Arbeitsstand Ideensammlung | Mai 2023

Mögliche Ansatzpunkte zur Anpassung von technischen eID-Richtlinien und der Personalausweisverordnung anhand von Beobachtungspunkten der User-Journey mit der eID

Dies ist ein Arbeitsstand aus der Pilotphase der BundesIdent App. Die übergreifende Zielsetzung der Ideen ist, das Nutzungserlebnis (UX) mit der eID wesentlich zu verbessern. Dazu schlagen wir vor, bestehende Entscheidungen zu hinterfragen und offen über mögliche Änderungen zu diskutieren.

Hinweis

Einer Ideensammlung wie dieser wohnt inne, dass die meisten Ideen wohl an der weiteren Validierung der Nutzerbedarfe, Sinnhaftigkeit oder Machbarkeit scheitern werden. Deshalb ist diese Sammlung von UX-Hürden und Ideen als Gedankenanstoß gedacht.

Vorgehen

Die meisten Hürden und Ideen sind aus der Pilotphase der BundesIdent App entstanden, welche qualitative wie quantitative Nutzungsdaten generiert hat. Regelmäßige Tests mit Nutzenden sowie technische Explorationen haben diese Erkenntnisse ergänzt.

Legende

⚡ : Hürden

💡 : erste Ideen, die weiter zu validieren sind

Erhalt des PIN-Briefes

- ⚡ Nutzende erhalten einen neuen Ausweis und richten diesen jedoch nicht direkt ein beziehungsweise nutzen ihn nicht direkt.
- ⚡ Nutzende bringen den PIN-Brief nicht in Verbindung mit dem Ausweis, den sie physisch im Bürgerbüro erhalten.
- 💡 Den Prozess in den Bürgerbüros analysieren und gegebenenfalls anpassen.
  - PIN direkt im Bürgeramt setzen und/oder einen Service vor Ort nutzen.
  - Hilfestellung für Nutzende anbieten, die nicht digitalaffin sind.
- 💡 Den zeitlichen Abstand und somit den Bruch zwischen Erhalt des Ausweises und Erhalt des PIN-Briefes eliminieren.

PIN vergessen

Relevante technische Richtlinien und Verordnung: BSI TR-03124 eID-Client, TR-03128 Teil 3 & PAuswV

- ⚡ Nutzende erwarten bei der Funktion einer PIN-Rücksetzung das gleiche Nutzungserlebnis wie bei einer gewöhnlichen „Passwort vergessen“-Funktion. Der PIN-Rücksetzdienst sowie der CAN- und PUK-Flow erfüllt diese Erwartungen nicht.
- ⚡ **User-Flow über mehrere Produkte, Medien oder Anbieter** kann verwirren:
  - Der PIN-Rücksetzbrief leitet auf die Website, von der aus wiederum in die App weitergeleitet wird, in der die PIN eingegeben werden muss.
  - Führung der Nutzenden über die externe Domain der Bundesdruckerei ist vorgeschrieben, da BDR als Anbieter des Dienstes festgelegt §7 PAuswG [4] (3a) ist. Zudem ist die Umsetzung in Form einer Website festgeschrieben.
- ⚡ Die Kommunikation rund um den Aktivierungscode sowie eine neue PIN ist verwirrend.
- ⚡ Briefversand verhindert Servicenutzung in einem konkreten Moment und erhöht die Abbruchquote stark. Der Briefversand ist deshalb eine UX-Hürde.

    - Zustellung des PIN-Rücksetzbriefes nach Überprüfung der Identitätsangaben durch Vorlage des Personalausweises vorgeschrieben, PAuswV [6] Neusetzen der PIN in §20 (2).
- 💡 Quick Fix: PIN-Rücksetzbrief direkt aus der App beantragen, ohne Wechsel zur Website.
- 💡 Alternativen für eine digitale PIN-Rücksetzung explorieren.

