Fraunhofer AISEC

Fraunhofer-Institut für Angewandte und Integrierte Sicherheit AISEC

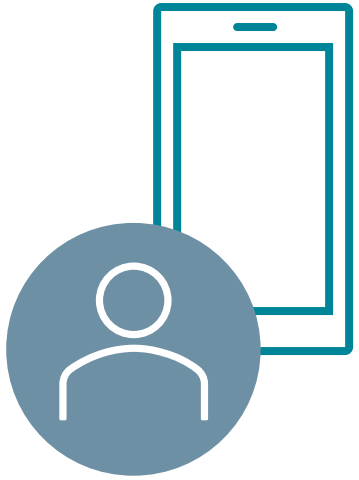
OMNISECURE - Sandra Kostic

23. Mai 2023

Digitalisierung und Vertrauen

Usability und Usable Security

Der Vergleich



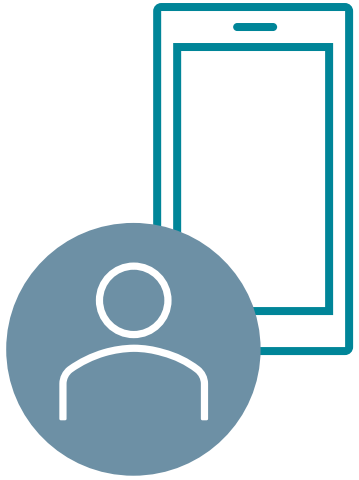
Usability

- Ziele mit minimalem Aufwand oder Frustration erreichen
- System soll intuitiv, effizient und einfach zu bedienen sein, unabhängig vom Kenntnisstand der Nutzenden
- Barrierefreier Einsatz

konzentriert sich auf die Benutzerfreundlichkeit (z.B. einfache Nutzung und schnelle Handhabung)

Usability und Usable Security

Der Vergleich



Usability

- Ziele mit minimalem Aufwand oder Frustration erreichen
- System soll intuitiv, effizient und einfach zu bedienen sein, unabhängig vom Kenntnisstand der Nutzenden
- Barrierefreier Einsatz

konzentriert sich auf die Benutzerfreundlichkeit (z.B. einfache Nutzung und schnelle Handhabung)

Usable Security

- Sicherheit bieten, ohne die Benutzerfreundlichkeit zu beeinträchtigen
- Nutzende sollen sicherheitsrelevante Aufgaben ohne Verwirrung oder Fehler ausführen können

Gleichgewicht zwischen Sicherheit und Benutzerfreundlichkeit

Wie wird eine gute Benutzbare Sicherheit erreicht

Drei Designprinzipien

Frühe Einbeziehung der Nutzenden

- Bereits bei Entwicklung des Konzept der Anwendung
- Aufnahme der Anforderung der Nutzenden (z.B. Berücksichtigung von unterschiedlichem Vorwissen und Technologieerfahrungen)

Wie wird eine gute Benutzbare Sicherheit erreicht

Drei Designprinzipien

Frühe Einbeziehung der Nutzenden

- Bereits bei Entwicklung des Konzept der Anwendung
- Aufnahme der Anforderung der Nutzenden (z.B. Berücksichtigung von unterschiedlichem Vorwissen und Technologieerfahrungen)

Studien durchführen und das Verhalten von echten Nutzenden evaluieren

- Im besten Fall mit Nutzenden aus der Zielgruppe
- Durchführung von Interview, Umfragen oder Vertestung von Mockups / Klickdummies

Wie wird eine gute Benutzbare Sicherheit erreicht

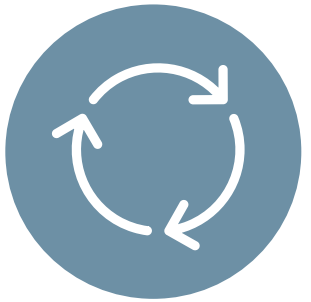
Drei Designprinzipien

Frühe Einbeziehung der Nutzenden

- Bereits bei Entwicklung des Konzept der Anwendung
- Aufnahme der Anforderung der Nutzenden (z.B. Berücksichtigung von unterschiedlichem Vorwissen und Technologieerfahrungen)

Studien durchführen und das Verhalten von echten Nutzenden evaluieren

- Im besten Fall mit Nutzenden aus der Zielgruppe
- Durchführung von Interview, Umfragen oder Vertestung von Mockups / Klickdummies



Interative Methoden nutzen

- Wiederholte Überarbeitung eines Mockups des Produktes mit Hilfe von Feedback der Nutzenden

Wallet Klick-Dummy

Aktuelle Recherchen

Fraunhofer AISEC

Übersicht zur Studie

Konzept der Wallet

Zusammenfassung

- Insgesamt ca. 60 Personen mit Hilfe von qualitativen Interviews befragt
  - Altersverteilung zwischen18-56 Jahren
  - Gleichverteilt zwischen Alter und Geschlecht

Vorgang der Studie

- Die Personen erhielten den interaktiven Prototyp und wurden bei der Verwendung des Prototyps beobachtet
- Ihnen wurden Aufgaben gestellt, die sie mit dem Prototyp lösen sollten
  - die Wallet einrichten, IDs erstellen, sich bei einem Dienst identifizieren lassen
- Am Ende wurde ein Interview durchgeführt, um die Akzeptanz und das Vertrauen in die App zu ermitteln

Aktuelle Ergebnisse und Herausforderungen
bei digitalen Identitäten

Transparenz

- Nutzende wollen sehen, welche Daten sie mit wem teilen
  - Weniger Bedenken bei den Personalausweis-Daten, weil der Ausweis immer sichtbar bei verschiedenen Diensten gezeigt wird
  - Größere Bedenken beim Digitalisieren von Bezahldaten oder Gesundheitsdaten

- **Nutzende wollen wissen, wer der Anbieter des Dienstes ist**
  - Äußerst relevant für das *Vertrauen in die Anwendung*, besonders bei sensiblen Daten
    - Ist es ein deutscher Anbieter?
    - Sind die Server in Deutschland?
    - Gilt die DSGVO?
    - *Ist der Staat involviert?*

Studienergebnisse

Vertrauen in digitale Identitäten

Studie aus 2020

16 von 16 vertrauten dem Konzept

9 Personen Betreiber sollte der Staat sein

7 Personen Betreiber sollte ein Unternehmen sein

5 Personen Betreiber **muss** der Staat sein, sonst kein Vertrauen

3 Personen Betreiber **muss** ein Unternehmen sein, sonst kein Vertrauen

Studienergebnisse

Vertrauen in digitale Identitäten

Studie aus 2020

16 von 16 vertrauten dem Konzept

- 9 Personen Betreiber sollte der Staat sein
  - 5 Personen Betreiber **muss** der Staat sein, sonst kein Vertrauen
- 7 Personen Betreiber sollte ein Unternehmen sein
  - 3 Personen Betreiber **muss** ein Unternehmen sein, sonst kein Vertrauen

Studie aus 2022

12 von 12 vertrauten dem Konzept

- 11 Personen Betreiber sollte der Staat sein
- 1 Personen Betreiber sollte der ein Unternehmen sein

