DLR Projektträger Eerlir
Eingegangen am:
30. Sep. 2020
Eingangsnr.: 4972/B8

Sina Beckstein & Julian Rösner GbR
Weichselstraße 56
12045 Berlin

Richtlinie zum „Software-Sprint“

01IS19S29 – Identity-Stick

Schlussbericht

Zuwendungsempfänger: Sina Beckstein & Julian Rösner GbR

Name des Zuwendungsempfängers: Sina Beckstein, Julian Rösner

Das diesem Bericht zugrundeliegende Vorhaben wurde mit Mitteln des Bundesministeriums für Bildung und Forschung unter dem Förderkennzeichen **01IS19S29** gefördert. Die Verantwortung für den Inhalt dieser Veröffentlichung liegt beim Autor.

Kurze Darstellung der Aufgabenstellung und Motivation

Motivation

Wir haben von August bis Oktober 2019 an Tech4Germany teilgenommen, einem Programm zur Verwaltungsdigitalisierung unter der Schirmherrschaft des Bundeskanzleramts. Gemeinsam mit den Unternehmen Governikus und Yes wurde ein Prototyp zur Online-Authentifizierung mittels eines Sparkassen-Logins in ein Nutzerkonto implementiert. Dieser Prototyp zeigte zum ersten Mal die Möglichkeit, sich nicht nur mit der kaum genutzten eID für öffentliche Leistungen identifizieren zu können, sondern mit nutzerfreundlicheren Möglichkeiten. Während dieses Projekts entstand die Idee, eine bessere Autent- und Identifizierungslösung zu entwickeln, die insbesondere den Login für private und öffentliche Dienste vereinen und erleichtern soll. Eine solche ganzheitliche Lösung existiert bislang nicht.

Problemstellung

Eine Identität kann im Analogen nur ein Staat vergebe. Im Digitalen sind private Unternehmen zentral und nehmen diese Aufgabe durch ihre Login-Services wahr. Die Privatisierung der Identität birgt aber gesellschaftliche Risiken: Normen wie Privacy und Sicherheit treten bei profitorientierten Modellen häufig in den Hintergrund. Gerade wegen der bevorstehenden Digitalisierung von 575 öffentlichen Leistungen bis 2022 (OZG) stellt

sich damit die Frage, wie staatliche Lösungen die Identität der Bürgerinnen wahren können – um Abhängigkeiten von Privaten zu vermeiden und Bürgerinnen eine nachhaltige, nutzerfreundliche und faire öffentliche Alternative zu bieten.

Vorgehensweise

Die Vorgehensweise beinhaltete zwei wesentliche Phasen: Zum Einen wurde in einem ersten großen Arbeitspaket das Identity-Stick Konzept entwickelt und getestet. Dies beinhaltete unter anderem die Analyse des FIDO2-Standards, Stakeholder- und Expertinneninterviews und Partnerabsprachen, als auch das Testen von frühen Versionen mit potentiellen Endnutzerinnen. In der zweiten Phase lag der Fokus auf der technischen Entwicklung und visuellen Umsetzung des Prototyps.

Meilensteine

Die Entwicklung des prototypischen Identity-Sticks gliedert sich in die konzeptuelle Vorarbeit und prototypische Fertigstellung des Identity-Sticks:

AP 1: Entwicklung und Test des Identity-Stick Konzepts

AP 1.1.: Analyse des FIDO2-Standards: Überprüfen bisheriger Implementationen des Standards auf mögliche Anknüpfungspunkte für Identitätsattribute

AP 1.2.: Partnerabsprachen: Festlegen eines gemeinsamen Projektrahmens bzw. Austausch zu Herausforderungen und Verbesserungsmöglichkeiten mit Governikus und/oder der Bundesdruckerei [Für die Erweiterung des FIDO2-Protokolls wird mit der Governikus KG und ggf. mit der Bundesdruckerei kooperiert]

AP 1.3.: Nutzertests: Iterative Entwicklung eines ersten Prototyps für Nutzertests zur Usability eines solchen Identity-Sticks.

