem Account-Namen eines Zugangs sollen immer wieder die gleichen vielstelligen Passwörter mit mehr als 60 Zeichen generiert werden. Dieses neuartige Konzept ermöglicht es, dass Passwörter nicht mehr auf dem eigenen Rechner abgespeichert oder auf Papier notiert werden müssen.

Umsetzung

Die Durchführung bestand in der Entwicklung einer plattformunabhängigen Anwendung für Windows und Linux.

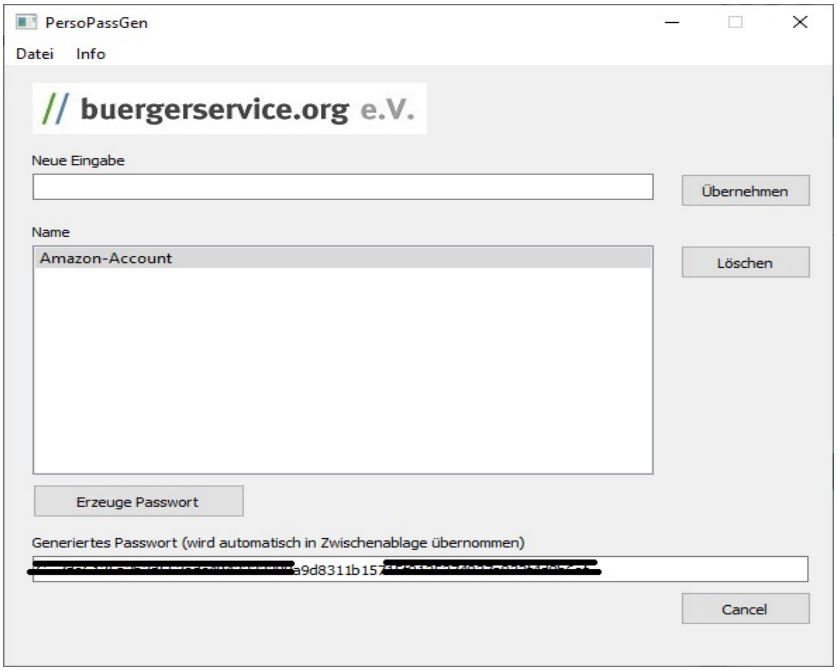


Abbildung 3: Anwendung PersoPassGen

PersoPassGen wird als eigenständige Anwendung gestartet:

Folgende Aufgaben werden von PersoPassGen durchgeführt:

- Hinweis auf die Voraussetzungen (AusweisApp2 gestartet, Kartenleser angeschlossen und Ausweis aufgelegt)



- Abfrage der PIN (nur bei Basiskartenlesegeräten durch das Plugin, bei Kartenlesegeräten mit eigener Tastatur erfolgt die Eingabe am Kartenleser)
- Übergabe der Befehlsfolge an die AusweisApp2
- Überschreiben der im Programmspeicher befindlichen PIN mit einer Zufallszahl zur Missbrauchsvermeidung (nur bei Basiskartenlesegeräten, s.o.)
- Hinweisfenster auf den Auslesevorgang einblenden, bis die Selbstauskunft abgeschlossen wurde (Anzeige der Informationen nach §18 (4) PAuswG vulgo das Berechtigungszertifikat und die zu übermittelnden Daten)
- Übernahme bestimmter Ausweisdaten von der AusweisApp2. Es werden diejenigen Daten verwendet, welche relativ selten eine Änderung erfahren (Vorname, Nachname oder wenn vorh. Geburtsname, Geburtsdatum und Geburtsort)
- Bilden eines Hash-Wertes aus den verwendeten Ausweisdaten und dem Namen des in der Anwendung hinterlegten Accounts
- Löschen der im Programmspeicher befindlichen Ausweisdaten (die für die Ausweisdaten im Programmcode verwendeten Variablen werden mit Zufallszahlen überschrieben). D. h. sämtliche ausgelesenen Ausweisdaten sind an dieser Stelle im Programmablauf nicht mehr vorhanden und können auch nicht wieder hergestellt werden
- Übergabe des Hash-Wertes als Passwort in die Zwischenablage

Nutzen

Für den Nutzer entsteht eine höhere Sicherheit für den Zugang zu Systemen mit Passwortschutz. Der Nutzer kennt sein 6-stelliges Zahlenpasswort für den Personalausweis und kann damit immer wiederkehrend ein über 60 Zeichen langes Passwort generieren.