Studienergebnisse

Vertrauen in digitale Identitäten

- Nutzerstudie aus 2020 exakt wiederholen

Studienergebnisse

Vertrauen in digitale Identitäten

- Nutzerstudie aus 2020 exakt wiederholen

Studie aus November 2022

16 von 16 vertrauten dem Konzept

13 Personen Betreiber sollte der Staat sein

3 Personen Staat hat Leitung + Unternehmen

3 Personen Betreiber sollte ein Unternehmen sein

1 Personen Unternehmen hat Leitung + Staat

Ideen
Einbindung der Zivilgesellschaft

Vorschläge

- Einbindung von Vertretern aus der Zivilgesellschaft
- Einbindung von interessierten Parteien
- Plattform zum Austausch für Fragen und Anmerkungen
  - Schafft Transparenz
  - Liefert Ideen und Möglichkeiten zur Verbesserung
  - Einzelstimmen wird Gehör verschafft
  - Mögliche Bedenken können früh erkannt und dediziert besprochen werden
- Software Entwicklung via Open Source
  - Unter Berücksichtigung von Standards und Best Practices

Kontakt

Sandra Kostic, M.Sc
Department Secure Systems Engineering
Team Lead Usable Security & Privacy

sandra.kostic@aisec.fraunhofer.de

Fraunhofer Institute for Applied and Integrated Security AISEC
c/o Breite Str. 12,
14199 Berlin,
Germany

Lichtenbergstraße 11
85748 Garching near Munich,
Germany

https://www.aisec.fraunhofer.de/

Fraunhofer
AISEC

Fraunhofer-Institut für Angewandte
und Integrierte Sicherheit AISEC

BACKUP

Sandra Kostic, M.Sc
Department Secure Systems Engineering
Team Lead Usable Security & Privacy

sandra.kostic@aisec.fraunhofer.de

Fraunhofer Institute for Applied and Integrated Security AISEC
c/o Breite Str. 12,
14199 Berlin,
Germany

Lichtenbergstraße 11
85748 Garching near Munich,
Germany

https://www.aisec.fraunhofer.de/

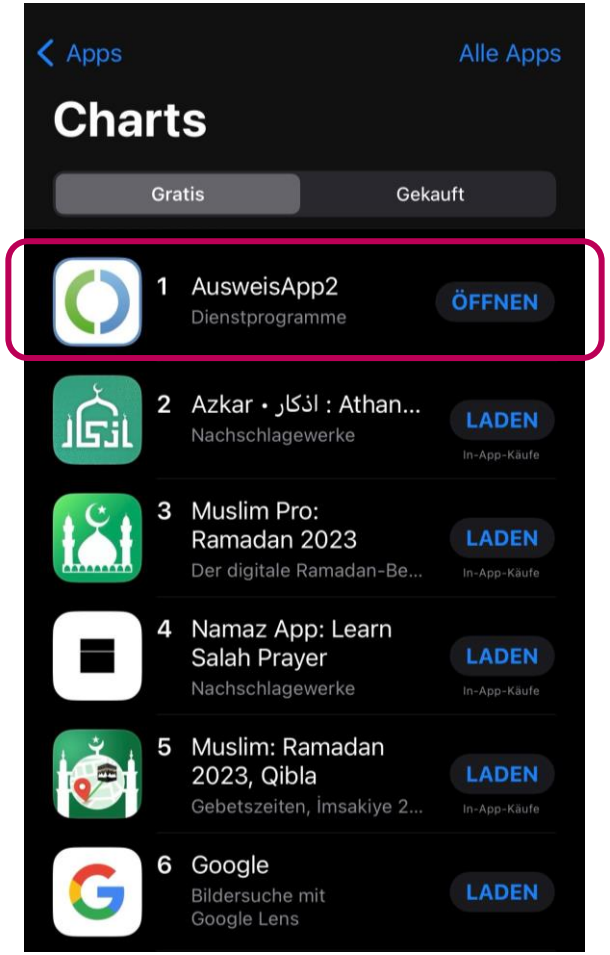
Fraunhofer
AISEC

Fraunhofer-Institut für Angewandte
und Integrierte Sicherheit AISEC

Usability von eID

Aktuelle Recherchen

1 Nutzende wollen digitale Identitäten einsetzen



Stand 23.03.2023

Usability von eID

Aktuelle Recherchen

1. Nutzende wollen digitale Identitäten einsetzen

2. Nutzende sind bereit ihre Gesundheitsdaten zu teilen

80%

of Europeans

would agree to share their health data, if privacy and security were ensured

https://www.eu2020.de/eu2020-en/eu-digitalisation-technology-sovereignty/2352828

Usability von eID

Aktuelle Recherchen

1. Nutzende wollen digitale Identitäten einsetzen
2. Nutzende sind bereit ihre Gesundheitsdaten zu teilen
3. Nutzende wollen Ihr Smartphone für digitale Identitäten verwenden

Agenda
Struktur

01 **Einführung in die Thematik Usable Security**
Definition, Vergleich zu Usability, Vorstellung von Methoden

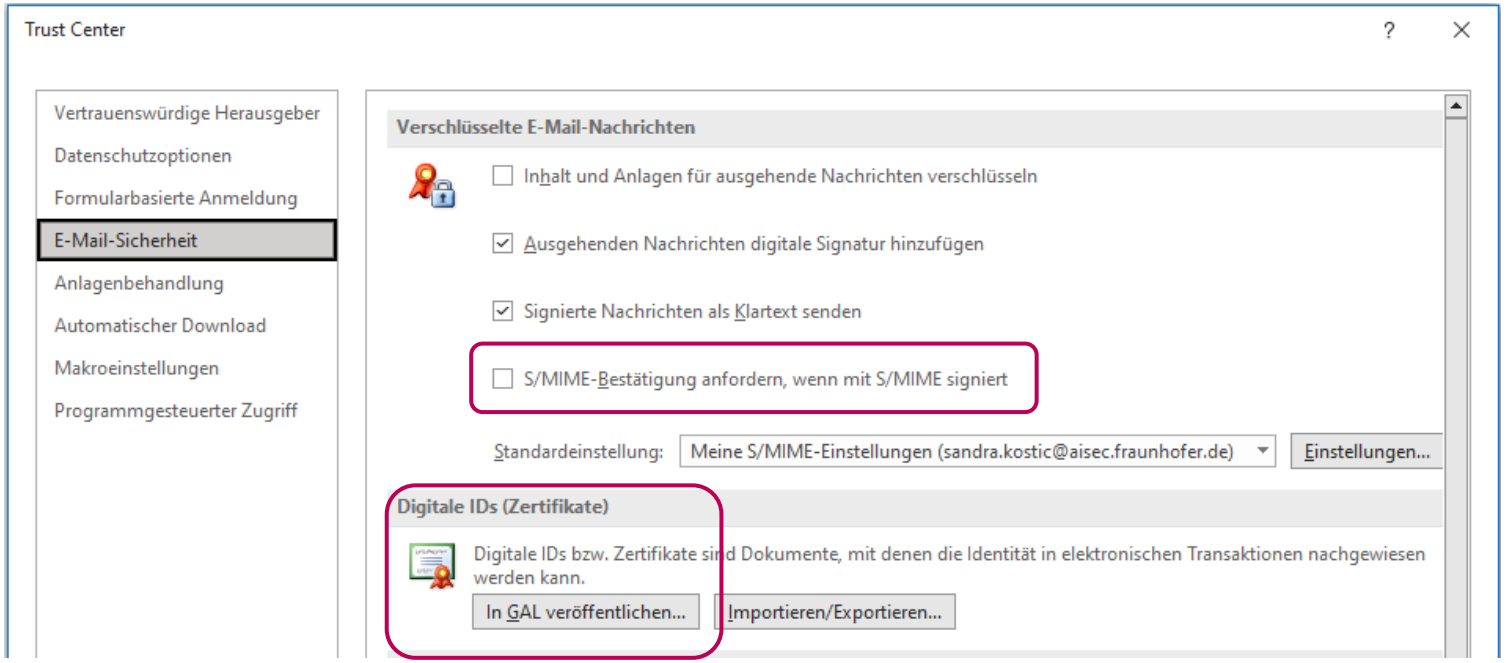
02 **Usability von eID**
Erfahrungen aus bisherigen Projekten