AP 1.4: Open Source Veröffentlichung des Konzepts und Nutzertestergebnisse

AP 2: Erstellung des Identity Sticks Prototyps

AP 2.1: Erweiterung des FIDO2-Standards um verifizierte Identitätsattribute: Anbindung der Identitätsfeststellung: Der Prototyp soll mittels der von Governikus bereitgestellten Architektur eine Identitätsfeststellung durch den neuen Personalausweis ermöglichen.

AP 2.2.: Umsetzung des WebAuthn- und CTAP-Standards

AP 2.3.: Open Source Veröffentlichung des Codes des Identity-Sticks

Beitrag des Projektes zu den Zielen der Förderinitative „Software-Sprint“

Zielgruppe

Der Identity-Stick kann für verschiedene Zielgruppen interessant sein: Für Unternehmen, für den öffentlichen Bereich (öffentliche Verwaltungen, Universitäten, Schulen), für Bürgerinnen im digitalen Raum (ca. 84% der Bevölkerung) oder Personen mit erhöhtem Sicherheitsbedarf (z.B. Journalistinnen, Patientinnen). Da unser Produkt sowohl den anonymen und passwortlosen Login für private Services und die sichere Identifikation für öffentliche Leistungen während der Antragstellung ermöglichen soll wird eine sehr breite Zielgruppe angesprochen. All diese unterschiedlichen Zielgruppen müssen sich entweder selbst oder ihre Kundinnen digital identifizieren und profitieren von sicheren und einfachen Lösungen dafür. Eine einheitliche Lösung könnte für sie alle von Vorteil sein (vgl. auch Abschnitt "Zielgruppe, Nutzen und mögliche Weiterentwicklung).

Bezüge zu den Themenfeldern und Zielen des Software Sprints

"Vertrauen" im Internet ist ganz wesentlich an die digitale Identität geknüpft. Ob jemandem oder etwas vertraut werden kann oder nicht hängt auch in erster Linie davon ab, ob sich diese Person oder Maschine glaubwürdig identifizieren kann. So können zum Beispiel Personen, die sich mit einem Schlüssel den nur sie besitzen vertraut werden und damit legitim Zugriff auf ein Konto gegeben oder ein Antrag gestellt werden. Im Vergleich zur analogen Welt ist es im Internet schwierig, Vertrauen herzustellen und einfacher, größere Angriffe auf vertrauenswürdige Instanzen durchzuführen. Im Internet gibt es auch die Besonderheit, dass Andere als "Identity Provider" an die Stelle von vertrauenswürdigen Instanzen treten, wie man es vom "Sign in mit Google" oder Facebook kennt: Sie bürgen als Identitätsprovider dafür, dass dem Konto vertraut werden kann. Die Privatisierung der Identität birgt aber auch gesellschaftliche Risiken: Normen wie Privacy und Sicherheit treten bei profitorientierten Modellen häufig in den Hintergrund. Gerade wegen der bevorstehenden Digitalisierung von 575 öffentlichen Leistungen bis 2022 (OZG) stellt sich damit die Frage, wie staatliche Lösungen die Identität der Bürgerinnen wahren können – um Abhängigkeiten von Privaten zu vermeiden und Bürgerinnen eine nachhaltige, nutzerfreundliche und vertrauenswürdige öffentliche Alternative zu bieten.

Ausführliche Darstellung der Ergebnisse

Erzielte Ergebnisse

- Identity Stick: Code für einen Solo Key mit der Möglichkeit des Ausweisens mittels der Identity Stick Extension
- Identity Stick Extension: Beschreibung des Protokolls für den Austausch von Identitätsattributen mittels CTAP (FID02)
- Interface Demos: User Interface Demos, die ein mögliches Interface für passwortlosen Login bzw. Ausweisen simulieren
- Identity Stick Server: Skript zum Testen der Funktionalität eines Identity Sticks
- FIDO Debugger: Webseite zum schnellen Testen der Daten, die von einem FIDO Token gesendet werden

- Zwei Tutorials für die Programmierung des Solo Hacker Sticks
- Signed Identity: Tool zum Erzeugen von signierten Identitätsattributen
- Identity-Stick.github.io: Code für unsere Webseite & eigene Projektwebseite unter der Domain
- Demovideo und eigene Demoanwendung auf identity-stick.github.io
- Blogpost für Prototypefund[1] und Veröffentlichung der Inhalte auf Webseite
- Expertinnengespräche und Konzepttests; Dokumentation der Vorgehensweise und Ideen