Über die Windows Zwischenablage wird das Passwort der jeweiligen Anwendung übergeben. Das Passwort selbst wird dabei nicht dauerhaft gespeichert sondern immer dann generiert, wenn das Passwort zum Einsatz gebracht werden soll.

Risiken und Gegenmaßnahmen

Veränderung der Daten auf dem Ausweis oder beim Selbstauskunftsdienst

Eine Veränderung der verwendeten Daten auf dem Personalausweis (Vorname, Nachname oder wenn vorh. Geburtsname, Geburtsdatum und Geburtsort) bedeutet, dass die Passwörter nicht mehr generiert werden können. Ebenso können Ausfälle, Änderungen oder Anpassungen am Selbstauskunftsdienst dazu führen, dass die Passwörter nicht mehr generiert werden können. Für diese Fälle muss der Nutzer die tatsächlich wichtigen Passwörter, welche keine eigene Rücksetzmöglichkeit zur Verfügung stellen, auf einem externen Medium abspeichern oder ausdrucken.



Kompromittierter Rechner

Auf einem kompromittierten Rechner sind umfangreiche Risiken gegeben. An dieser Stelle soll nur der Bezug zu PersoPassGen erläutert werden.

Die Verwendung von Basiskartenlesegeräten birgt die Gefahr, dass auf kompromittierten Rechnern die PIN zum Ausweis einem Angreifer in die Hände fallen kann. Bei Verwendung eines Kartenlesegerätes mit eigenem Tastaturfeld ist dieses Risiko nicht gegeben.

Bei einem kompromittierten Rechner ist eine Neuinstallation des Betriebssystems die beste Lösung.

buergerservice.org

Pilotanwendung 4:
eID-Türöffner MyPersoDoor

SdS Lane
Selbstschutz durch Selbstauskunft mit Online-Ausweis
MyPersoDoor

Konzept

Bei diesem Konzept sollte Programmcode für einen Raspberry PI 4 entwickelt werden. Der Raspberry steuert nach einer erfolgreich durchgeführten Selbstauskunft über ein Schaltrelais einen Türöffner an.

Umsetzung

Die konkrete Umsetzung sieht vor, dass der Hauseigentümer den Hotspot seines Smartphones als WLAN-Access-Point für den Raspberry zur Verfügung stellt. Über diese WLAN-Verbindung wird im Anschluss das eigene Smartphone als externer Kartenleser zur AusweisApp2 auf dem Raspberry gekoppelt. Dabei wird voreingestellt, dass immer die Tastatur des Smartphones zur PIN-Eingabe verwendet werden soll.