03 **Handlungsempfehlungen**
Beschreibung von Beispielen und Umsetzungen

04 **Einbindung der Zivilgesellschaft**
Ideen, Vorschläge und Diskussion

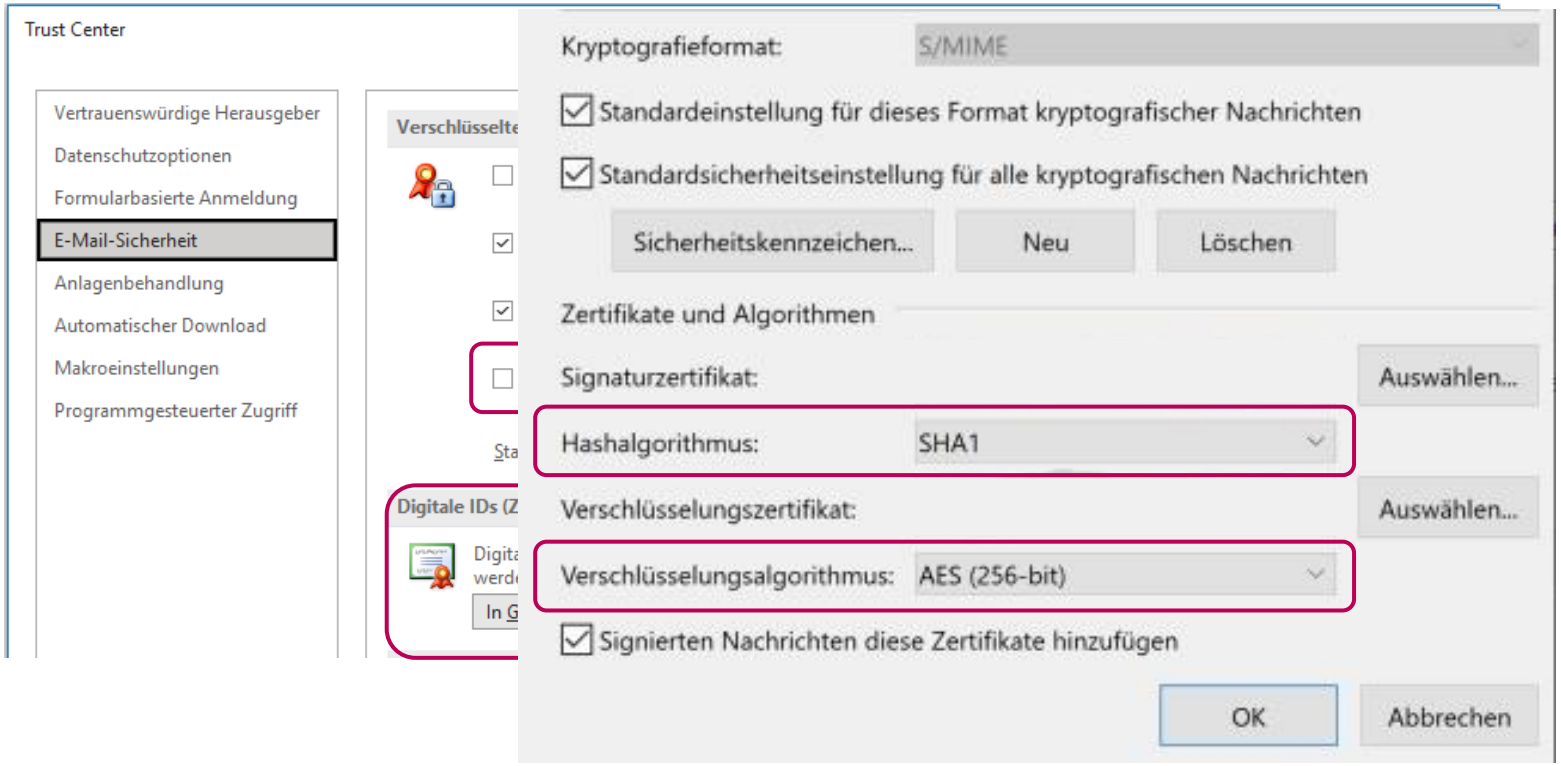
Security vs. Usability

Die Balance - ein Beispiel



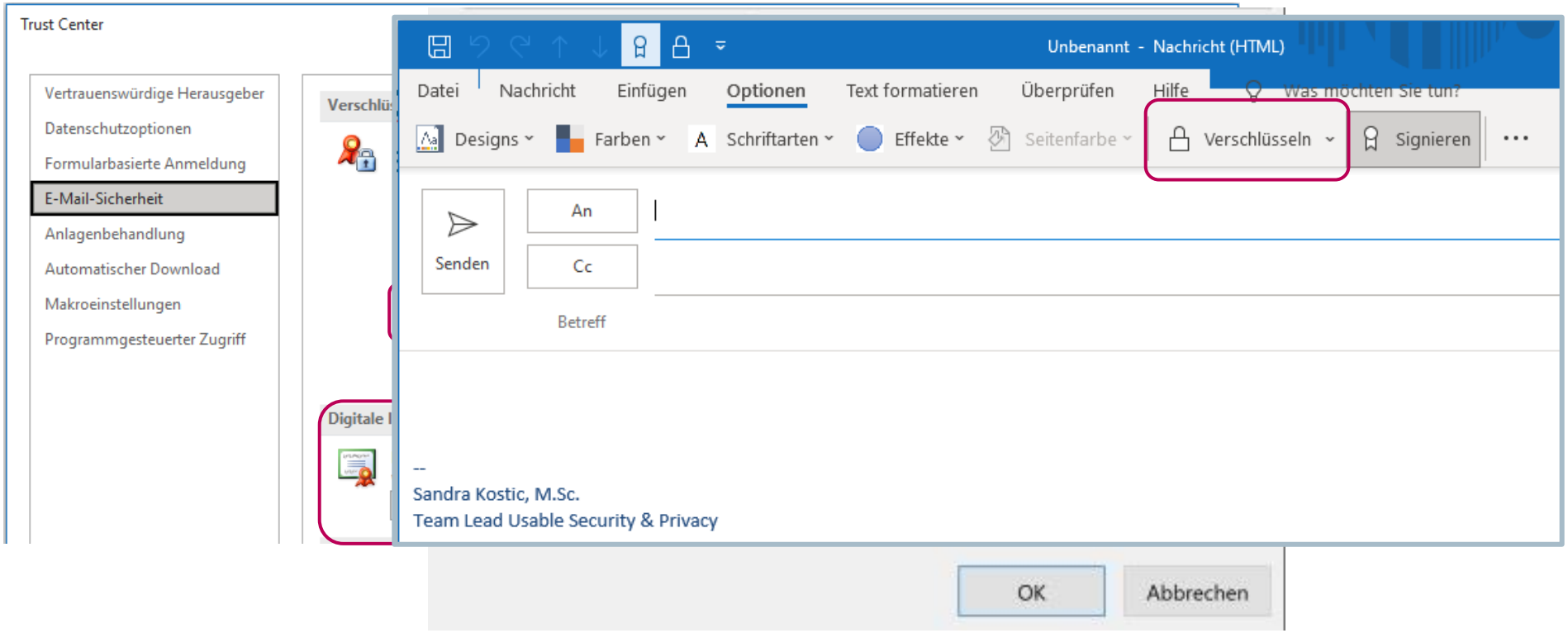
Security vs. Usability

Die Balance - ein Beispiel



Security vs. Usability

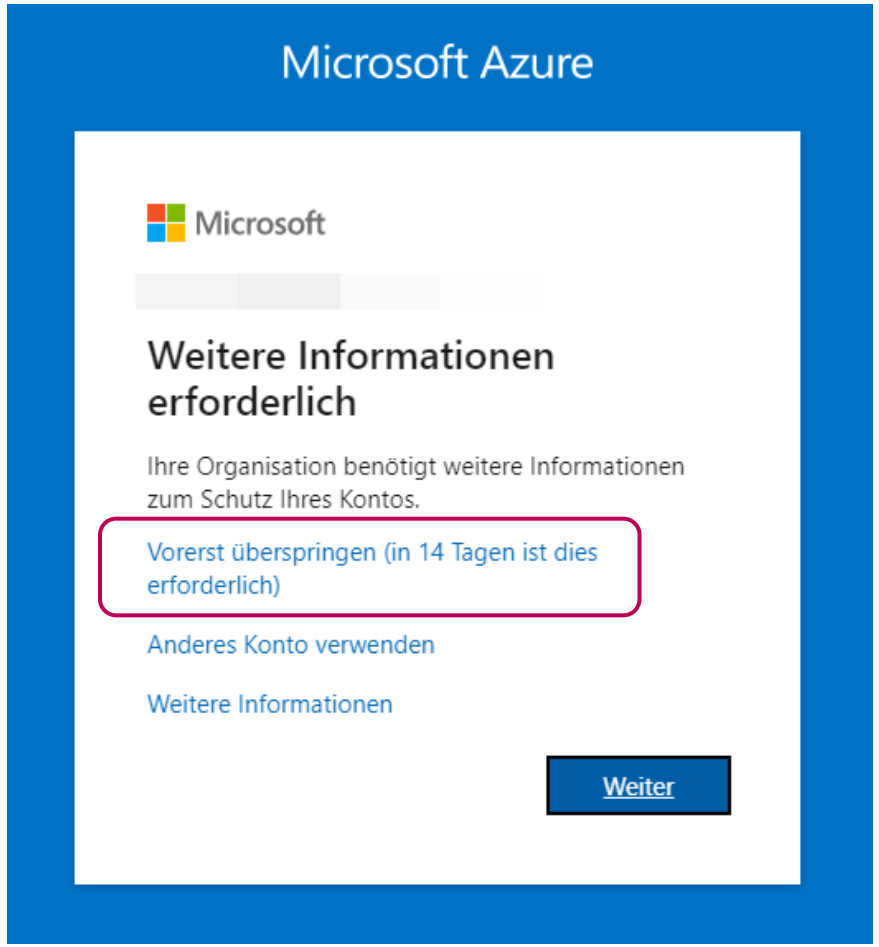
Die Balance - ein Beispiel



Fraunhofer AISEC

Security vs. Usability

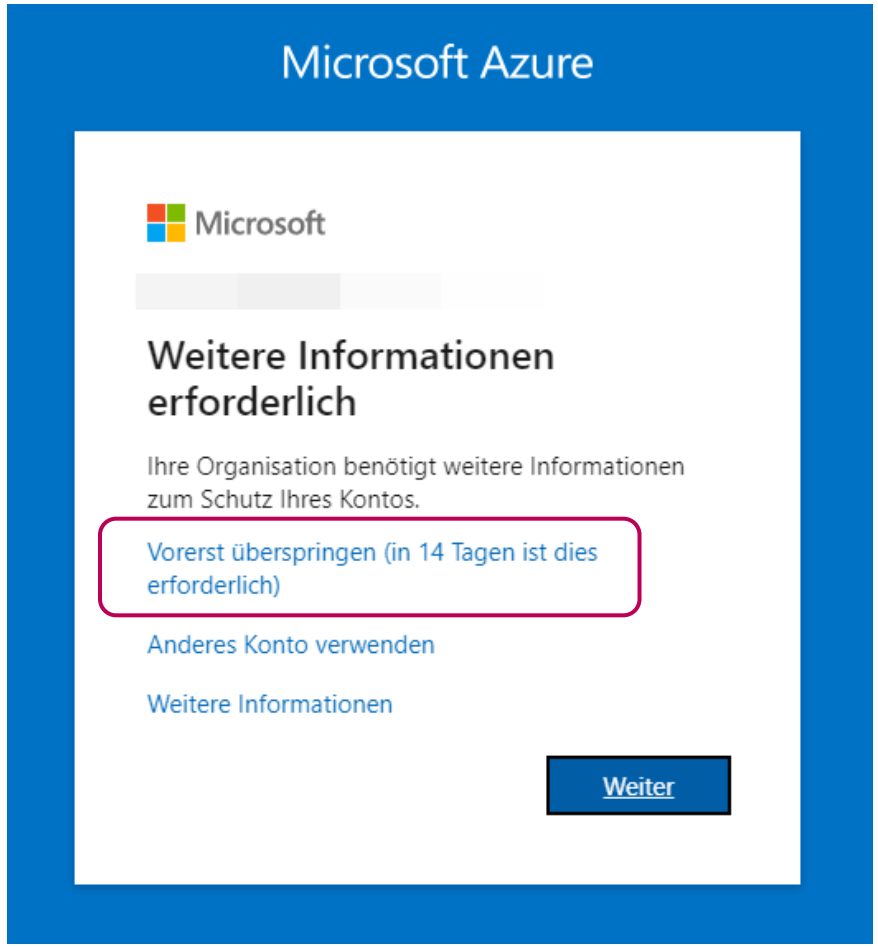
Die Balance - ein Beispiel



Quelle: zueschen.eu/microsoft-office-365-2-faktor-authentifizierung-deaktivieren-mfa-2fa/

Security vs. Usability

Die Balance - ein Beispiel



Quelle: zueschen.eu/microsoft-office-365-2-faktor-authentifizierung-deaktivieren-mfa-2fa/

Quelle: https://docplayer.net/185948437-Coupa-supplier-portal-admin-and-user-guide.html

Fraunhofer AISEC

Usable Security (Benutzbare Sicherheit)

Zusammenfassung

1. Teilt sich gemeinsame Grundsätze mit der Usability wie z. B. Einfachheit, klares Verständnis, Akzeptanz in die Anwendung und Konsistenz
2. Gestaltung der Sicherheit unter Berücksichtigung der Anforderungen an die Benutzerfreundlichkeit
3. Usability Probleme können zu kritischeren und schwerwiegenden Problemen führen

Usable Security (Benutzbare Sicherheit)

Zusammenfassung

1. Teilt sich gemeinsame Grundsätze mit der Usability wie z. B. Einfachheit, klares Verständnis, Akzeptanz in die Anwendung und Konsistenz
2. Gestaltung der Sicherheit unter Berücksichtigung der Anforderungen an die Benutzerfreundlichkeit
3. Usability Probleme können zu kritischeren und schwerwiegenden Problemen führen

Das entwickelte System soll sich immer den Anforderungen der Nutzenden anpassen!