Erreichte Meilensteine

Die Meilensteine konnten alle erreicht werden. Durch die Verwendung des "Solo Sticks for Hackers" konnte auf eine Umsetzung des Webauthn/CTAP aufgebaut werden. Dadurch konnte die Erstellung und Prüfung von Konzepten stärker fokussiert werden. Lediglich das Arbeitspaket der Nutzertests konnte durch die Covid-19 Pandemie nicht im geplanten Umfang durchgeführt werden. Da es sich bei dem Identity-Stick um ein Hardware Produkt handelt, war es schwierig, ein Testsetting zu entwerfen, dass in einem Fernzugriff Kontext funktioniert.

Zielgruppe, Nutzen und mögliche Weiterentwicklungen

Für diese Zielgruppen könnte die Lösung interessant sein:

- **Für Unternehmen**
  Unternehmen haben häufig besonders sensible Daten. Dafür braucht es gesteigerte Sicherheitsvorkehrungen. Ein USB-Schlüssel kann Mitarbeitenden Zugang zu ihren Accounts geben und dabei Datensicherheit an erste Stelle setzen.

- **Für den öffentlichen Bereich**
  Schulen, das digitale Rathaus und vieles mehr: Wir brauchen Ausweise, um unsere Identität zu bestätigen. Mit einem digitalen Schlüssel können diese Prozesse vereinfacht werden.

- **Für Bürgerinnen**
  Sicherheit soll nicht nur für Kryptoexpert:innen gelten. Bürgerinnen sollen ihre digitale Identität einfach schützen und online Ausweisprozesse integrieren können. In einem Produkt.

- **Für Personen mit erhöhtem Sicherheitsbedarf**
  Manche Gruppen brauchen besonderen Schutz ihrer Daten und Accounts. Journalistinnen müssen ihre Quellen sichern oder Ärztinnen den Zugang zu Daten

[1] https://demoweek.prototypefund.de/projects/08-identity-stick.html

von Patientlinnen. Manche Personen legen besonderen Wert darauf sich online abzusichern.

Weitergehende Effekte der Open-Source-Stellung der Ergebnisse

Der Identity-Stick kann weiterentwickelt werden und für verschiedene Sicherheitsbedürfnisse angepasst werden, sodass bestimmte gewünschte Standards erfüllt werden. Außerdem ermöglicht dies auch den Einsatz für kleine Kreise, die ihn zum Ausweisen benutzen wollen. Dies könnten beispielsweise Vereine, andere Organisationen oder Einrichtungen wie Schulen sein.

Ideen für die Weiterentwicklung der Lösung und Pläne zu deren Umsetzung

Für ein vollumfängliches Produkt könnten weitere Entwicklungsschritte unternommen werden:

- **Personalisierung des Sticks und Signatur von Daten**
  Die Personalisierung des Sticks bzw. Signatur der Daten müsste in einem Produktionsumfeld von einer vertrauenswürdigen Instanz gesichert werden. Dafür käme eine staatliche Stelle wie bspw. die Bundesdruckerei in frage, die auch die technische Infrastruktur der eID betreut. Für eine einsatzfähige und sichere Version des Sticks müsste die Hardware von dieser Instanz hergestellt, die Maintenance gesichert und die entsprechenden individuellen Daten bei Erstausstellung für jede Bürgerin signiert werden. Es wäre nützlich, Bürgerinnen mit entsprechenden Informationen und Materialien über die Funktionsweise aufzuklären.

- **Weiterentwicklung des Protokolls**
  In der momentanen Version des Identity Stick Prototyps werden die Daten signiert auf dem Stick abgelegt und dann an Diensteanbieterinnen weiter gesendet. Dies verhindert zum Einen keine Replay-Attacken. Zum Anderen könnten die bestätigten Daten von Diensteanbieterinnen an Dritte weitergegeben werden. Daher müssten weitere Verbesserungen des Protokolls erfolgen. So sollte ein authentifizierter sichererer Kanal zwischen Stick und Diensteanbieterin aufgebaut werden über den Daten ausgetauscht werden könnten.

