Was die EUDI-Wallet für Unternehmen bedeutet

Die Standards sind da, der politische Wille auch, aber was erwartet Unternehmen konkret, wenn die EU die EUDI Ende des Jahres ausrollt? Im Interview mit einem IAM-Anbieter finden sich Antworten.

Von Kornelius Kindermann

Quelle: Vanessa Bahr / iX

Die EUDI-Wallet kommt und die Frage für Unternehmen ist nicht mehr, ob, sondern wie die Einführung abläuft. Michael Doujak, Product Manager für IAM beim Schweizer Securityunternehmen Airlock, hat das Thema Self-Sovereign Identity (SSI) seit den ersten politischen Debatten um die Schweizer e-ID begleitet. Sie stellt zusammen mit der dazugehörigen swiyu-Wallet eine schweizerische Parallelentwicklung zur europäischen EUDI-Wallet dar; beide sollen voraussichtlich Ende 2026 verfügbar sein.

Der Securityanbieter Airlock sieht bei Unternehmen bereits eine hohe Erwartungshaltung hinsichtlich der EUDI. Im Gespräch mit iX erklärt Michael Doujak, welche Business Cases sich bereits konkret abzeichnen, wie IAM-Systeme als Orchestrator zwischen klassischen Authentifizierungsmethoden und SSI-basierter Credential-Verifikation vermitteln – und wo technische Standards und Marktmechanismen noch für Unsicherheit sorgen.

iX: Herr Doujak, besonders interessant an der EUDI ist ja das Interoperabilitätsversprechen – sowohl Ticketanbieter als auch Banken können auf dieselbe Basis setzen. Wie sieht der Zeithorizont aus – wann sind wir in dieser schönen neuen interoperablen Welt angekommen?

Doujak: Das hängt maßgeblich von der Adoption in der Bevölkerung ab. Vergleichbare Daten und Projekte von Eurostat zeigen, dass der Erfolg stark vom Kundennutzen beeinflusst wird. Sobald Banken und Behörden auf den Zug aufspringen und die EUDI für Prozesse wie zum Beispiel die Wiederherstellung des Passworts einsetzen, kann das eine erhebliche Auswirkung auf die Verbreitung haben. Dänemark hat auf diese Art und Weise rund 97 Prozent der erwachsenen Bevölkerung dazu gebracht, ihre nationale digitale Identität zu nutzen. Das e-ID-Team der Schweiz hat sich vorgenommen, im ersten Jahr über eine Million Schweizer Bürger für die e-ID zu gewinnen – ein ambitioniertes Ziel, bei dem ich aber zuversichtlich bin, dass es erreicht wird.

Was macht die EUDI-Wallet für Unternehmen relevant?

Im Prinzip gibt es einen Paradigmenwechsel: Die Credentials werden direkt dem Nutzer übergeben und er kann sie überall dort einsetzen, wo eine Identifikation erforderlich ist. Ein Beispiel: Fußballtickets werden in der Wallet hinterlegt und sind damit an den Nutzer gebunden. Sie können dann nicht mehr weiterverkauft werden. Für Ticketanbieter ergeben sich dadurch komplett neue Möglichkeiten. Damit ließe sich womöglich der ganze Ticketschwarzmarkt austrocknen.

Oder stellen Sie sich vor, Sie mieten ein Auto im Urlaub: Das Fahrzeug wird im Voraus ausgewählt, vor Ort angekommen greift die Wallet. Sie erkennt Standort, Zeitpunkt und hinterlegten Führerschein und der Mietvertrag beginnt automatisch zu laufen. Im besten Fall ließe sich sogar die eigene in der Wallet hinterlegte Haftpflichtversicherung mit anbringen.

Das sind nur zwei Beispiele, die aber zeigen: The sky is the limit. Identifikation wird der erste Schritt sein und darauf fokussieren sich die Nationalstaaten jetzt gerade. Aber Identifikation ist nur der Einstieg. Immer wenn es eine Interaktion zwischen einer Person und einem Service gibt, der Daten erfordert, könnte man die EUDI-Wallet einsetzen. Den Möglichkeiten sind kaum Grenzen gesetzt.

Welche Business Cases haben Sie bei Airlock im Blick?