Vorteile des nutzerzentrierten Ansatzes mit Mockups

Drei wesentliche Punkte

1 **Frühe Tests von Mockups / Klickdummies mit Nutzenden spart viel Zeit später im Projekt**

- Bedarf von Anpassungen in der Umsetzung ist gering
- Steigert die Zufriedenheit der Nutzenden

Vorteile des nutzerzentrierten Ansatzes mit Mockups

Drei wesentliche Punkte

1 **Frühe Tests von Mockups / Klickdummies mit Nutzenden spart viel Zeit später im Projekt**

- Bedarf von Anpassungen in der Umsetzung ist gering
- Steigert die Zufriedenheit der Nutzenden

2 **Ansatz zeigt auf, was umgesetzt werden muss**

- Bauplan zur Umsetzung (Bsp. Übersicht der relevanten Funktionen, Sicherheitsfeatures etc.)
- Hinweis, ob alle Funktionen beachtet wurden

Vorteile des nutzerzentrierten Ansatzes mit Mockups

Drei wesentliche Punkte

1 **Frühe Tests von Mockups / Klickdummies mit Nutzenden spart viel Zeit später im Projekt**

- Bedarf von Anpassungen in der Umsetzung ist gering
- Steigert die Zufriedenheit der Nutzenden

2 **Ansatz zeigt auf, was umgesetzt werden muss**

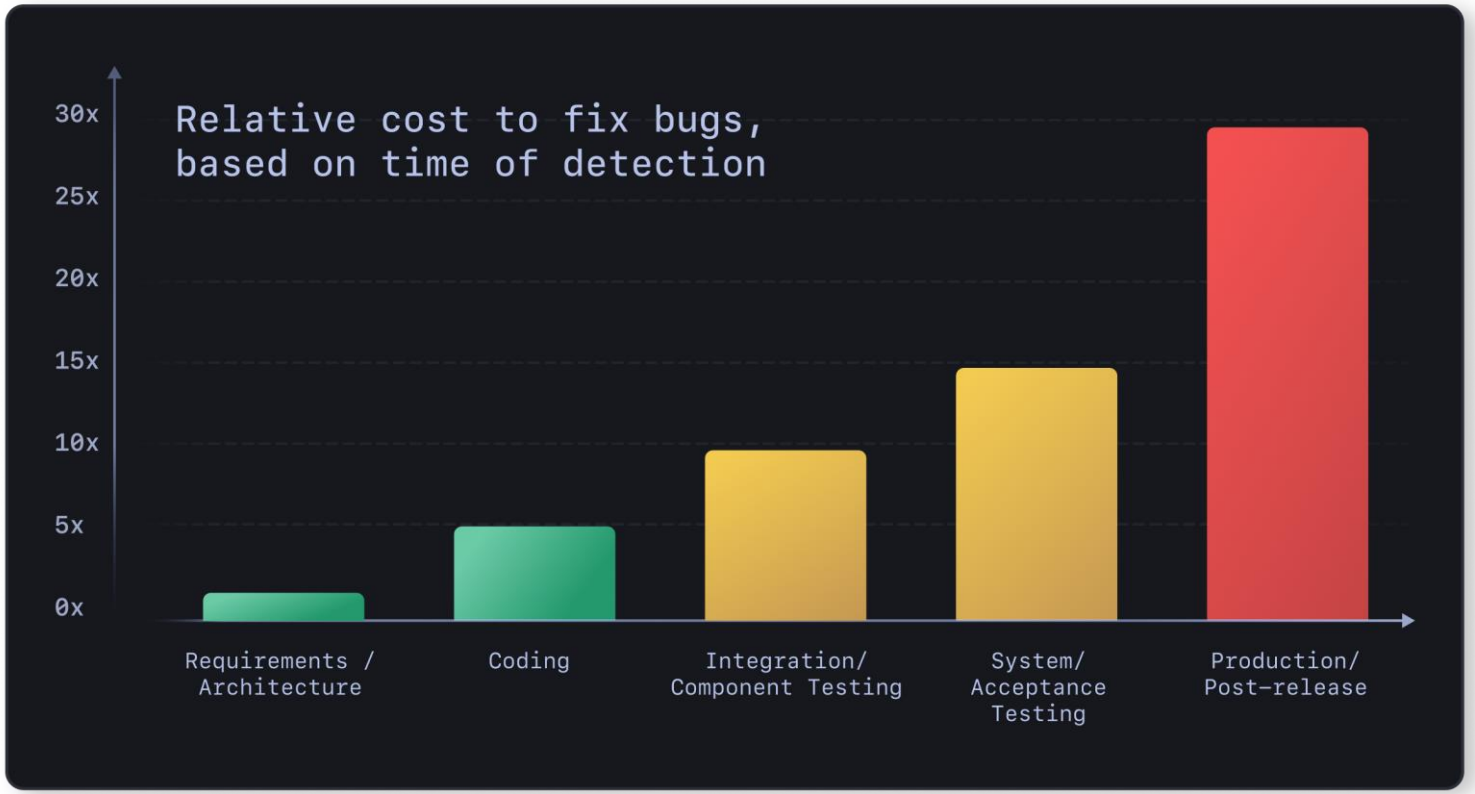
- Bauplan zur Umsetzung (Bsp. Übersicht der relevanten Funktionen, Sicherheitsfeatures etc.)
- Hinweis, ob alle Funktionen beachtet wurden

3 **Probleme können früh erkannt und behoben werden**

- Keine Frustration beim Programmierer auf Grund von komplizierten Anpassungen
- Ein Problem in einem nahezu fertigen Produkt zu beheben kann sehr teuer sein

Kostenübersicht

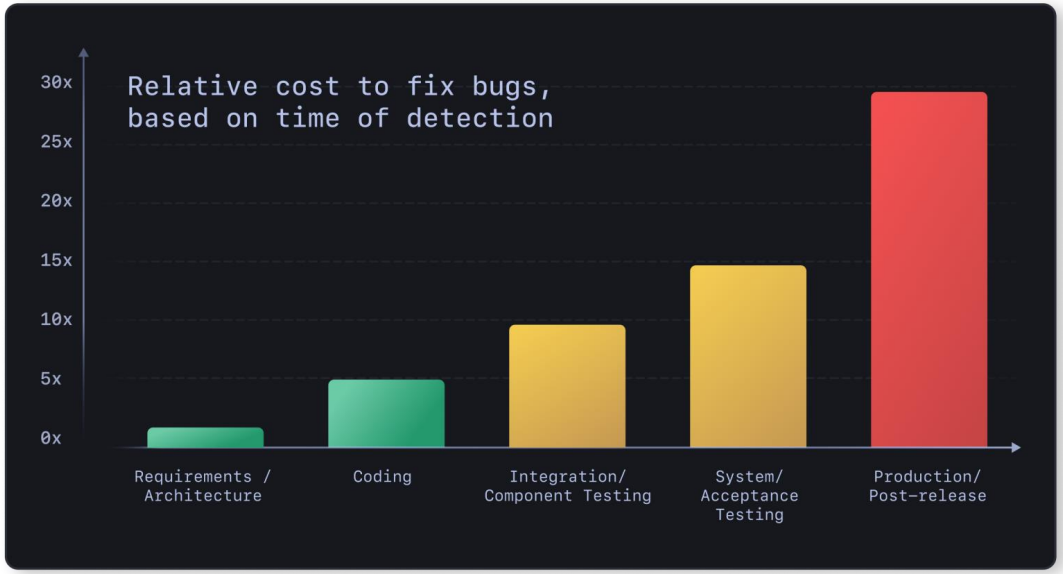
Hinsichtlich Bug Fixes und Usability Problemen



