SocietyByte
Wissenschaftsmagazin des BFH-Zentrums Digital Society
https://www.societybyte.swiss

Passwortfreie Loginverfahren als Key Player der digitalen Transformation

Autoren : Silvano Fari, Peter Egli

Datum : 10. März 2020

PSD2 und Open Banking eröffnen neue Möglichkeiten bei der digitalen Transformation des Bankkundengeschäfts. Ein vielversprechender Ansatz ist hier FIDO, das starke und zugleich benutzerfreundliche Authentisierungsmechanismen bietet. Und auf viele andere Bereiche anwendbar ist, schreiben unsere Autoren.

Die Payment Service Directive 2 (PSD2) schreibt den Banken in der EU vor, Schnittstellen für den Zugriff auf Kundenkonti anzubieten. Dies ermöglicht es Drittanbietern, neue, bankenübergreifende Services bereitzustellen. Mit dieser Öffnung der Banken hofft die EU, Anreize zu schaffen für mehr Innovation und Wettbewerb. Die Schweiz zielt mit den Open-Banking-Bestrebungen ebenfalls Richtung Öffnung. Auch wenn diese auf Selbstregulierung basiert, wird man sich den gleichen Herausforderungen wie die EU stellen müssen.

Damit Drittanbieter diese Schnittstellen verwenden dürfen, muss das Einverständnis des Kontoinhabers eingeholt werden. Der technische Regulierungsstandard (RTS), der PSD2 ergänzt, zwingt die Banken, den Kunden für solche Einwilligungen stark zu authentifizieren. Das heisst, die Authentizität wird mittels zweier voneinander unabhängiger Sicherheitsmerkmale aus den Bereichen "Wissen" (z.B. Passwort), "Besitz" (z.B. Handy) und "Inhärenz" (z.B. Fingerabdruck, Face ID) bewiesen.

Herausforderungen beim Zugriff von Dritten

Während der Kunde Kontoinformationen früher direkt bei seiner Bank abrufen musste, wird dies nun auch über Dritte (sogenannte Third-Party Providers, TPP) möglich werden. Hierbei ergeben sich neue Herausforderungen für die beteiligten Parteien, insbesondere wenn die Informationen von mehreren Banken parallel bezogen werden.

Angenommen ein Kunde möchte die Kontoinformationen seiner drei Bankbeziehungen über einen TPP verwalten. Dann müsste jede der drei Banken das Einverständnis des Kunden mittels starker Authentifizierung einholen – was sich umständlich gestalten könnte, da es bei den verschiedenen Banken heute eine Vielfalt von starken Authentisierungsmechanismen (PhotoTAN, mTAN, SecureID usw.) gibt.
Ein solches Vorgehen ist für die meisten Kunden nicht nachvollziehbar und wahrscheinlich gar inakzeptabel. Es ist deshalb davon auszugehen, dass das Bestreben, eine Angleichung in den Authentisierungsmitteln zu erreichen, mit PSD2 wachsen wird.

Standards tragen zur Vereinfachung bei

Die Verwendung von Standards und der Einsatz von Smartphones als Sicherheitstoken könnten eine Vereinfachung bringen. Ein möglicher Standard wäre FIDO (Fast Identity Online), das eine normierte Interaktion zwischen verschiedenen Authentifizierungsmechanismen bietet. Insbesondere kann FIDO auf einfache Weise etablierte Authentifizierungsverfahren auf

Smartphones (zum Beispiel Face ID, Fingerprint oder Voice) mit jenen auf der Serverseite verbinden. Der FIDO- Standard basiert auf Public-Key-Verschlüsselung. Die Serverseite, hier die Bank, kennt den öffentlichen Schlüssel des Kunden. Das Schlüsselpaar des Kunden wird auf seinem Smartphone in einem sicheren Modul (Trusted Platform Module, TPM) generiert, wobei der private Schlüssel dieses Modul nie verlässt und mittels Authenticator geschützt wird. Um den privaten Schlüssel zu verwenden, verlangt der Authenticator ein Merkmal aus dem Bereich «Wissen» oder «Inhärenz». Zusammen mit dem Besitz des Geräts wären damit die Vorgaben des RTS erfüllt. So ist auch sichergestellt, dass die Systeme der Bank keine biometrischen Informationen des Benutzers erhalten. Diese sind einzig auf dem Smartphone hinterlegt und werden vom Authenticator verwendet, um den Zugriff auf den privaten Schlüssel zu entsperren.

Wie sähe das nun im beschriebenen Szenario aus?

Wenn die betreffenden drei Banken FIDO unterstützen würden, könnte der Kunde seine Einwilligung jeweils einfach mittels Fingerabdruck, Face ID oder Voice bestätigen.

PSD2 und Open Banking eröffnen neue Möglichkeiten für die digitale Transformation des Bankkundengeschäfts. Denn benutzerfreundliche starke Authentisierungsmechanismen können Innovation in diesem Umfeld fördern. Dabei wird FIDO dank der breiten nativen Unterstützung durch die Geräteherstellerindustrie eine entscheidende Rolle spielen. Da Bankkunden zugleich auch immer Bürger eines Landes, eines Kantons und einer Gemeinde sind, liessen sich die gleichen Konzepte ohne zusätzlichen Aufwand für den Bürger wiederverwenden, um damit auf eine einfache und sichere Art den Zugang zu elektronischen Behördendienstleistungen zu gewährleisten.

Die Anwendung von Standards, die die Authentisierungsmittel von heutigen Smartphones mit einbeziehen, würde es erlauben, die Kosten für Entwicklung, Betrieb, Wartung und Support von Behörden-Portalen insgesamt zu senken. Gleichzeitig würde das Erlebnis der Bürger bei der Nutzung von Behördendienstleistungen verbessert, dies unter Einhaltung der Persönlichkeits- und Datenschutzrechte. Das müsste eigentlich auch in die Strategie "Digitale Schweiz" des Bundes passen, die den Menschen in den Mittelpunkt stellt, um ihn optimal in die Transformationsprozesse der digitalen Gesellschaft einzubinden.

Ob Bürger oder Bankkunden: Am Ende sind es dieselben Personen, die die Login-Verfahren nutzen, die ihnen die Dienstleistungsanbieter (Banken, Behörden usw.) bereitstellen. Die Implementierung des FIDO-Standards, der die Authentisierungsmittel von heutigen Smartphones unterstützt, ist ein sehr gutes Beispiel dafür, wie Dienstleister hohe Anforderungen sowohl an Sicherheit als auch an Usability mit technischer Innovation erfüllen können. Mit anderen Worten: Als Key Player der digitalen Transformation kann FIDO2.0 seine Stärken – einfach, schnell, sicher – voll ausspielen und so eine hohe Benutzerakzeptanz erzielen. Und genau diese entscheidet massgeblich darüber, ob ein Digitalisierungsprojekt erfolgreich ist.