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

User wurden bisher zu wenig berücksichtigt

Autor : Laura Kieser

Datum : 10. September 2018

Bei der eID wird der entscheidende Prozessschritt – die Bestätigung der Identität – nicht durch einen Menschen physisch getätigt, sondern elektronisch. Bei diesem Authentifizierungsmechanismus wird im Zusammenhang mit der eID oft von technischen Herausforderungen gesprochen. In der Praxis sowie in der Forschung ist jedoch klar, dass es längst nicht nur technische, sondern auch rechtliche, politische und organisatorische Herausforderungen sind.

Es ist ein System aus privatwirtschaftlichen Absichten und staatlichen Aufgaben. In diesem komplexen interdisziplinären Konstrukt aus verschiedenen Akteuren stellt sich folgende Frage: Was wünscht eigentlich der Nutzer – der Endanwender? Längst ist bewiesen, dass die Akzeptanz der Endanwender eine wichtige Rolle zum Erfolg einer Lösung auf dem Markt beitragen. Anhand eines renommierten Models aus der Forschung wurde analysiert, welche Faktoren eine Rolle spielen, damit eine Lösung von Endanwendern akzeptiert wird. Dabei wurde festgestellt, dass bei Lösungen wie der eID Vertrauensfaktoren ganz oben stehen. Basierend auf diesen Erkenntnissen wurden Empfehlungen für Entscheidungsträger im eID Ökosystem abgeleitet.

Identität hat grundsätzlich zwei Bedeutungen. Im Sinne der Zusammengehörigkeit sowie auch im Sinne der Abgrenzung. Diskussionen zu «Identität» gehen weit zurück in der Philosophie- und Sozialgeschichte. Sie wurden damals und werden bis heute als kompliziert, interdisziplinär und polarisierend angesehen. Bei einer elektronischen Identität werden die Definition und die Verständlichkeit zusätzlich abstrakter. Das bereits interdisziplinäre Thema wird durch das technische Umfeld erweitert.

Die Voranalyse der Masterarbeit "End-User Acceptance of Electronic Identity" hat ergeben, dass in verschiedenen laufenden Vorhaben, in unterschiedlichen Staaten, zur Einführung einer eID die Endanwender bis jetzt wenig bis nie im Mittelpunkt waren. Dabei ist es heutzutage unbestritten, dass die Akzeptanz seitens Endanwender den Erfolg des Produktes stark beeinflussen. Deshalb standen im Rahmen einer These die Endanwender einer eID im Vordergrund.

Methode

In einem ersten Schritt wurde anhand von Interviews analysiert, was Endanwender dazu bewegt, eine eID zu akzeptieren. Mit Hilfe des Technologieakzeptanzmodels (Unified Theory of Acceptance and Use of Technology, UTAUT) und verschiedenen Methoden wurde mit einem qualitativen Ansatz evaluiert, welche Erwartungen Endanwender an eine eID haben. Zentral dabei waren vorgegebene Aspekte aus dem Model wie: Welche Leistung Endanwender erwarten, welcher Aufwand sie bereit sind einzugehen, welche Rolle der soziale Einfluss spielt und welche Form von Anwenderunterstützung erwartet wird. Zudem wurde das Profil des Endanwenders aufgenommen. Dazu gehörten Informationen zu Alter, Berufstätigkeit, Ausbildung, sowie eine Selbsteinschätzung der IT-Affinität.

Im zweiten und abschliessendem Schritt wurden Empfehlungen für die Förderung der Endanwenderakzeptanz, abgeleitet. Anhand weiterer Interviews wurden die Empfehlungen von drei Experten validiert. Die ausgewählten Experten haben verschiedene Hintergründe und haben deshalb unterschiedliche Perspektiven vertreten: Die Sicht des *Service Providers*, die Sicht des *Identity Providers* sowie die Sicht des Bundes. Die Empfehlungen richten sich an Entscheidungsträger im eID Ökosystem.