Quelle: https://deepsource.io/blog/exponential-cost-of-fixing-bugs/

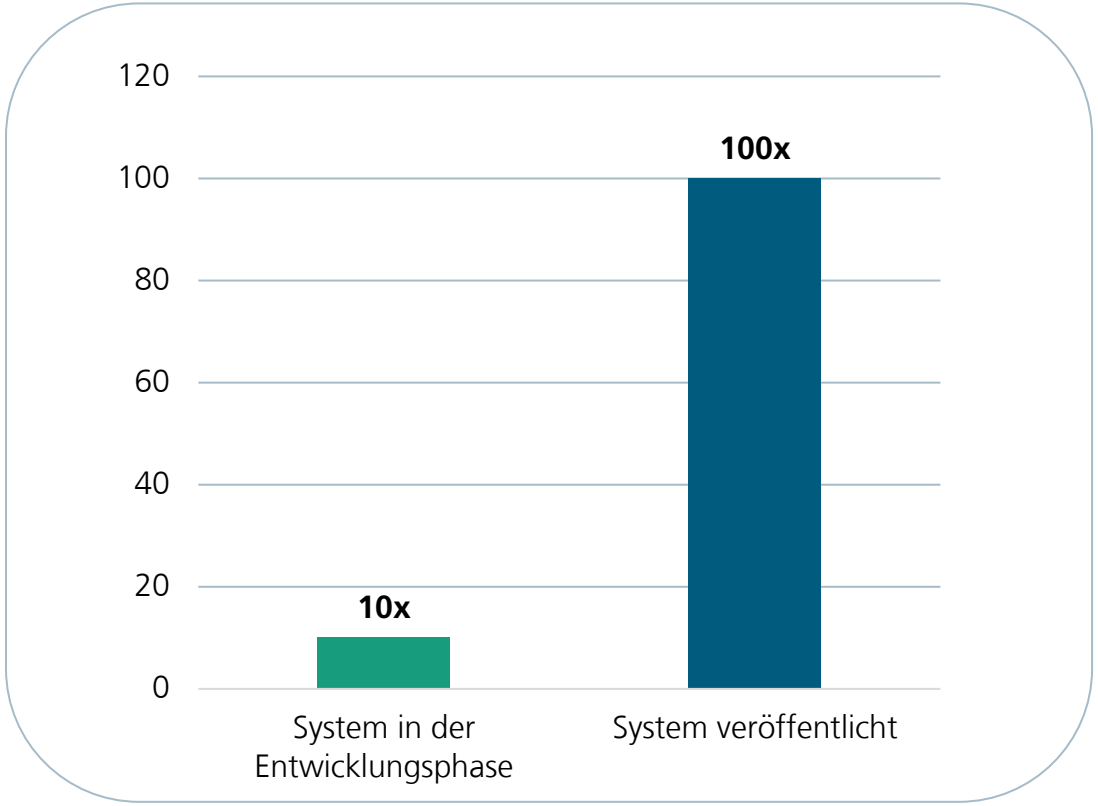
Kostenübersicht

Hinsichtlich Bug Fixes und Usability Problemen



Quelle: https://deepsource.io/blog/exponential-cost-of-fixing-bugs/

Kostenübersicht – Behebung von Usability Problemen



Quelle: https://uxpa.org/the-roi-of-usability/

Methoden
im Bereich Usable Security

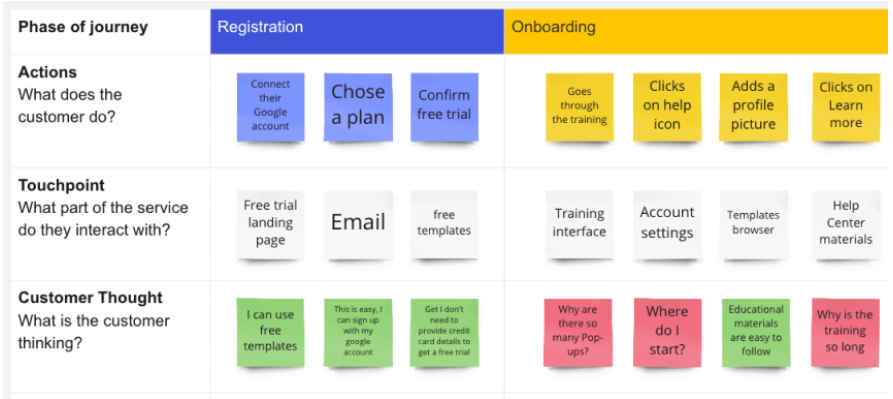
Interviews oder Umfragen mit Nutzenden

Fraunhofer AISEC

Methoden
im Bereich Usable Security

Interviews oder Umfragen mit Nutzenden

Entwicklung von User Journey Map, User Flows

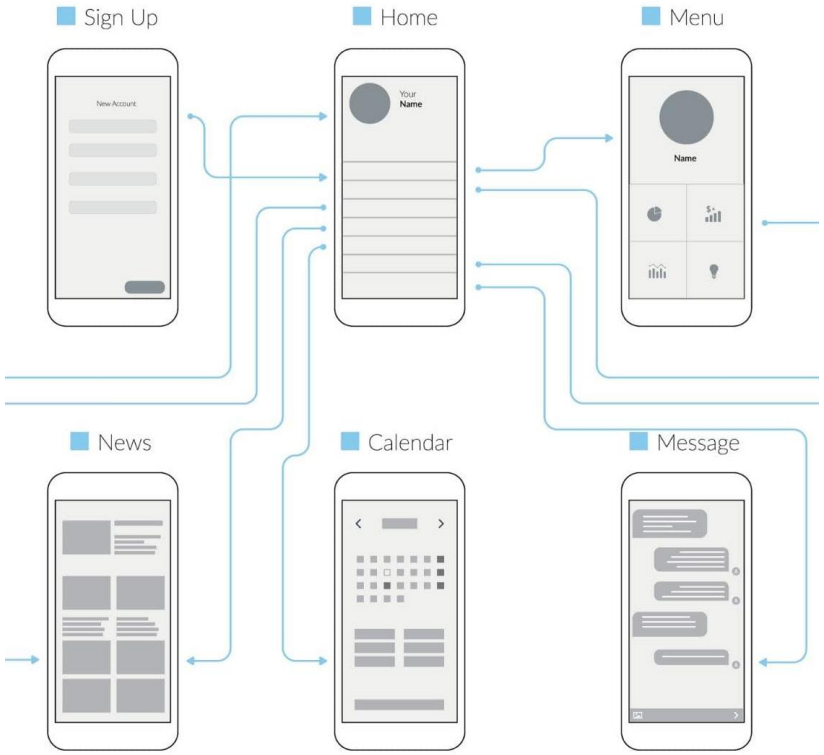