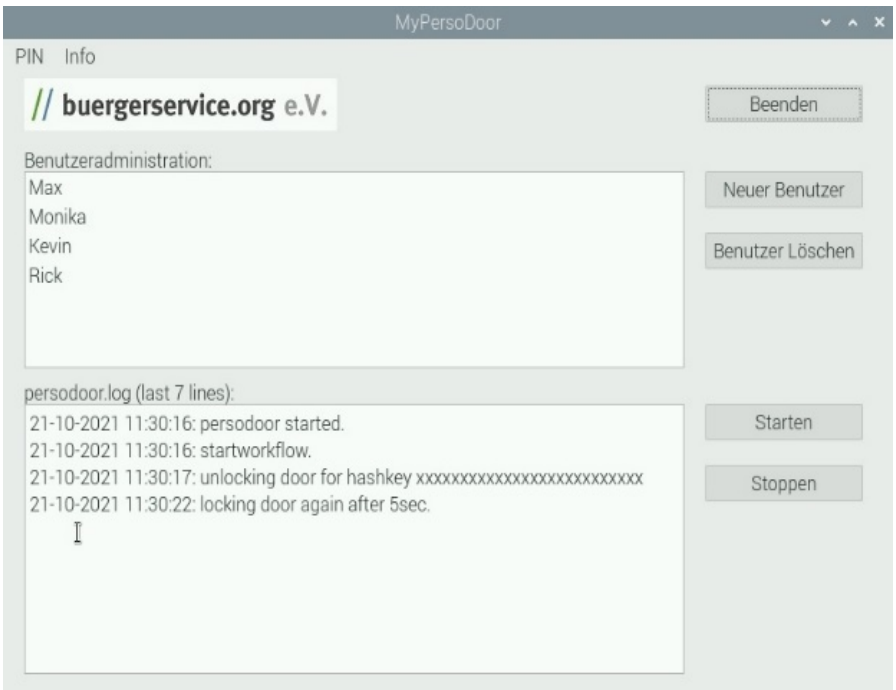


Abbildung 4: Anwendung MyPersoDoor



Die Durchführung bestand in der Entwicklung des entsprechenden Programmcodes als Endlosschleife mit einer Wartezeit von 15 Sekunden nach einem Öffnungsvorgang. In Ergänzung zu dieser Endlosschleife wurde eine Bedienoberfläche entwickelt, mit welcher neue Benutzer (z.B. Familienmitglieder) angelegt, bzw. veraltete Benutzer gelöscht werden können.

MyPersoDoor wird als eigenständige Anwendung gestartet:

Folgende Aufgaben werden von MyPersoDoor durchgeführt:

- Hinweis auf die Voraussetzungen (AusweisApp2 gestartet, Kartenleser angeschlossen und Ausweis aufgelegt)
- Übergabe der Befehlsfolge an die AusweisApp2
- Abfrage der PIN am Smartphone (es ist auch eine Variante mit einem Komfortkartenlesegerät neben der Haustüre umsetzbar, einfacher für die Umsetzung ist jedoch die Verwendung des eigenen Smartphones vor der Haustüre)
- Überschreiben der im Programmspeicher befindlichen PIN mit einer Zufallszahl zur Missbrauchsvermeidung (hat bei MyPErsoDoor keine Relevanz, nur bei Basiskartenlesegeräten von Bedeutung, s.o.)
- Übernahme bestimmter Ausweisdaten von der AusweisApp2. Es werden diejenigen Daten verwendet, welche relativ selten eine Änderung erfahren (Vorname, Nachname oder wenn vorh. Geburtsname, Geburtsdatum und Geburtsort)
- Bilden eines Hash-Wertes aus den verwendeten Ausweisdaten
- Löschen der im Programmspeicher befindlichen Ausweisdaten (die für die Ausweisdaten im Programmcode verwendeten Variablen werden mit Zufallszahlen überschrieben). D. h. sämtliche ausgelesenen Ausweisdaten sind an dieser Stelle im Programmablauf nicht mehr vorhanden und können auch nicht wieder hergestellt werden
- Vergleich des Hashwertes mit den zuvor hinterlegten Hashwerten der zugangsberechtigten Personen
- Bei positivem Vergleich wird das Relais für den Türöffner für 5 Sekunden angesteuert.

Nutzen

Für den Nutzer entsteht eine Möglichkeit, seine eigene Haustüre ohne physischen Schlüssel zu öffnen. Das System kann auch auf andere Bereiche verlagert werden (z.B. Öffnen eines Garagentores oder einer Schranke)

buergerservice.org

Demonstrator

Für Vorführungen und Schulungen wurde ein Demonstrator hergestellt.