Akzeptanzfaktoren

Die Interviews mit potentiellen Endanwendern hat folgendes ergeben:

1. Das Hauptanliegen der Endanwender ist, dass eine eID gegenüber den bestehenden Lösungen einen Mehrwert erbringen soll, damit man als Endanwender diese auch benützt. Dabei werden die heutigen elektronischen Identifikationslösungen, wie zum Beispiel eBanking als leistungsstark bezeichnet und mit angemessenem Aufwand in Verbindung gebracht.
2. Die Endanwender vertrauen in der Regel ihrer eBanking-Lösung und fühlen sich sicher. Das Argument, dass die eID Sicherheit bringt, wurde deshalb nicht per se als «Mehrwert» resp. als Alleinstellungsmerkmal (USP) sondern eher als selbstverständlich

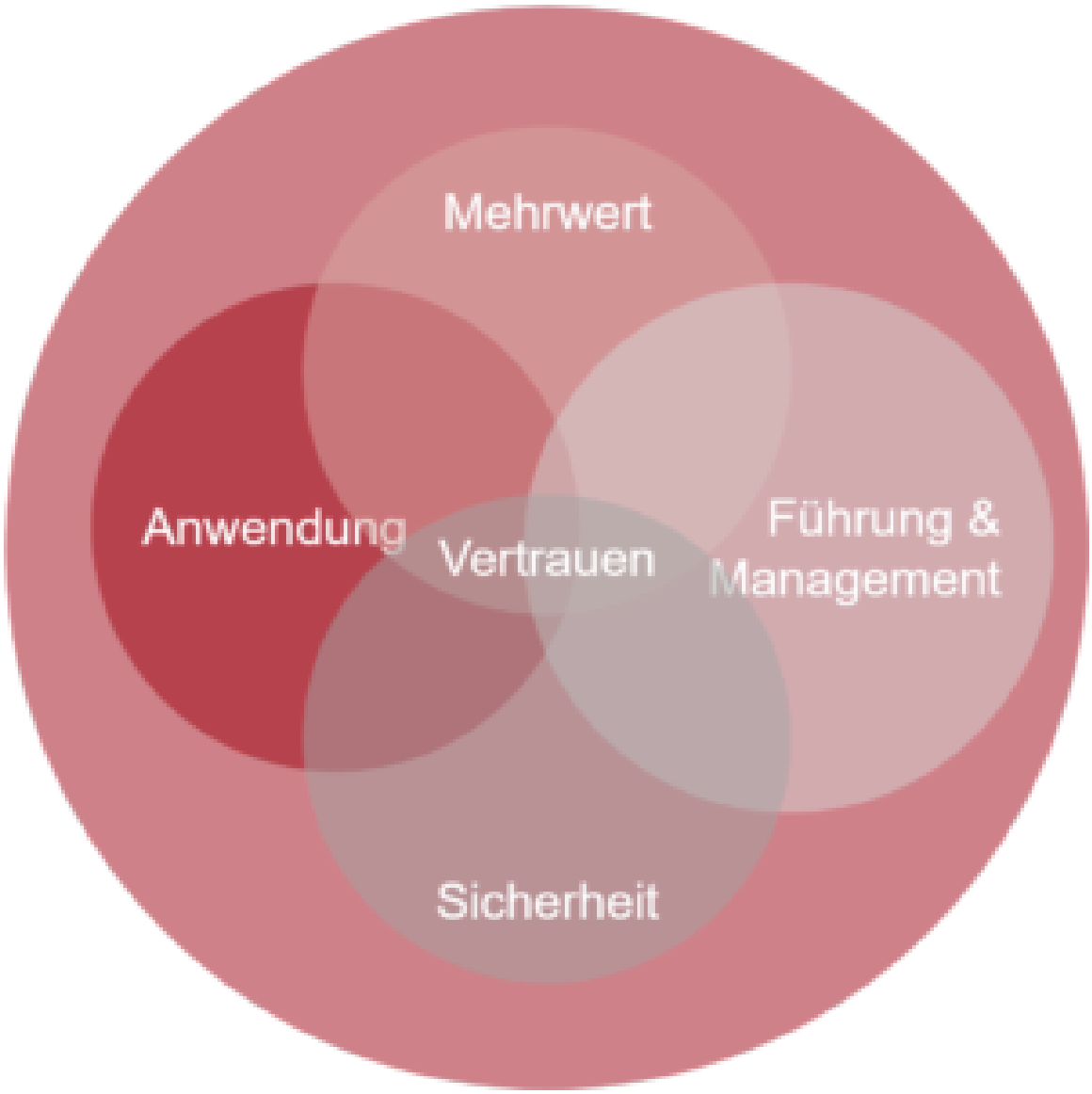
angesehen.
3. Der soziale Einfluss spielt eine grosse Rolle – auch aufgrund der empfundenen «Abstraktheit». Alle Befragten, unabhängig davon wie gut sie ihre IT-Kenntnisse einschätzten oder wieviel Berufserfahrung sie hatten, bestätigten, dass sie sich in den Medien, direkt beim Anbieter, bei Freunden, Berufskollegen oder direkt bei Informationsquellen des Bundes über die eID Lösung informieren und Meinungen einholen.
4. Es wurde zudem betont, dass die Lösung vertrauenswürdig sein muss. Es stellte sich dabei heraus, dass Vertrauen ein übergeordneter Aspekt ist. Dies bedeutet, wenn Vertrauen einmal aufgebaut ist, kann es auch trotz möglicher Sicherheitslücken zu einer langfristigen Endanwenderakzeptanz führen. Vertrauen muss in einem Zusammenspiel zwischen allen staatlichen oder privaten Akteuren im gesamten eID Ökosystem an die Endanwender übermittelt werden.