Quelle: https://miro.com/templates/customer-journey-map/

Methoden
im Bereich Usable Security

Interviews oder Umfragen mit Nutzenden

Entwicklung von User Journey Map, User Flows

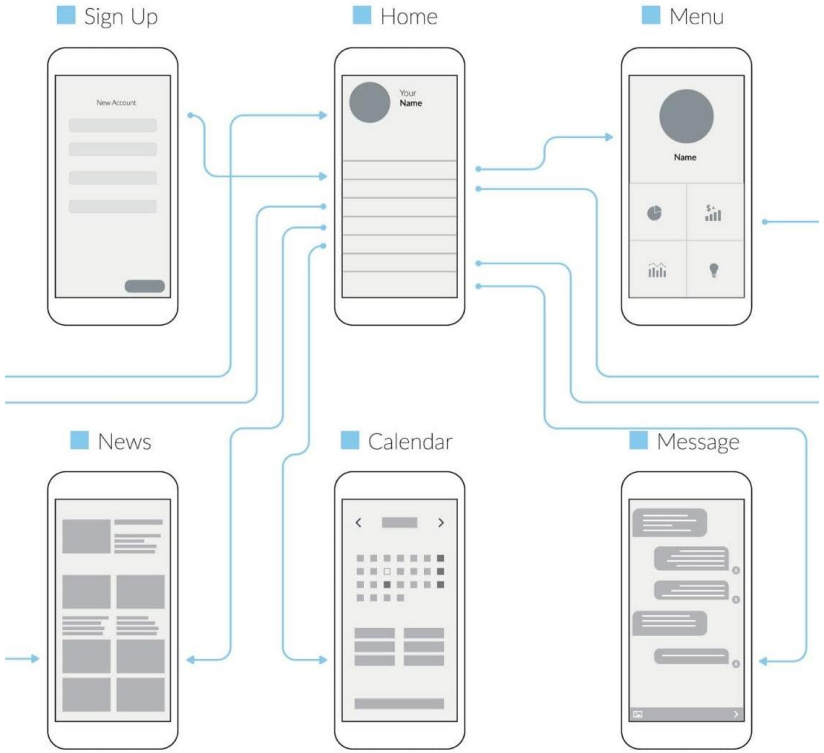


Quelle: https://www.leanplum.com/blog/user-flow/

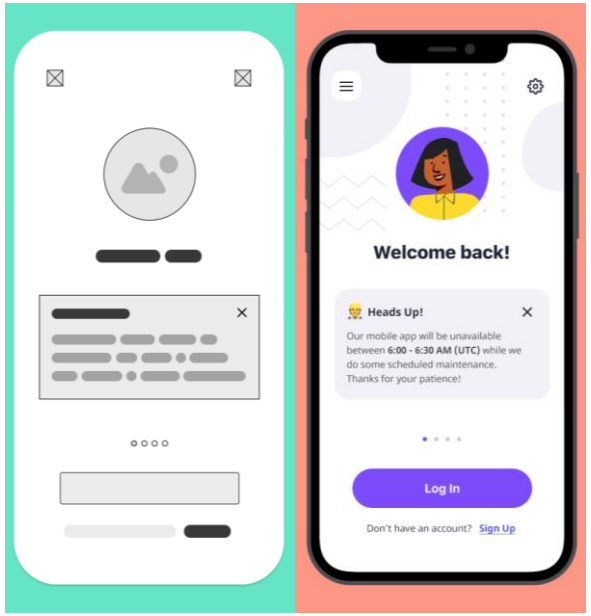
Methoden
im Bereich Usable Security

Interviews oder Umfragen mit Nutzenden

Entwicklung von User Journey Map, User Flows



Quelle: https://www.leanplum.com/blog/user-flow/



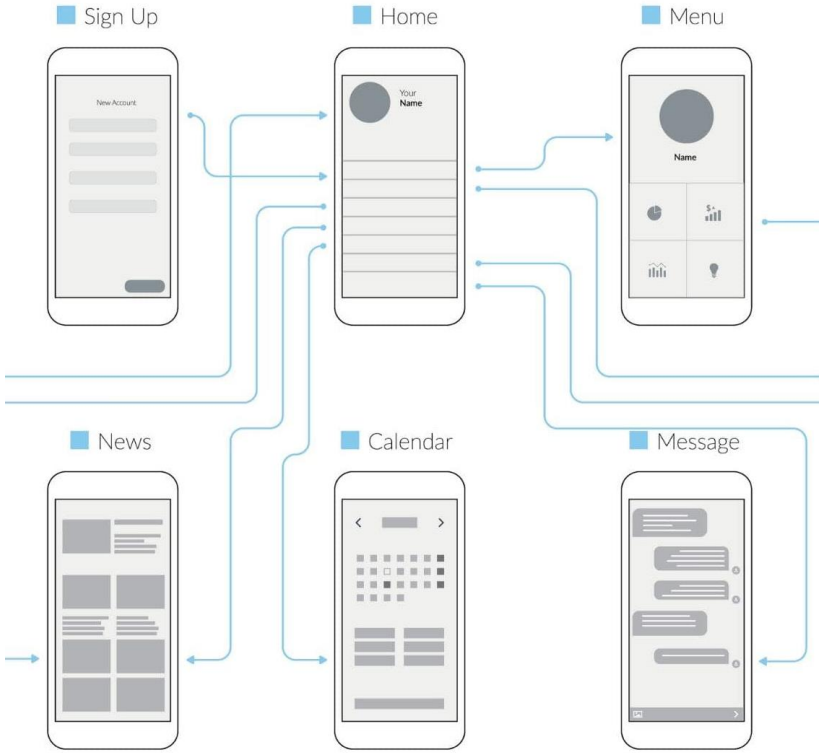
Quelle: https://moqups.com/blog/low-fidelity-vs-high-fidelity-wireframes/

