Bild: KI Midjourney | Collage c't

Wie hältst Du's mit der Wallet-App?

EUDI-Wallet: Die Debatte um die deutsche Personalausweis-App

Die Bundesregierung muss dem E-Perso bald eine Wallet-App zur Seite stellen, so verlangt es die EU. Dann soll man sich auch in Deutschland bequem mit dem Handy ausweisen können. Nun ringen Datenschutzaktivisten mit Pragmatikern um die richtige Technik für die App.

Von Christian Wölbert

Beim dritten Anlauf muss es klappen: Der deutsche E-Perso muss aufs Smartphone kommen. Denn die im Mai in Kraft getretene neue eIDAS-Verordnung der EU verlangt, dass alle Mitgliedsstaaten ihren Bürgern eine Wallet-App anbieten, mit der diese sich über das Internet ausweisen können [1]. Bis Anfang 2027 muss auch die deutsche Variante des „EU Digital Identity Wallet" (EUDI-Wallet) in den App-Stores stehen.

Die Erwartungen an die deutsche Wallet-App sind riesig, denn hierzulande ist digitale Identität bislang ein Leidensthema. Der 2010 gestartete E-Perso gilt als supersicher, aber auch als superkompliziert – vor allem, weil man den Chip in der Karte umständlich via NFC auslesen muss. In den vergangenen Jahren stiegen zwar die Nutzungszahlen, doch von einem Durchbruch kann keine Rede sein. In anderen EU-Ländern wie Österreich oder Dänemark ist das Online-Ausweisen mit dem Handy längst selbstverständlich.

Schon zweimal gescheitert

Die Bundesregierung versuchte schon zweimal, die Personalausweisdaten ins Handy zu verfrachten, um die Nutzung zu vereinfachen. Im Herbst 2021 veröffentlichte das Bundeskanzleramt eine App namens ID Wallet, nahm sie aber schon

c't kompakt

- Die Bundesregierung arbeitet an einer Wallet-App, mit der man sich im Internet sicher ausweisen und Nachweise wie Führerscheine übermitteln kann.
- Datenschutzaktivisten wollen verhindern, dass dabei staatliche signierte Identitätsdaten eingesetzt werden, die für Kriminelle besonders attraktiv sind.
- Im Rahmen eines Wettbewerbs entwickeln unter anderem Google und Samsung Prototypen für die deutsche Wallet-App.

ein paar Tage später wieder offline. Zuvor hatten Sicherheitsforscher demonstriert, dass Angreifer die Ausweisdaten leicht abphishen können.

Beim zweiten Versuch namens Smart-eID nutzte das Bundesinnenministerium (BMI) die bestehende E-Perso-Infrastruktur, die Ausweisdaten wurden aber in einem speziellen Sicherheitschip (Secure Element) im Smartphone statt auf der Chipkarte abgelegt. Ende 2023 stellte das BMI den Testbetrieb ein, weil viele Handyhersteller, darunter Apple, ihre Secure Elements nicht freigeben wollten und diese Chips ohnehin nur in relativ teuren Modellen stecken. Entwicklung und Testbetrieb der Smart-eID hatten bis dahin schon 90 Millionen Euro verschlungen.

Nun, im dritten Anlauf, wirkt die Bundesregierung bemüht, die Fehler der Vergangenheit nicht zu wiederholen. Statt wie bisher im stillen Kämmerlein zu tüfteln, hat das BMI die Bundesagentur für Sprunginnovationen (Sprind) beauftragt, einen Konsultationsprozess durchzuführen. Im Rahmen dieses Prozesses hat die Sprind ein 150-seitiges Architekturkonzept mit diversen technischen Varianten auf der Plattform open CoDE veröffentlicht und sammelt dort Feedback (ct.de/yd5g). In Workshops diskutieren Vertreter von Behörden, Unternehmen und zivilgesellschaftlichen Organisationen zum Beispiel Datenschutzaspekte und Geschäftsmodelle; die Aufzeichnungen werden ebenfalls auf open CoDE veröffentlicht.