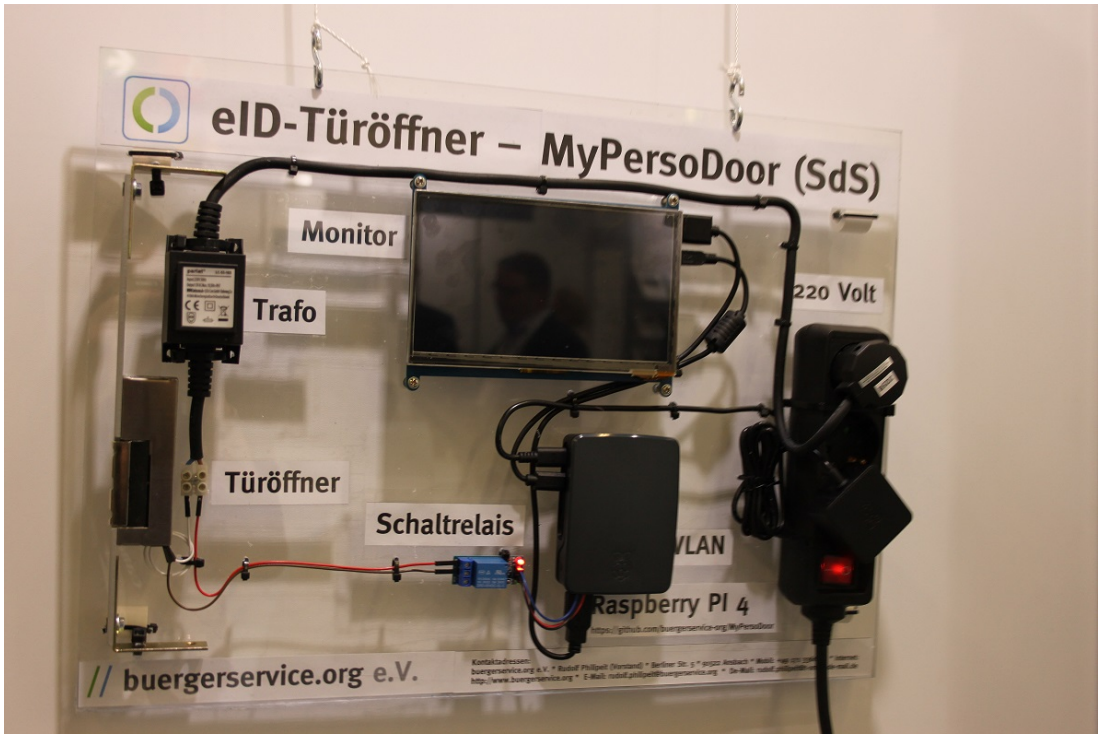


Abbildung 5: Demonstrator MyPersoDoor

Risiken und Gegenmaßnahmen

Veränderung der Daten auf dem Ausweis oder beim Selbstauskunftsdienst

Eine Veränderung der verwendeten Daten auf dem Personalausweis (Vorname, Nachname oder wenn vorh. Geburtsname, Geburtsdatum und Geburtsort) bedeutet, dass die Passwörter nicht mehr generiert werden können. Ebenso können Ausfälle, Änderungen oder Anpassungen am Selbstauskunftsdienst dazu führen, dass die Hashwerte nicht mehr generiert werden können. Für diese Fälle muss der Nutzer einen alternativen Zugangsmechanismus vorhalten.

Kompromittierter Raspberry

Auf einem kompromittierten Raspberry sind umfangreiche Risiken gegeben. An dieser Stelle soll nur der Bezug zu MyPErsoDoor erläutert werden.

Das hier dargestellte Szenario verwendet die Hotspot-Funktion des Smartphones eines Zugangsberechtigten. D. h. der Raspberry ist im Wartemodus nicht mit dem Internet verbunden. Erst wenn der berechtigte Benutzer in die WLAN-Reichweite kommt und den Hotspot auf seinem Smartphone einschaltet, erhält der Raspberry für einen kurzen Zeitraum eine Internetverbindung. Damit ist die Gefahr eines Angriffs



aus dem Internet nahezu ausgeschlossen. Der verwendete Raspberry könnte nur noch kompromittiert werden, wenn jemand sich physischen Zugang zum Gerät verschafft.

Bei einem kompromittierten Rechner ist eine Neuinstallation des Betriebssystems die beste Lösung.

buergerservice.org



Faktencheck

Recht

Welche datenschutzrechtlichen Belange sind zu berücksichtigen?

Es gibt aus Sicht von buergerservice.org keine Beschränkungen durch den Datenschutz. Die Datenschutzaspekte zur Selbstauskunft sind klar geregelt und erlauben dem Ausweisinhaber seine Daten aus dem Personalausweis auf den eigenen Rechner (in der eigenen Hoheit) zu holen.

Konkret: ein „über die Schulter schauen“ durch Dritte ist bei der analogen Eigenprüfung nicht erlaubt (sonst wäre es bereits eine Sichtprüfung der Identitätsdaten für Dritte) und in der elektronischen Variante Selbstauskunft ist es ebenfalls verboten.