- **Erweiterter Hardwarespeicher und Features**
  Der Speicherplatz des Solo-Sticks ist limitiert, weshalb nur eine begrenzte Menge an Informationen darauf abgelegt werden kann. Mit der Produktion eigener Hardware könnte dieser Speicherplatz und damit die Funktionalität des Sticks erweitert werden. So könnte der Stick neben der sicheren (multi- und passwortlosen) Authentifizierung und Identifizierung auch einen sicheren Datenspeicher beinhalten, auf dem wichtige Dateien und Zertifikate abgelegt werden können, einen Passwortmanager beinhalten und vieles mehr.

- **Bekanntheitsgrad und Verbreitung von FID02**
  Der noch recht junge Standard wurde bisher von relativ wenigen Webseiten komplett implementiert. In Zukunft ist damit zu rechnen, dass mehr Diensteanbieterinnen die

Kurze Darstellung der Arbeiten, die zu keiner Lösung geführt haben

Arbeiten bzw. Lösungsansätze, die nicht weiter verfolgt wurden

Wir starteten mit der Frage "Wie lässt sich der Login mittels FIDO und das online Ausweisen verknüpfen?" Dazu hatten wir drei Konzeptrichtungen erstellt.

- **FIDO-Provider**
  Identitätsproviderstellen eine Schnittstelle zwischen Nutzerinnen und Diensten dar. Wenn der Dienst den Identitätsprovidern traut, können diese etwas über die Identität von Nutzerinnen aussagen (z. B. deren Alter). Ganz genau wie bspw. eine Freundin und jemand Fremden vorstellt. Dazu müssen sich Nutzerinnen aber bei Identitätsprovidern einloggen. Dies geschieht bisher über Passwörter und teilweise zusätzliche zweite Faktoren wie mobile TANs. Dies könnte aber durch den passwortlosen Login mittels FIDO ersetzt werden. Nutzerinnen würden sich somit über Identitätsprovider ausweisen, nutzen dafür aber genau das gleiche Mittel wie bei einem Login, nämlich ihren FIDO-Sicherheitsschlüssel. Der Vorschlag wird auch vom Bundesamt für Sicherheit in der Informationstechnik erwähnt.[3]

- **FIDO mit Ausweis**
  Mit dem deutschen Personalausweis können sich Nutzerinnen auch elektronisch ausweisen. Die Idee hinter diesem Konzept war es den Ausweis als Sicherheitsschlüssel für einen passwortlosen Login mittels FIDO2 zu nutzen. Den Ausweis mittels dem FIDO1 Standard (U2F-Protokoll) als 2. Faktor bei Webseiten zu hinterlegen ermöglicht bereits Fidelio.[4] Mehr dazu wird in einem Video[5] genauer erläutert. Die Überlegung wäre gewesen darauf aufbauend eine Art 2.0 Variante zu entwickeln, bei der der Ausweis direkt über die AusweisApp2 genutzt und der neue FIDO2 Standard eingesetzt werden könnte.

- **Fido-Vault**
  Der Identity Stick könnte weiter entwickelt werden, um Privatpersonen eine stärkere Kontrolle über ihre Daten zu geben. So könnten neue Konzepte, wie zum Beispiel eine Art 'FIDOVault' Daten- und Identitätsschutz noch transparenter machen. In einem Vault könnte ein Sicherheitsschlüssel als Speicher für wichtige Daten benutzt werden, die mit der Identität verknüpft sind. Das könnte einen Passwortmanager, eine Auflistung der Dienste, die mit dem passwortlosen Login oder 2-Faktor Authentifikation genutzt wurden, oder auch Zertifikate enthalten. Online Dienste könnten selbst über entsprechende Schnittstellen Informationen im Vault ablegen (z. B. Röntgenbild) und Nutzende selbst Daten (z.B. das 'Elster Zertifikat') eintragen.