Parallel dazu veranstaltet die Sprind im Auftrag des BMI einen „Funke“ genannten Wettbewerb, in dem elf Unternehmen Wallet-Prototypen entwickeln sollen. An diesem Wettbewerb nehmen unter anderem die Schwergewichte Samsung und Google teil (siehe Kasten „Der Wallet-Wettbewerb“).

Signiert oder nicht signiert?

Bereits jetzt steht fest, dass der Konsultationsprozess und der Wettbewerb nicht zu einer Lösung führen werden, die alle Interessengruppen zufriedenstellt. Denn egal, wie man es dreht und wendet: Es gibt keine Technik, die hinsichtlich aller Sicherheits- und Datenschutzaspekte die höchsten Anforderungen erfüllt und obendrein mit allen Smartphones kompatibel ist. Jede der diskutierten Varianten hat Vor- und Nachteile. Und am Ende wird das BMI entscheiden müssen, welche Nachteile es in Kauf nimmt. Denn die Vorgaben der europäischen eIDAS-Verordnung sind eher abstrakt und lassen den Mitgliedsstaaten Spielraum bei der Umsetzung (siehe Kasten „eIDAS, was ist das?“).

Umstritten ist momentan vor allem die Frage, wie die Echtheit der vom Nutzer an einen Empfänger übermittelten Ausweisdaten sichergestellt werden soll. Anders formuliert: Wie verhindert man, dass jemand Ausweisdaten manipuliert, um zum Beispiel ein Bankkonto unter falschem Namen zu eröffnen? Das aktuelle Architekturkonzept stellt zwei Ansätze zur Sicherstellung der „Unforgeability“, also der Unfälschbarkeit, zur Diskussion:

- **Sicherer Kanal („Authenticated Channel“):** Diese Methode ist vom E-Perso bekannt. Der Grundgedanke lautet, dass der Empfänger von der Korrektheit der Ausweisdaten ausgehen kann, weil ein vertrauenswürdiges IT-System ihm diese über einen sicheren Kanal schickt. Im Fall des E-Perso ist dieses System der Chip in der Ausweiskarte. Der Chip gilt als vertrauenswürdig, weil der Ausweisherausgeber, also die Bundesregierung, selbst ein Interesse daran hat, dass nur korrekte Ausweisdaten übertragen werden und entsprechend manipulationssichere, zertifizierte Chips verwendet. Das Ganze ließe sich auch ohne die Ausweiskarte realisieren: Dafür könnte ein ähnlich manipulationssicherer Chip im Smartphone, ein Secure Element, oder ein Server der Bundesregierung den Kanal aufbauen.
- **Signierte Daten („Signed Credentials“):** Dieses Prinzip ist zum Beispiel von der Qualifizierten Elektronischen Signatur (QES) bekannt. Dabei signiert der Ausweisherausgeber, also der Bund, die Ausweisdaten: Er berechnet, vereinfacht gesagt, aus den Ausweisdaten und einem geheimen Schlüssel einen Signaturwert. Der Empfänger der Ausweisdaten kann mithilfe des Signaturwerts und des öffentlichen Schlüssels des Herausgebers prüfen, ob die Daten manipuliert wurden.

Pro Kanal …

Viele Datenschützer und Netzaktivisten favorisieren die Methode des authentifizierten Kanals, denn dabei kann der Empfänger die Echtheit der Ausweisdaten innerhalb der Kommunikation mit dem Nutzer prüfen, aber nicht gegenüber Dritten beweisen. Daraus folgt: Sollte ein Unternehmen die Daten unberechtigt weitergeben oder gehackt werden, können Kriminelle nicht sicher sagen, ob es sich um echte Daten handelt. Und ein betroffener Nutzer kann glaubhaft abstreiten, dass er seine Daten übermittelt hat, was zum Beispiel bei sozial unerwünschten Anwendungen erstrebenswert sein kann.