Sicherheit

Wie hoch ist das Vertrauensniveau einzustufen?

Die Daten werden zwar bei der Selbstauskunft mit dem Vertrauensniveau hoch auf dem PC des Nutzers angeliefert, verlieren dann aber jegliches Vertrauensniveau. Die Gründe hierzu sind:

- der Quellcode des Plugin ist öffentlich zugänglich. Die Bildung des Hash-Wertes ist nachvollziehbar
- das Plugin kann auf einem kompromittierten Rechner leicht ausgetauscht oder manipuliert werden
- die Verwendung der Daten zum Ausweisinhaber für die Bildung des Hash-Wertes können leicht, auch ohne Personalausweis zu verwenden, von „Angreifern“ ermittelt werden.

Trotz des verlorengegangenen hohen Vertrauensniveaus wird auch in den beschriebenen Fällen die Sicherheit deutlich erhöht, da ein Angreifer mehrere Hürden überwinden muss.

Allgemein

Kann man die Selbstauskunft anstelle des „normalen“ Online-Ausweisens einsetzen?

Technisch könnte man die ausgelesenen Ausweisdaten nach der Selbstauskunft in eine Anwendung bringen, jedoch ist dieses Verfahren nur ohne jegliches Vertrauensniveau machbar (s. Sicherheit-Vertrauensniveau). Damit ist der rechtsgültige elektronische Identitätsnachweis nicht möglich.

Zum besseren Verständnis sei hier auf die eingangs dargestellten grundsätzlichen Erläuterungen verwiesen. Die Selbstauskunft bedeutet, dass der Ausweisinhaber selbst die Daten auf seinem Ausweis kontrolliert und diese im Rahmen seiner Hoheit verwendet. Solange er seine Daten für seine eigenen Anwendungen verwendet, wird er keinen Missbrauch betreiben. Käme ein Dritter mit hinzu, wäre dem Missbrauch Tür und Tor geöffnet.



Für die analoge Welt wäre das Szenario so als würde er die Daten auf seinem Ausweis lesen und an anderer Stelle in ein Formular eingeben. Will der Ausweisinhaber Missbrauch betreiben, so könnte er falsche Daten in das Formular übernehmen. Beim normalen Online-Ausweisen ist dieser Angriffsvektor nicht gegeben, da der „hoheitliche“ eID-Server die Weitergabe korrekter Ausweisdaten garantiert.

buergerservice.org



Darstellung der Beteiligten und Ansprechpartner

Bundesministerium des Innern, für Bau und Heimat

Die Aufgaben des Bundesministeriums des Innern, für Bau und Heimat (BMI) sind ebenso vielfältig wie verantwortungsvoll. Das Spektrum reicht von der Rolle als Hüter der Verfassung und Förderer des gesellschaftlichen Zusammenhalts über die Integration, Sportförderung des Bundes und die Informationstechnik bis hin zu den Sicherheitsaufgaben. Als "Verfassungs- und Kommunalministerium" ist das Bundesinnenministerium für die Modernisierung von Staat und Verwaltung zuständig. Aber auch für Kernfragen unserer staatlichen und föderalen Ordnung, wie beispielsweise das Wahlrecht. Grundlage unseres politischen wie gesellschaftlichen Miteinanders bildet die freiheitlich-demokratische Grundordnung. Sie muss von den Menschen vor Ort jeden Tag mit Leben erfüllt werden. Deswegen haben das Ehrenamt und die politische Bildung einen festen Platz im Aufgabenspektrum des Hauses. Um alle diese Aufgaben zum Wohle der Bürgerinnen und Bürger erfüllen zu können, arbeiten in drei Dienstsitzen in Berlin und Bonn mehr als 2.100 Mitarbeiterinnen und Mitarbeiter.

Aufgabenstellung bzgl. der Online-Ausweisfunktion Selbstauskunft:
Das BMI ist Zuständig für den Deutschen Personalausweis, den elektronischen Aufenthaltstitel und die eID-Karte für Unionsbürger.