Transport-PIN vs. persönliche Ausweis-PIN

Relevante technische Richtlinie: BSI TR-03124 eID-Client

- ⚡ Nutzende verstehen den Unterschied zwischen einer fünfstelligen Transport-PIN und der sechsstelligen persönlichen Ausweis-PIN nicht. Nutzende verstehen nicht, dass die Einrichtung vom Ausweis abhängig ist und nicht vom Gerät (so kennen sie es von Banking-Apps).
- ⚡ Nutzende verstehen daher nicht, dass die fünfstellige Transport-PIN nach einmaliger Eingabe verfällt. Nutzende geben die bereits verwendete Transport-PIN erneut ein, weil sie denken, sie müssen den Ausweis auf dem Gerät nochmals einrichten. Das technische Framework wiederum kann nicht feststellen, ob ein Ausweis bereits eingerichtet wurde. Dies führt dann zu einer Sperrung.
- ⚡ Wir Es wird komplett den Nutzenden überlassen zu verstehen, ob sie den Ausweis bereits eingerichtet haben. Das führt dazu, dass sie gefragt werden müssen, ob sie eine fünf- oder sechsstellige PIN haben. Wenn Nutzende jetzt im CAN-Szenario landen, müssen diese wieder eine neue sechsstellige Nummer eingeben. Im schlimmsten Fall auch noch die zehnstellige PUK, da nur diese die erneute sechsstellige PIN-Eingabe freischaltet. Das stresst und frustriert die Nutzenden, da die Situationen, in denen sie sich ausweisen müssen, meistens dringend sind (Führungszeugnis, Grundsteuererklärung).
- 💡 Dem Framework die Möglichkeit geben, eigenständig zu erkennen, ob ein Ausweis bereits eingerichtet ist. So wird verhindert, dass ein Ausweis fälschlicherweise gesperrt wird.
- 💡 Anwendung der CAN hinterfragen beim Anwendungsfall, dass jemand seinen PIN tatsächlich vergessen hat. Hier kann auch ein direkter Link zum PIN-Rücksetzdienst hilfreich sein.
- 💡 Der Aufbau der CAN sollte sich von der persönlichen PIN unterscheiden bzw. die CAN auf dem Ausweis könnte z. B. mit einem Label versehen werden, um Verwirrung zu vermeiden.

Scannen des Ausweises

- ⚡ Das Scannen des Personalausweises ist eine neue Erfahrung für die Nutzenden. Es ist daher ein natürliches Verhalten, den Ausweis hin und wieder vom Smartphone wegzubewegen. Doch wenn der Ausweis während des Scanvorgangs entfernt wird, meldet das Framework eine Fehlermeldung. Der Scanvorgang kann weder automatisch noch direkt in der App erneut gestartet werden. Nutzende müssen die Identifizierung jetzt erneut beim Diensteanbieter starten. Dieser Medienbruch führt zu Verwirrung.
- 💡 Das Framework erlaubt bei einer Fehlermeldung den Scanvorgang automatisch bzw. direkt in der App auf dem Smartphone erneut zu starten.

Gerätewechsel zwischen Desktop/Tablet zu Smartphone

Relevante technische Richtlinie: TR-03112-6 - eCard-API-Framework

- ⚡ Die Gerätekopplung der aktuellen Desktop-Version der AusweisApp2 (AA2) mit der mobilen Version der AA2 stellt eine sichere, jedoch schwierig zu nutzende Lösung dar, die sich nicht etablieren konnte. Beispiele für UX-Hürden: Beide Versionen der App müssen installiert sein, die Geräte müssen sich im gleichen WLAN befinden und die Kopplung als Vorgang selbst.
- ⚡ Aus der Privatwirtschaft sind die Nutzenden einfache Flows für den Gerätewechsel gewohnt, die jedoch häufig mit nicht mitigierten Risiken des Phishings einhergehen. Private Diensteanbieter nutzen zum Beispiel einen QR-Code für den Gerätewechsel, jedoch ohne weitere Sicherheitsmaßnahmen.
- 💡 Für die Erarbeitung eines sicheren sowie nutzungsfreundlichen Gerätewechsels schlagen wir die Erprobung neuster Sicherheitsstandards wie WebAuthN oder auch die geräteübergreifende Identifizierung mit Hilfe eines Nutzerkontos wie der BundID vor. Erste Explorationen dazu wurden veröffentlicht.