Diese letzten Erkenntnisse bezüglich Vertrauensaspekte sind in diesem Sinne nicht neu. Einen Blick auf die Praxis zeigt, dass die Post CH AG zusammen mit SwissSign Group AG den ersten Schritt gewagt hat. Die Post CH AG hat 2017 entschieden, das Kundenlogin Post abzulösen und dafür eine externe Lösung einzusetzen. Mit SwissID sind die Voraussetzungen für einen zukünftigen Mehrwert gegeben: Eine elektronische Identifikation, welche in verschiedenen Situationen für unterschiedliche Zwecke angewendet werden kann. Die Anbindung dieser Lösung hat aus organisatorischer und technischer Sicht gut funktioniert. Die Kunden der Post haben jedoch ein grosses Bedürfnis, detailliert über diese Lösung aufgeklärt zu werden. Das Thema digitale Identität birgt noch viel Unsicherheit, da es sich um sensible Daten handelt.

Auf der einen Seite braucht es ein grosses eID Ökosystem mit vielen Endanwendern und vielen Service Providern, damit die Lösung an Akzeptanz und Vertrauen gewinnt. Auf der anderen Seite gibt es jedoch viele Endnutzer und *Service Provider*, die abwarten möchten und dieser neuen Lösung noch nicht vertrauen. Beide Seiten verfügen über berechtigte Argumente. Diese Huhn-Ei Situation macht das Vorhaben an sich zusätzlich komplexer.

Empfehlungen

Wie kann nun Vertrauen geschaffen werden und somit eine Endanwenderakzeptanz erzielt werden? Basierend auf den identifizierten Erwartungen und eingeholten Informationen der Endanwender wurden Empfehlungen definiert und validiert. Die Empfehlungen wurden in fünf Kategorien unterteilt. Die Kategorie «Vertrauen» ist ein übergeordneter Aspekt, welcher in allen Empfehlungen und in allen Situationen einfliessen soll.



VERTRAUEN	**1.**	Vertrauen muss in einem Zusammenspiel auf allen Ebenen und alle Akteuren im ganzen eID Ökosystem aufgebaut werden.
	2.	Vertrauen wird durch den Staat sowie von den Medien, Forschung u Privatwirtschaft erzeugt.
	3.	Vertrauen wird durch positive Erfahrungen der Endanwender stark g

MEHRWERT	**1.**	Eine eID soll verschiedene Anwendungsfälle und verschiedene Zug ermöglichen.
	2.	Eine eID soll gleich anerkannt sein wie der physische offizielle Pass können Prozesse ersetzt werden, welche heute eine physische Ers voraussetzen.