Wir als Hersteller sind im Open Banking Project in der Schweiz aktiv, das in den

iX-TRACT

- Eine Frage der Adoption: Die vereinte Anstrengung der EU stimmt zuversichtlich, letztlich hängt der Mehrwert der EUDI-Wallet aber davon ab, ob Nutzer sie breit aufnehmen.
- Die neue Anmeldemethode bringt IAM-Systeme in die Rolle eines Orchestrators, der klassische Authentifizierungsmethoden und Credential-Verifikation auf Basis von Self-Sovereign Identities parallel betreibt.
- Google und Apple könnten die EUDI-Wallet-Funktion in ihre Betriebssysteme integrieren – das würde die Adoption fördern und Business-Apps ließen sich leichter entwickeln, wenn das OS den Umgang mit den Credentials als Service übernimmt.

vergangenen anderthalb Jahren zwei Workshopserien durchführte: zu Use Cases der e-ID für Schweizer Banken und zu Proof-of-Concept-Umsetzungen. Zentral waren dabei das Onboarding und die Reidentifikation als Anwendungsfälle. Bis 2030 müssen alle Schweizer Banken rund 30 Prozent ihrer Kunden neu identifizieren, weil die vorhandenen Daten zu schlecht sind, etwa wegen veralteter Kopien oder unleserlicher Scans.

Ein weiterer Use Case ist für uns der Besuch in der Filiale – ein Kunde, der seine Brieftasche zu Hause gelassen hat, kann sich dann über die e-ID ausweisen, um Geld abzuheben. Für solche Szenarien existieren bereits PoCs, die nun begleitend umgesetzt werden. Banken in der Schweiz werden also vielleicht nicht am ersten Tag, aber kurz nach der Einführung der e-ID entsprechende Angebote für die Wallet haben, und das sollte die Adoption durchaus stärken.

Die großen Piloten der EUDI lassen sich also als echte Implementierungsvorbilder betrachten?

Ja, wir hatten bei einem PoC zum Onboarding Identity Provider dabei, die ganz klar gesagt haben, dass sie ihr Angebot so erweitern werden und die e-ID beziehungsweise die EUDI als zusätzlichen Identifikationskanal im Onboarding einer Bank integrieren. IAM-Anbieter arbeiten jetzt also aktiv daran, diese Funktionalität in ihre Produkte einzubringen, sodass Banken diesen Prozess direkt nach Einführung nutzen können.

Wie können IAM-Anbieter auf der einen und die interne IT auf der anderen Seite die EUDI in ihre Unternehmen bringen?

In der EU und in der Schweiz gibt es natürlich diese öffentlichen Komponenten, die man einfach einsetzen und integrieren kann. Wir sind da ein bisschen einen anderen Weg gegangen und haben uns mit einem Partner zusammengetan, der eine SSI-Komponente bereitstellt, die sowohl die Schweizer swiyu-App als auch die EUDI-Wallet bedient. Diese Komponente versorgt das IAM, das als Orchestrator agiert. Statt klassischer Protokolle wie OpenID Connect, bei denen Access-Token oder Refresh-Token ausgestellt werden, kann das IAM von dieser Komponente einen Proof Request anfordern – konkret die URL zum Proof Request – und diesen gegenüber der Wallet exponieren. Zum Beispiel als QR-Code auf dem Bildschirm oder App-to-App mit einem Universal Link.

Die Wallet kommuniziert anschließend direkt mit der SSI-Komponente. Sobald das Prüfverfahren erfolgreich abgeschlossen ist, kann das IAM die darin enthaltenen Daten übernehmen. Die Attribute aus dem Verified Credential lassen sich dann in weiteren Prozessen nutzen. Ob man das über eine externe Komponente abbildet oder in die eigene Software integriert, ist eine reine Make-or-Buy-Entscheidung.

Welche technischen Aspekte der EUDI-Wallet befinden sich noch im Umbruch?

Die größte Komplexität steckt in der SSI-Komponente. Dort ist aus meiner Sicht noch Entwicklung zu erwarten. Die bisher definierten Credential-Formate und die Protokolle OID4VCI und OID4VP sind seit ein paar Monaten finalisiert. Aber Protokolle rund um die Verwaltung und Prüfung von Trust sind noch in der Erarbeitung. Zudem wird es zukünftig Veränderungen geben. Quantencomputing wird dafür sorgen, dass Signaturalgorithmen angepasst werden müssen, auch das wird Auswirkungen auf die Credential-Formate haben.

Werden diese Weiterentwicklungen auf den Schultern von Unternehmen liegen oder wird das eher von der öffentlichen Seite kommen?

Eine spannende Frage, ich bin bei der Antwort ambivalent. Es gibt Argumente, dafür, solche Funktionen in die nationale Infrastruktur zu integrieren, damit die EUDI-Wallet die entsprechenden Protokolle unterstützt. Bei privaten Anbietern ist die Wahrscheinlichkeit hoch, dass die nationalen Wallets solche Lösungen nicht übernehmen.