Leaken hingegen die Ausweisdaten samt staatlicher Signatur, können Cyberganoven sicher sein, dass sie über authentische Daten verfügen, was den Wert auf dem Schwarzmarkt steigern dürfte. Der österreichische Datenschutzexperte Thomas Lohninger vom Verein epicenter.works sieht darüber hinaus die Gefahr,

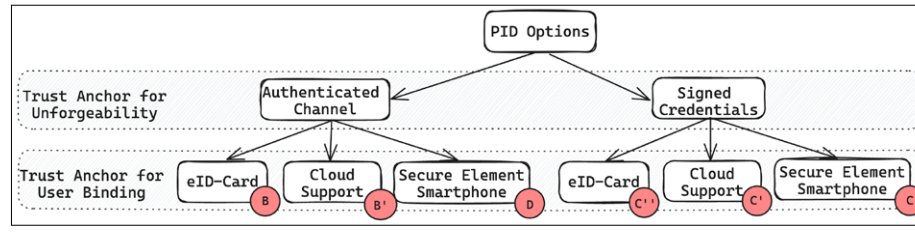

Bild: open CoDE

Das aktuelle Architekturkonzept stellt Varianten für die Unfälschbarkeit und die Nutzerbindung der staatlichen Ausweisdaten in der geplanten EUDI-Wallet-App zur Diskussion.

dass Unternehmen die signierten Daten sammeln und heimlich für andere Zwecke verwenden als von den Nutzern freigegeben. „Die DSGVO allein reicht nicht aus, um das zu verhindern, das zeigen die bisherigen Erfahrungen“, warnt Lohninger, der in der Jury des Wallet-Wettbewerbs der Sprind sitzt.

… und pro Signaturen

Aber die Signaturvariante bietet auch Vorteile. Voraussichtlich werden praktisch alle anderen EU-Mitgliedsstaaten im Rahmen der eIDAS-Umsetzung auf diese Technik setzen. Deshalb wäre ein deutsches Wallet, das auf signierten Daten beruht, problemlos EU-weit kompatibel, so wie die eIDAS-Verordnung es verlangt. Geht Deutschland einen Sonderweg, müssten europaweit alle „Relying Parties“ – also Datenempfänger wie Banken oder Behörden – auch die deutsche Technik implementieren.

Theoretisch könnte eine Interoperabilitätsschicht zwischen den Welten vermitteln. Doch dafür müsste der Betreiber dieser Schicht die Daten prüfen und umwandeln, es gäbe also keine kryptografische Ende-zu-Ende-Absicherung mehr, erklärt Torsten Lodderstedt. Der promovierte Informatiker und Experte für digitale Identität leitet bei der Sprind den Konsultationsprozess für die Entwicklung der deutschen Wallet-App sowie den „Funke“-Wettbewerb.

Im Konsultationsprozess gehe es um eine „sorgsame Abwägung der Vor- und Nachteile der beiden Varianten“, betont Lodderstedt im Gespräch mit c’t. Ziel sei es „die richtige Balance zwischen Sicherheit, Datenschutz, Nutzbarkeit und Reichweite“ zu finden und im Wettbewerb auch zu erproben.

Deutschland habe sich bei der Entwicklung der Online-Ausweisfunktion des E-Perso für den Authenticated Channel entschieden, „weil dieser zum Zeitpunkt der Entwicklung den besten Schutz der Nutzenden versprach“, ergänzt Lodderstedt. Mittlerweile habe man jedoch mehr Erfahrung mit digitalen Identitäten gesammelt, sodass man die Entscheidung noch einmal prüfen sollte. „Zum Beispiel speichern die Empfänger meiner Erfahrung nach in der Regel nur die ausgelesenen Daten in einer Datenbank, also nicht samt Signatur“. Zudem verweist Lodderstedt auf ID-Systeme wie die schwedische BankID und die dänische NemID, die bereits seit vielen Jahren signierte Identitätsdaten verwenden.