---

[3] https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03t 59/tr03159_node.html
[4] FIDELIO verfügbar hier:
https://plav.aooale.com/store/apps/details?id=de.persoapp.android.FIDELIO&hNde
[5] Video verfügbar unter: https://youtu.be/Oc32AwPL2Nw

Nutzende würden den Diensten dann ausgewählt Daten zur Verfügung stellen, wenn diese benötigt werden.

Hintergründe und alternative Vorgehensweise

Während der Analyse gäbe es folgende Aspekte, die gegen die obigen Konzepte sprachen:

- 'FIDO mit Ausweis' wurde unabhängig von uns während der Projektlaufzeit teilweise umgesetzt (es existieren Browser-Erweiterungen).[6] Es gibt hier ein paar nicht ohne Weiteres zu lösende Usability Herausforderungen (unklar, wann Nutzende Daten pseudonym übertragen; unklar, dass der 'Ausweis' als "Sicherheitsschlüssel" verwendet werden kann; Download von Plugin und AusweisApps notwendig). Außerdem haben uns die Nutzertests gezeigt, dass Useninnen Bedenken hatten, den Ausweis als Login Mittel einzusetzen.
- Da bei 'FIDOProvider' nur die Art des Logins beim Identitätsprovider angepasst wird, ist das Potenzial einer solchen Lösung geringer. Weiterhin muss dem Identitätsprovider vertraut werden. Wenn dies eine private Organisation ist, so wird die Verantwortung für digitale Identitäten weiter auf den privaten Markt verschoben. Außerdem bietet eine einzelne Stelle wie sie der Identitätsprovider darstellt, Gefahren für den Datenschutz.
- 'FIDO-Vault' kam erst im späteren Projektverlauf auf. Da es als Konzept noch sehr schwammig war und von den benötigten Ressourcen ebenfalls unklar war, hat es leider nicht mehr in den Rahmen dieses Projekts gepasst

Stattdessen verfolgten wir vor allem das Konzept FIDO-Ident:

FIDO-Ident Konzept

Entgegengesetzt zur Nutzung eines Personalausweises zum Login ist die Idee von FIDO-Ident, einen FIDO2-Sicherheitsschlüssel ebenfalls zum Ausweisen einzusetzen. Dazu soll FIDO2 als Protokoll zur Übermittlung von Identitätsattributen genutzt werden, die sich auf dem Sicherheitsschlüssel befinden.

Das Konzept 'FIDOIdent' bietet auf Anbieterseite großes Potenzial, da der Standard schon von Unternehmen umgesetzt wird. Darauf aufzubauen bietet auch den Vorteil, dass sich Nutzerinnen viel häufiger bei Services einloggen, als sich online auszuweisen. Für beides dieselbe Methode zu nutzen, ist damit für Nutzerinnen praktischer.

Weiterleitung der FIDO Erweiterung durch den Browser

Der FIDO-Standard besteht aus zwei Teilen (Webauhtn und CTAP). Webauthn bezieht sich auf die Kommunikation zwischen Webseite und Browser und CTAP auf die Kommunikation zwischen Browser und Sicherheitsschlüssel. Erweiterungen des FIDO-Protokolls müssen von der Webseite an den Browser gesendet, aber von diesem auch weitergeleitet werden. Dies wird vom Standard nicht strikt gefordert. Daher wurde in der Mitte des Projekts geprüft,

[6] Browser Erweiterungen verfügbar unter:
https://addons.mozilla.org/de/firefox/addon/webauthn-eid-for-firefox/

inwieweit Browser eine solche Weiterieitung unterstützen. Google Chrome bzw. Chromium untersützen die Weiterleitung nur für einige spezielle Erweiterungen. Der Code von Chromium ist Open Source. Daher würde geprüft, inwieweit die Möglichkeit besteht, eine abgeänderte Variante von Chromium zu verwenden, die die Identity Stick Extension weiterleitet. Dies wurde schlussendlich nicht weiter verfolgt, da der Aufwand zu groß gewesen wäre und die Arbeit am Protokoll und dem Prototypen selbst dadurch stärker eingeschränkt worden wäre.
Im Zuge dieser Analyse konnte aber festgestellt werden, dass eine entsprechende Weiterleitung analog zu der Implementierung anderer Erweiterungen erfolgen könnte.