Ich halte ein Szenario für möglich, in dem sich große Player wie Google und Apple an nationalen Stellen zertifizieren lassen und damit zum „Über-Provider" für das ganze Ökosystem werden. Statt als App sollte man die Lösung dann eher als Infrastruktur begreifen, die direkt ins Betriebssystem integriert ist und über entsprechende APIs den Zugriff auf Credentials sowie die Interaktion darüber ermöglicht. Die Wallet von Google bietet heute schon solche Schnittstellen, iOS nach meinem Kenntnisstand auch. Das wäre natürlich sehr viel einfacher als eine isolierte Lösung einzelner Anbieter. Diese haben am Anfang sicher Chancen, könnten in zwei bis drei Jahren aber an Bedeutung verlieren.

Erfordern unterschiedliche Sicherheitsstandards oder Einsatzfelder Sonderlösungen?

In der EUDI-Wallet ist das ganz elegant gelöst: Dort gibt es Policy-Anforderungen in den Trust-Protokollen sowie Anforderungen für die Trust Registry. Wer als Issuer auftreten will, muss registriert sein. Dabei wird hinterlegt, welche Schemata, also Credential-Typen, er ausstellen darf und welche Regelwerke gelten. Als Verifier kann ich daraufhin verifizieren, ob der Level of Assurance, den der Issuer in das Credential investiert hat, meinen Anforderungen genügt. Die Trust-Infrastruktur der EUDI-Wallet übernimmt damit einen großen Teil der Absicherung. Wer etwa Konzerttickets ausstellt, muss geringere Prozessanforderungen erfüllen als eine Bank, die KYC-Credentials ausstellt.

Wie werden sich Credential-basierte Angriffe weiterentwickeln?

Es ist möglich, dass man die Registrierungsstelle des Staates zu täuschen versucht, aber die Hürde wäre sehr viel höher, als sie es heute ist. Heute muss man nur ein Ausweispapier oder ein Ausweisdokument erstellen, das den Leser des

Im Interview: Michael Doujak

Quelle: Airlock

Michael Doujak ist Product Manager für den Airlock Secure Access Hub bei der Ergon Informatik AG und Experte für IAM, Multi-Faktor-Authentifizierung und Web-Application-Firewall. Nach seinem Studium an der ETH Zürich begleitet er einschlägige IAM-Projekte wie den Aufbau von SwissSign als Herausgeber von qualifizierten Zertifikaten in der Schweiz, die Patientendossierplattform MonDossier-Medical und die EPD-Infrastruktur der Schweizerischen Post.

Ein aktueller Fokus seiner Tätigkeit liegt auf dem Einsatz von Self-Sovereign Identities in bestehenden Geschäftsprozessen, nicht zuletzt im Zuge der Einführung von E-ID und EUDI in der Schweiz und Europa.

Dokuments überzeugt – mit der EUDI-Wallet muss man die staatliche Stelle überzeugen, dass man tatsächlich der richtige Bürger ist, um einen elektronischen Personalausweis zu kriegen. Der Vorteil im SSI-Ökosystem im Hinblick auf Betrug ist ja, dass Issuer und Verifier mit einer hohen Qualität identifiziert wurden. Kryptografisch und in Bezug auf Selective Disclosure mache ich mir auch keine großen Sorgen. Aber: Social Engineering wird weiterhin möglich sein. Es lässt sich schwer verhindern, dass jemand ein gefälschtes Dokument mit der EUDI-Wallet signiert.

Gleichzeitig lassen sich Betrugsfälle besser nachvollziehen. Wenn eine Person bereits auffällig geworden ist, weil sie schon als Money Mule oder Ähnliches agiert hat, muss sie vielleicht mit einem Personalausweis vorstellig werden, um sich eine EUDI-Wallet und die entsprechende Person Identification Data (PID) zu holen. Da weiß man dann wenigstens genau, wer den Betrug begangen hat.

Ist es ein relevantes Risiko, dass ein Trusted Issuer kompromittiert wird?

Das ist ein bekanntes Szenario. Man denke an den Mitarbeiter, der bei einer Botschaft arbeitet und quasi echte Pässe gefälscht herausgibt. Dieses Risiko lässt sich in einem gewissen Maß auch auf die EUDI-Wallet übertragen. Spannend wird vor allem die Frage – und das wird dann erst die Praxis zeigen –, ob und wie viel Kontrolle ich als Benutzer überhaupt über das Vertrauen meiner Wallet haben werde. Muss meine Wallet grundsätzlich allen verifizierten Issuern oder Verifiern vertrauen, oder kann ich als Nutzer steuernd eingreifen? Bei Browsern konnte ich früher die Root-Trust-Liste nach dubiosen Roots durchforsten – funktioniert so etwas vielleicht auch im Kontext der EUDI-Wallet? So könnte man beispielsweise nach Spanien reisen und dort zunächst das Ökosystem lokaler Tourismusanbieter aktivieren. Eine Wallet-App mit Fraud Detection wäre in der Zukunft ebenfalls denkbar.

Wie sieht jetzt die Übergangszeit aus? Alte IAM-Strukturen parallel zur EUDI-Authentisierung?