Was sagt das BSI?

Die Entscheidung pro Kanal oder pro Signaturen muss das BMI treffen, aber eine wichtige Rolle spielt dabei das Votum des Bundesamts für Sicherheit in der Informationstechnik (BSI). Die Behörde formulierte 2022 im Rahmen einer Bundestagsanhörung zu digitalen Identitäten klipp und klar, dass Ausweisdaten „nicht einfach mit einer Signatur versehen und an den Empfänger übermittelt werden“ sollten (siehe ct.de/yd5g). Wie sich das BSI nun verhält, ist aber unklar: Auf Anfrage von c’t sagte ein Sprecher, dass man sich zu dem Thema zurzeit nicht öffentlich äußere. „Hintergrund sind laufende Gespräche und Beratungen, denen das BSI nicht vorgreifen kann.“

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) signalisiert, dass ihm die Kanalmethode lieber wäre, er sich aber auch die Signaturvariante vorstellen kann. Ein sicherer Kommunikationskanal biete „einen gewissen Schutz vor Zweckänderungen“ und mache die Daten „weniger attraktiv für den Weiterverkauf beispielsweise nach Leaks“, sagte ein BfDI-Sprecher. Daher sei es eine sinnvolle technische Maßnahme, auf Signaturen zu verzichten. „Die Entscheidung hat aber noch andere Abhängigkeiten, sodass die Verantwortlichen hier eine Abwägung treffen müssen.“ Falls die Bundesregierung sich für Signaturen entscheide, müsse sie „zusätzliche Maßnahmen“ ergreifen, damit die staatlich bestätigten Identitätsdaten nicht missbraucht werden. Welche Maßnahmen das sein könnten, führte der Sprecher auch auf Rückfrage nicht aus.

Diebstahlschutz über die Cloud

Neben der Frage der Fälschungssicherheit muss das BMI auch über die der Nutzerbindung entscheiden: Wie wird sichergestellt, dass nur berechtigte Nutzer ihre Ausweisdaten mit der Wallet-App übermitteln und nicht zum Beispiel jemand, der das Smartphone geklaut hat? Dafür setzt das aktuelle Architekturkonzept eine Zwei-Faktor-Authentifizierung voraus. Der Nutzer müsste demnach im ersten Schritt mit den Systemfunktionen von iOS oder Android nachweisen, dass er der rechtmäßige Besitzer des Smartphones ist, also zum Beispiel via Gesichtserkennung oder Fingerabdruck.

Als zweiten Faktor sieht das Konzept eine PIN vor, mit der der Nutzer seine Ausweisdaten freischaltet. Aber wie setzt man eine sichere PIN-Prüfung um, ohne sich allein auf die Mechanismen von Android oder iOS zu verlassen? Dafür listet das Konzept drei Varianten auf. In der ersten Variante würde der E-Perso-Chip die Geheimnummer prüfen. Dann müssten Nutzer allerdings jedes Mal (wie bisher) umständlich via NFC eine Verbindung zur Ausweiskarte aufbauen, weshalb das BMI diese Option vermutlich nicht ernsthaft in Betracht zieht. In der zweiten Variante würde ein Secure Element im Smartphone die PIN prüfen, in der dritten Variante ein zentrales Cloud-

eIDAS, was ist das?

eIDAS steht für „electronic IDentification, Authentication and trust Services“ und bezeichnet eine EU-Verordnung von 2014, die unter anderem rechtssichere digitale Unterschriften und digitale Identitätsnachweise regelt. Im Mai 2024 trat eine umfangreiche Novelle der Verordnung in Kraft, die die Grundregeln für die EUDI-Wallet-Apps enthält. Diese müssen zum Beispiel Open Source sein und eine pseudonyme Nutzung erlauben. Behörden und Unternehmen, die Wallet-Daten von Nutzern empfangen, müssen sich vorab registrieren und angeben, welche Daten sie für welche Zwecke abfragen wollen. Zudem verlangt die Verordnung, dass niemand benachteiligt werden darf, weil er keine Wallet-App verwendet.