	3.	eID Anwendungsfälle, welche genau diese physische Erscheinung sollten als erstes auf dem Markt etabliert werden.
	Stossrichtung	Dies betrifft beispielsweise die Versicherungsindustrie oder staatlic Dienste (eGovernment).
FÜHRUNG & MANAGEMENT	**1.**	Der Bund muss als Vertrauensanker agieren.
	Stossrichtung	Der Bund zertifiziert Anbieter in der Privatwirtschaft. Die Bedeutung Zertifizierung wird von Endanwendern sofort erkannt und verstande
	2.	Die Rolle des Bundes und der Privatwirtschaft muss klar definiert s transparent kommuniziert werden.
	Stossrichtung	Die Rolle des Bundes beinhaltet zwei Aufgaben: Die Führung und Überwachung der eID sowie auch das Aufbauen von Anwendungsf eGovernment-Bereich, damit Mehrwert entsteht.
	3.	Mögliche private eID Anbieter müssen Endkunden-Loyalität erzeug indem transparente Kommunikation bezüglich Datenmanagement u Bewahrung der Privatsphäre eingehalten wird.
	Stossrichtung	Es gibt bereits eID Lösungen auf dem Markt. Die Anbieter sollen pr Kampagnen lancieren und die Absicht erklären innerhalb der gegeb rechtlichen Grundlagen.
ANWENDUNG	**1.**	Der Authentifizierungsprozess soll die bestmögliche Performanz au während gleichzeitig Sicherheitsaspekte eingehalten werden.
	2.	Die Prozesse sollten auf den Prinzipien der Kundenführung aufgeb werden (*User Experience*).
	Stossrichtung	Falls es während dem Prozess zwischen verschiedenen Anbietern Absprünge gibt (zum Beispiel zwischen *Service Provider* und *Ident Provid*er), muss der Kunde verstehen, weshalb und wo genau er si befindet.
	3.	Es sollen, nebst Anmeldedaten wie Benutzername, Passwort und Z Faktor-Authentifizierung, zusätzliche neue bzw. zeitgemässe und s Identifizierungsmechanismen angeboten werden.
	Stossrichtung	Aufgrund der schnell wechselnden Technologie und daraus resultie Möglichkeiten, sollten zukünftige Identifizierungsmöglichkeiten früh erkennt und entwickelt werden. Dazu gehören auch biometrische D Gesichtserkennung, Stimmerkennung oder Fingerabdrücke.

SICHERHEIT	**1.**	Persönliche Daten müssen verschlüsselt und sicher in der Schweiz aufbewahrt werden.
	2.	Im technologischem Sinne müssen stets die höchsten Sicherheitss angewendet werden und diese müssen konstant gewartet bzw. aus werden.
	3.	Endanwender sollen nicht bei jedem Authentifizierungsprozess ihre kompletten Identitätsdaten ausgeben müssen.
	Stossrichtung	Falls ein Endanwender die höchste Authentifizierungsstufe erreicht Assurance), werden die untergeordneten Stufen zwar obsolet, es b jedoch nicht, dass Prozesse, beispielsweise für Onlineshopping komplizierter werden. Der Endanwender liefert je nach Anwendung (Risikostufe) verschiedene Identitätsdaten.

Fazit

In Bezug auf Vertrauen ist die Haupterkenntnis aus der Analyse mit Endanwendern und Experten, dass Vertrauen nicht nur ein technologischer oder sicherheitsspezifischer Aspekt ist. Vertrauen hat stark damit zu tun, welche Reputation eine Lösung auf dem Markt hat. Dabei geht es in diesem interdisziplinären Umfeld um viel mehr als eine technologisch sichere Umsetzung.

Referenz

Laura Kieser, "End-User Acceptance of Electronic Identity", Olten, 2018.