Kontakt:

Bundesministerium des Innern, für Bau und Heimat

Alt-Moabit 140 in 10557 Berlin

Bundesverwaltungsamt

Das Bundesverwaltungsamt (BVA) ist eine Bundesoberbehörde im Geschäftsbereich des Bundesministeriums des Innern, für Bau und Heimat. Es beschäftigt derzeit (Anfang des Jahre 2021) rund 6.000 Mitarbeiterinnen und Mitarbeiter. Als Partner von Bürgern, Behörden, Unternehmen und Vereinen nimmt das BVA mehr als 150 Aufgaben wahr. An der Spitze des Hauses stehen der Präsident, die Vizepräsidentin und der Vizepräsident.

Aufgabenstellung bzgl. der Online-Ausweisfunktion Selbstauskunft:
Zuständig für die Vergabe von Berechtigungszertifikaten zum Auslesen von Ausweisdaten.

Kontakt:

Bundesverwaltungsamt

Barbarastr. 1 in 50735 Köln



Bundesamt für Sicherheit in der Informationstechnik (BSI)

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) ist die Cyber-Sicherheitsbehörde des Bundes und Gestalter einer sicheren Digitalisierung in Deutschland.

Aufgabenstellung bzgl. der Online-Ausweisfunktion Selbstauskunft:
Erarbeitung von technischen Richtlinien zum Online-Ausweisen

Kontakt:

Bundesamt für Sicherheit in der Informationstechnik (BSI)

Godesberger Allee 185-189 in 53175 Bonn

Governikus GmbH & Co. KG

Governikus steht wie kein zweites Unternehmen in Deutschland für Sicherheit und Vertraulichkeit in der digitalen Kommunikation. Seit 1999 entwickeln und betreuen wir IT-Sicherheitslösungen, die zu den Standardanwendungen in den Bereichen E-Government und E-Justice zählen. Mit unseren Produkten decken wir dabei den gesamten Lebenszyklus der elektronischen Datenübermittlung ab: von der Authentisierung über den sicheren Datentransport bis zur Beweissicherung und langfristigen Beweiswerterhaltung elektronischer Daten.

Aufgabenstellung bzgl. der Online-Ausweisfunktion Selbstauskunft:
Entwicklung der AusweisApp2 im Auftrag des Bundes und Bereitstellung der Selbstauskunft

Kontakt:

Governikus GmbH & Co. KG

Hochschulring 4 in 28359 Bremen, Germany

buergerservice.org e.V.

Der Verein buergerservice.org verfolgt ausschließlich und unmittelbar gemeinnützige Zwecke im Sinne des Abschnitts „Steuerbegünstigte Zwecke“ der Abgabenordnung.

Zweck des Vereins ist die Förderung der Erziehung, Volks- und Berufsbildung einschließlich der Studentenhilfe zur Erlangung von Medienkompetenz für die Nutzung einer rechts- und datensicheren elektronischen Kommunikation, Identifizierung und Authentifizierung bei allen Bürgerinnen und Bürgern.

Der Satzungszweck wird verwirklicht insbesondere durch das Betreiben eines auf Wissensvermittlung basierenden Veränderungsmanagements zur Sensibilisierung von Bürgerinnen und Bürgern, Unternehmen, Institutionen und Behörden für die Akzeptanz und Nutzung von sicheren digitalen Kommunikationswegen (z.B. sichere



E-Mail) und Identifizierungs- und Authentifizierungsinstrumenten (z.B. die Online-Ausweisfunktion im Personalausweis).

Aufgabenstellung bzgl. der Online-Ausweisfunktion Selbstauskunft: Wissensvermittlung

Kontakt:

buergerservice.org e.V.

Berliner Str. 5 in 91522 Ansbach

buergerservice.org



Abkürzungsverzeichnis

BSI	Bundesamt für Sicherheit in der Informationstechnik)
BVA	Bundesverwaltungsamt
eID	elektronische Identität, in Deutschland: Personalausweis mit Online-Ausweisfunktion
SDI	Sichere digitale Identität
SdS	Selbstschutz durch Selbstauskunft
SSI	Self-Sovereign Identity

buergerservice.org



Anhang

Verlinkung zur Projektseite SdS:

https://www.buergerservice.org/projekte/sds/

buergerservice.org