Datenschützer haben damit viele ihrer Forderungen in der Novelle unterbringen können. Allerdings befürchten Kritiker nach wie vor, dass die EUDI-Wallet-Apps zu einer Überidentifizierung führen: dass Nutzer sich also künftig nicht mehr pseudonym zum Beispiel bei sozialen Netzwerken anmelden, sondern mit echtem Namen und Adresse, weil das mit den Wallet-Apps einfacher wird als bisher [1]. Der Datenschutzverein epicenter.works sieht zudem die Gefahr, dass pseudonyme Nutzer nachträglich identifiziert werden könnten.

Der Wallet-Wettbewerb: Diskussion um Google-Teilnahme

Die Bundesagentur für Sprunginnovationen (Sprind, siehe c't 24/2022, S. 136) sieht Wallets als „Basis von Sprunginnovationen", weil sie eine vollständige Digitalisierung von Prozessen ermöglichten. Im Auftrag des Bundesinnenministeriums führt sie einen Wettbewerb durch, in dem elf Teams funktionsfähige Prototypen von Wallet-Apps entwickeln sollen. Die Agentur erhofft sich davon Erkenntnisse, „die in die Entwicklung sicherer, datensparsamer, nutzbarer und reichweitenstarker EUDI-Wallets einfließen werden". Bislang gebe es noch zu wenig „Implementierungserfahrung".

Ende Mai gab die Sprind bekannt, welche Wettbewerbsteilnehmer die Jury ausgewählt hat: Im „Funded Track" starten sechs Firmen, unter anderem Governikus und Authada aus Deutschland sowie Startups aus den Niederlanden und der Schweiz. Diese Teilnehmer erhalten eine Förderung und müssen im Gegenzug den Quellcode ihres Prototypen unter einer Open-Source-Lizenz publizieren. Im „Non-Funded Track" starten fünf Firmen, darunter die Schwergewichte Samsung und Google.

Innerhalb der zehnköpfigen Jury war die Entscheidung für Google umstritten. „Ein Jurymitglied sprach sich aufgrund von Datenschutz- und Wettbewerbsbedenken deutlich gegen Google aus", heißt es auf der Sprind-Website. Die Mehrheit habe jedoch entschieden, Google zur Teilnahme einzuladen und diese Aspekte am Ende der ersten Stufe des Wettbewerbs erneut zu bewerten. In der Jury sitzen unter anderem Beamte vom BMI und BSI, Forscher und Wirtschaftsvertreter sowie der Datenschutzaktivist Thomas Lohninger. Google betonte, dass man eine „vollständig quelloffene Referenz-Wallet-Implementierung" bereitstelle und „starke Sicherheits- und Privatsphäre-Eigenschaften" anstrebe.

Backend, also zum Beispiel ein staatlicher Server.

Die „Zwischenlösung" des BSI

BSI-Chefin Claudia-Plattner machte Anfang des Jahres in einem Vortrag klar, dass sie prinzipiell eine dezentrale Lösung mit Secure Elements bevorzugt. Da sichere und zertifizierte Secure Elements aber noch nicht weit genug verbreitet seien, brauche man als „Zwischenlösung" ein zentrales Backend-System. Diese Rolle könnte zum Beispiel ein staatlicher Server übernehmen. Das muss kein Datenschutzalbtraum sein, denn die PIN-Prüfung lässt sich so umsetzen, dass der Staat nicht erfährt, wer sich wann gegenüber wem ausweist.

Torsten Lodderstedt plädiert gegenüber c't ebenfalls für eine PIN-Prüfung in der Cloud für eine erste Version der Wallet-App. Und auch aus seiner Sicht ist später ein Schwenk auf Secure Elements sinnvoll. Das Wallet solle „so dezentral wie möglich" sein, sagt er.