Kurze Angabe von Präsentationsmöglichkeiten für mögliche Nutzer

Neben dem Blogartikel und Video, die für die Demoweek des Prototype Funds erstellt wurden[7], gibt es eine Webseite (https://identity-stick.aithub.io) mit weiteren Erläuterungen und Beschreibungen. Von uns erstellter Code sowie die Beschreibung der Erweiterung finden sich auf Github (https://aithub.com/Identity-Stick). Darauf findet sich der Code für:

- Identity Stick: Code für einen Solo Key mit der Möglichkeit des Ausweisens mittels der Identity Stick Extension
- Identity Stick Extension: Beschreibung des Protokolls für den Austausch von Identitätsattributen mittels CTAP (FIDO2)
- Interface Demos: Demos, die ein mögliches Interface für passwortlosen Login bzw. Ausweisen simulieren
- Identity Stick Server: Skript zum Testen der Funktionalität eines Identity Sticks
- FIDO Debugger: Webseite zum schnellen Testen der Daten, die von einem FIDO Token gesendet werden
- Signed Identity: Tool zum Erzeugen von signierten Identitätsattributen
- Identity-Stick.github.io: Code für unsere Webseite

Kurze Erläuterung zur Einhaltung der Arbeits- und Kostenplanung

Ereignisse im Projektverlauf, die eine Anpassung der Planung erforderlich machten

Die Covid-19 Maßnahmen haben dazu geführt, dass Nutzertests und Interviews nicht in dem

[7] Blogartikel, Video und Demoweek Inhalte:
https://demoweek.prototypefund.de/projects/08-identity-stick.htmi

Umfang durchgeführt werden konnten wie anfangs geplant. Dafür wurde mehr Arbeit in die Überprüfung der technischen Machbarkeit der verschiedenen Konzepte gesteckt.

Kurze Darstellung von etwaigen Ergebnissen bei anderen Stellen

Entwicklungen anderer Personen oder Institutionen, die Einfluss auf die Arbeit und Zielsetzung hatten

Während der Arbeit an den Konzepten hatte Christoph Kahlo FIDELIO[8] weiterentwickelt Dies hat eine mögliche Entwicklung von uns in diese Richtung voraus gegriffen. Die Umsetzung hat uns aber auch gezeigt, welche offenen Fragen bei einer solchen Lösung immer noch bestehen (siehe oben Konzept "FIDO mit Ausweis"). Da uns damit deutlich wurde, dass wir nicht viel dazu beitragen könnten, haben wir diese Richtung nicht weiter verfolgt.

Da wir auf den FIDO2 Standard aufbauen, hatte dieser Standard große Auswirkungen auf unsere Arbeit. Während der Projektlaufzeit hat sich zum Beispiel Apple der FIDO Allianz angeschlossen und unterstützt jetzt FIDO2 mit dem Safari-Browser.[9] Der noch recht junge Standard FIDO2 befindet sich noch im Implementationsprozess und wird sich in Zukunft stärker verbreiten.

Wir haben den SoloKey Flacker verwendet. Dies ist ein Open Source (Flardware und Software) FIDO2 Token, dessen Code angepasst werden kann. Da die FIDO2-Funktionalität besteht, hat es sich angeboten diesen als Basis zu verwenden, um darauf aufzubauen und diesen um eine Ausweisfunktion zu erweitern. Allerdings hat dies auch bedeutet, dass Restriktionen durch die Hardware vorgegeben sind. So ist der Speicher begrenzt und ermöglicht nur einge begrenzte Länge beim Versenden der Nachrichten. Daher wurde das von uns entwickelte Protokoll so angepasst, dass es mit diesen Einschränkungen umgehen kann und zu lange Nachrichten aufgeteilt und die Teile einzeln versendet werden können.

---

[8] https://play.google.com/store/apps/details?id=de.persoapp.android.FIDELIO&hl=de

[9] Heise Online (2020): Passwort-Nachfolger: Apple bei FIDO-Allianz mit an Bord. Online: https://www.heise.de/mac-and-i/meldung/Passwort-Nachfolger-Apple-bei-FIDO-Allianz-mit-an-Bord-4657979.html