Wir verstehen IAM als einen Orchestrator, der einerseits verschiedene Authentisierungsmittel – Username, Passwort, OAuth und Ähnliches – sowie andererseits die Integration mit Backend-Systemen orchestriert. Während die meisten modernen Systeme in der Lage sind, Access-Token aus JSON-Strukturen zu interpretieren, gibt es bei Banken noch Legacy-Systeme mit speziellen Anforderungen.

Uns brachte das auf eine IAM-Architektur, bei der sich für jeden Einsatzzweck unterschiedliche Flows konfigurieren lassen. Es spielt dann keine Rolle, ob ein Prozess die EUDI-Wallet, OAuth oder klassische Logins durchlaufen hat, weil wir auf die Art und Weise ein hybrides Angebot machen können. Der Kunde entscheidet. Für den Betreiber des IAM ist das lediglich eine zusätzliche Konfiguration, die er aktivieren muss, damit seine Kunden die EUDI-Wallet nutzen können. Aber es ist kein separates System, das er zusätzlich benötigt.

Welche Entscheidungen stehen jetzt für CEOs und CTOs an?

Als Unternehmen sollte ich mich fragen: Wo kann ich den maximalen Nutzen mit der EUDI für mein Unternehmen erreichen – und welche Risiken bestehen, wenn ich versuche, die EUDI zu ignorieren? Was passiert, wenn meine Konkurrenz EUDI anbietet und ich nicht? Ich habe vorhin vom Open Banking Project erzählt. Da ging es zuerst darum, Use Cases zu identifizieren und zu bewerten, und ich glaube, das ist genau das, was auf C-Level passieren muss. Das ist keine Frage für den IAM-Administrator.

Bei einem Kunden gehen wir so etwas typischerweise in Ideation-Workshops an und machen dabei eine SWOT-Analyse aller bestehenden identitätsbezogenen Prozesse – und starten auch mit einer Einführung in die EUDI-Wallet an sich. Bekommt man fünf bis zehn Leute aus unterschiedlichen Bereichen in solch einem Workshop zusammen, hat man schnell eine ganze Sammlung an Ideen, die dann im Hinblick auf den Business Impact konsolidiert werden müssen: Welche Ideen bringen den Kunden etwas, welche bringen etwas für das Unternehmen und wie schnell können wir sie umsetzen beziehungsweise können wir sie überhaupt aus eigener Kraft umsetzen?

Ein Aspekt ist dabei auch die Adoption in anderen Feldern: Möchte ich als Autovermieter beispielsweise mit den Credentials eines Versicherungsanbieters arbeiten, müssen entsprechende Partner auch vorhanden sein. Erst dann, wenn es um die Umsetzung eines konkreten Use Case geht, sollte der Blick aufs IAM gehen und darauf, ob es die Voraussetzungen mitbringt, um mit SSI und der EUDI-Wallet zu arbeiten.

Was muss ein Unternehmen befürchten, das jetzt mit der Einführung zögert?

Das ist wieder eine Frage der Adoption und damit ein Blick in die Kristallkugel. Ich bin zuversichtlich, denn die Large Scale Pilots haben gezeigt, dass man auf das Angebot möglicher Anwendungsfälle gut vorbereitet ist. Und sollte die Adoption tatsächlich so gut und schnell ausfallen wie angedacht, dann wird es für Kunden schlicht attraktiver, mit SSI umzugehen – und unattraktiver, bei herkömmlichen Login-Methoden zu bleiben.

Wäre eine Altersverifikation auf Social Media möglicherweise der entscheidende Schritt für eine Adoption?

Ich habe da Bedenken, die Altersverifikation ist eines der Szenarien, die sehr gut angreifbar sind. Ein Kind könnte sich relativ einfach mit dem Smartphone seiner Eltern als volljährig ausgeben. Die EU hat da bessere Adoption-Anreize: Unternehmen mit gesetzlicher Pflicht zur starken Authentisierung – etwa im Rahmen von PSD2 und PSD3 (EU-Zahlungsrichtlinie, Payment Service Directive) – müssen die EUDI akzeptieren. Das betrifft insbesondere Banken, Internetprovider und weitere regulierte Branchen. Diese regulatorischen Vorgaben sind der „Pull"-Faktor im Vergleich zum „Push"-Faktor in Form der Large Scale Pilotes. Die Altersverifikation spielt dabei aus meiner Sicht nur eine untergeordnete Rolle.

Herr Doujak, danke für das Gespräch.

(kki@ix.de)

Quellen

Hintergrundinformationen zum Open Banking Project und den Large Scale Pilots finden sich unter ix.de/zdvn.

KORNELIUS KINDERMANN

ist iX-Redakteur und beschäftigt sich mit den Themen Cloud, Security, Compliance und E-Government.