Vorerst läuft aber alles auf die Cloud hinaus. Spannend wird, welches „Vertrauensniveau" das Wallet dann erfüllt. Die eIDAS-Verordnung unterscheidet zwischen den drei Niveaus „niedrig", „substanziell" und „hoch". Welche Stufe das Wallet erreicht, wird das BSI voraussichtlich im Auftrag des BMI prüfen. Gegenüber c't wollte das BSI sich auch zu diesem Thema nicht äußern.

Der BfDI teilte mit, dass nach seinem Verständnis für ein hohes Vertrauensniveau „grundsätzlich eine Hardwarebindung unter Nutzendenkontrolle" vorhanden sein müsse, also ein Chip in einer Karte oder im Gerät statt ein zentraler Server. Schafft das Wallet nur „substanziell", könnten Wallet-Nutzer nicht alle Anwendungsfälle allein mit der App erledigen. Für sensible Vorgänge, wie etwa im Gesundheitsbereich oder bei bestimmten Anträgen bei Behörden, müssten sie dann doch wieder die E-Perso-Chipkarte hervorkramen und via NFC auslesen. So oder so wird die EUDI-Wallet-App den E-Perso nicht vollständig ersetzen: Zumindest bei der Ersteinrichtung der App werden Nutzer ihre Daten voraussichtlich aus der Ausweiskarte auslesen müssen.

Wer darf Wallets bauen?

Eine weitere offene Frage ist, ob die Bundesregierung selbst eine Wallet-App anbieten und betreiben wird oder ob sie stattdessen oder zusätzlich Wallets privater Unternehmen zulassen wird. Geht es nach Wirtschaftsvertretern, sollte es auch private Anbieter geben. Sie argumentieren, dass ein Wettbewerb für eine höhere Qualität und eine schnellere Verbreitung sorgen würde. Anbieter wie Google und die Sparkassen haben schon klargemacht, dass sie gerne eine EUDI-Wallet-App entwickeln würden.

Der Datenschützer Thomas Lohninger sieht bei einer Wahlfreiheit den Vorteil, dass Nutzer sich dann für die datenschutzfreundlichste Lösung entscheiden könnten. „Aber für die Wallets muss es strenge Anforderungen geben, und der Zertifizierungsprozess muss ernst genommen werden."

Die Zeit rennt

Das sind aber längst noch nicht alle Fragen, die die Bundesregierung zu klären hat. Die EUDI-Wallet-Apps sollen nicht nur als digitale Ausweise dienen, sondern auch Nachweise wie Zeugnisse oder Führerscheine übermitteln und damit etwa Bewerbungen oder Mietwagenbuchungen vereinfachen.

In Deutschland müssen also Tausende kommunaler Behörden, die bislang zum Beispiel analoge Führerscheine ausstellen, in die Lage versetzt werden, digitale Credentials zuzustellen. Es muss geklärt werden, auf welchen Wegen und in welchen Formaten diese Nachweise im Wallet landen. Torsten Lodderstedt hofft deshalb, dass die Entscheidung zwischen signierten Ausweisdaten und sicherem Kanal bald getroffen wird: „Wir haben so viele Herausforderungen zu lösen, die damit gar nichts zu tun haben."

Schon Mitte nächsten Jahres sollen der Sprind-Wettbewerb und der Konsultationsprozess abgeschlossen sein. Selbst, wenn das BMI sich dann schnell entscheidet, bleiben im Anschluss weniger als zwei Jahre bis zum angepeilten Starttermin. „Die Zeit ist knapp für ein derart ambitioniertes IT-Projekt", sagt Lodderstedt. *(cwo@ct.de)* c't

Literatur

[1] Sylvester Tremmel, Die EU-Wallets kommen, Licht und Schatten bei der neuen eIDAS-Verordnung, c't 7/2024, S. 14

Architekturkonzept, BSI-Stellungnahme: ***ct.de/yd5g***