Entwicklung von Mockups

Methoden
im Bereich Usable Security

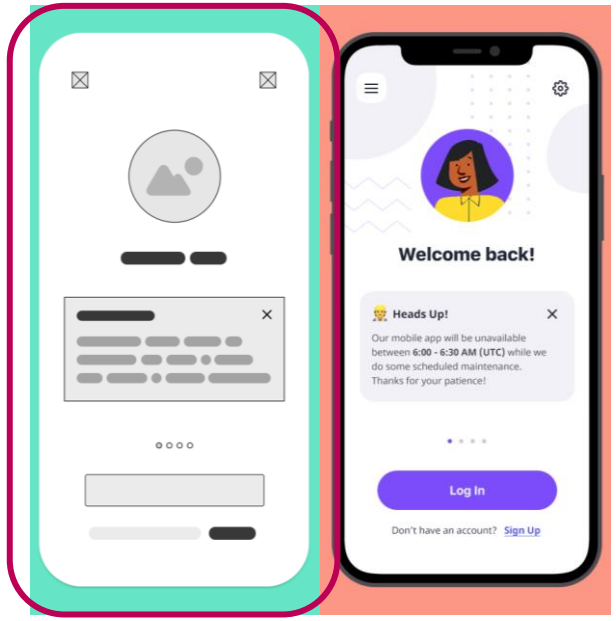
Interviews oder Umfragen mit Nutzenden

Entwicklung von User Journey Map, User Flows



Quelle: https://www.leanplum.com/blog/user-flow/

Besonders hilfreich für die Anfangsphase

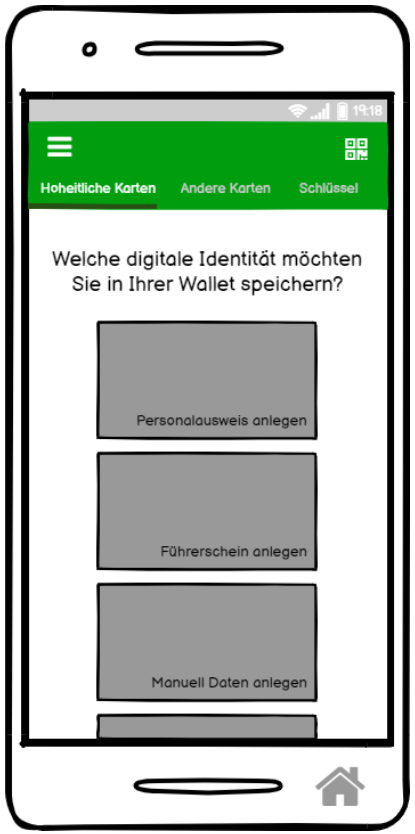


Quelle: https://moqups.com/blog/low-fidelity-vs-high-fidelity-wireframes/

Entwicklung von Mockups

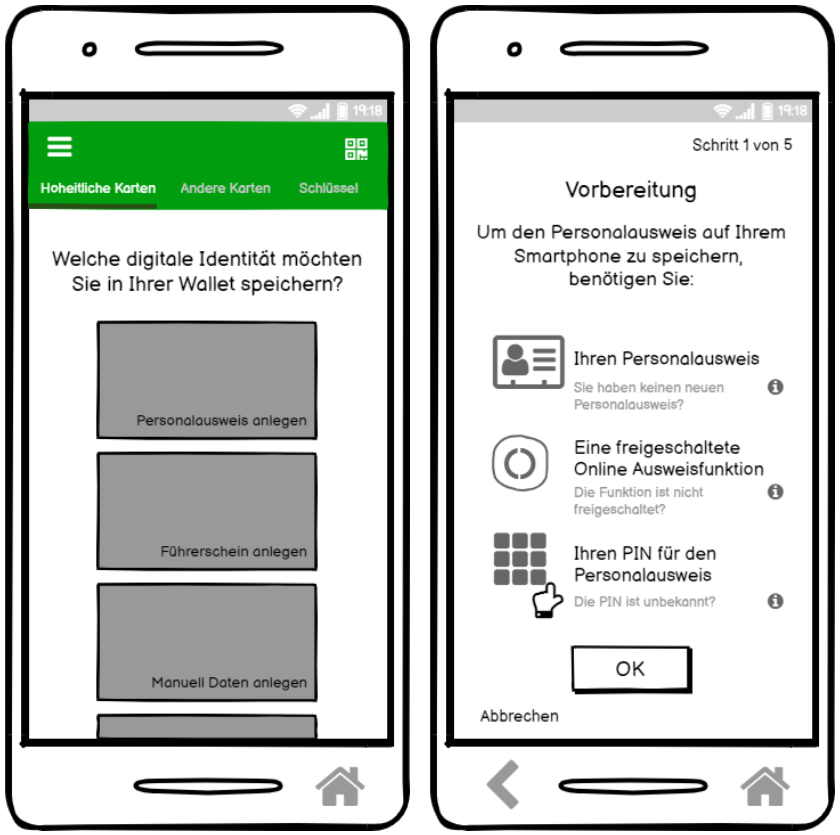
Wallet Mockup

Aktuelle Recherchen



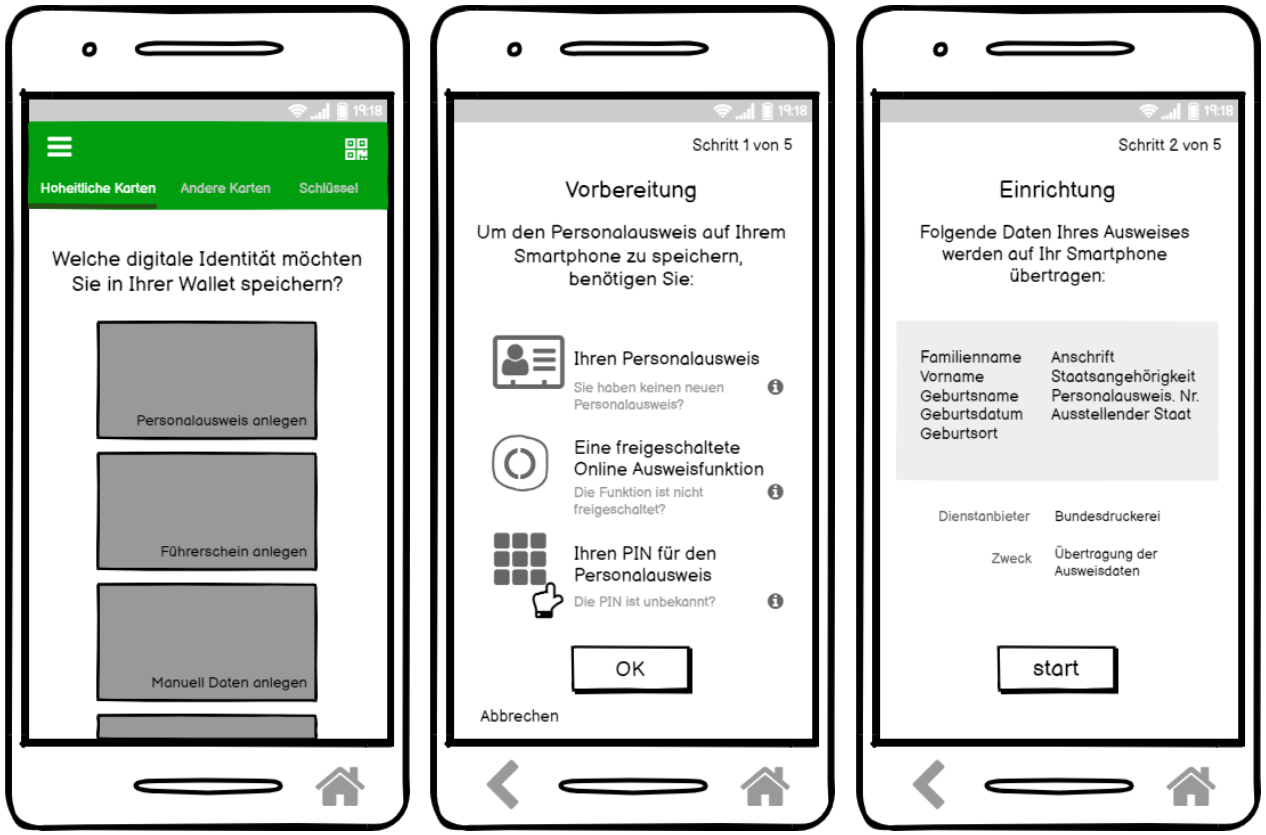
Wallet Mockup

Aktuelle Recherchen



Wallet Mockup

Aktuelle Recherchen



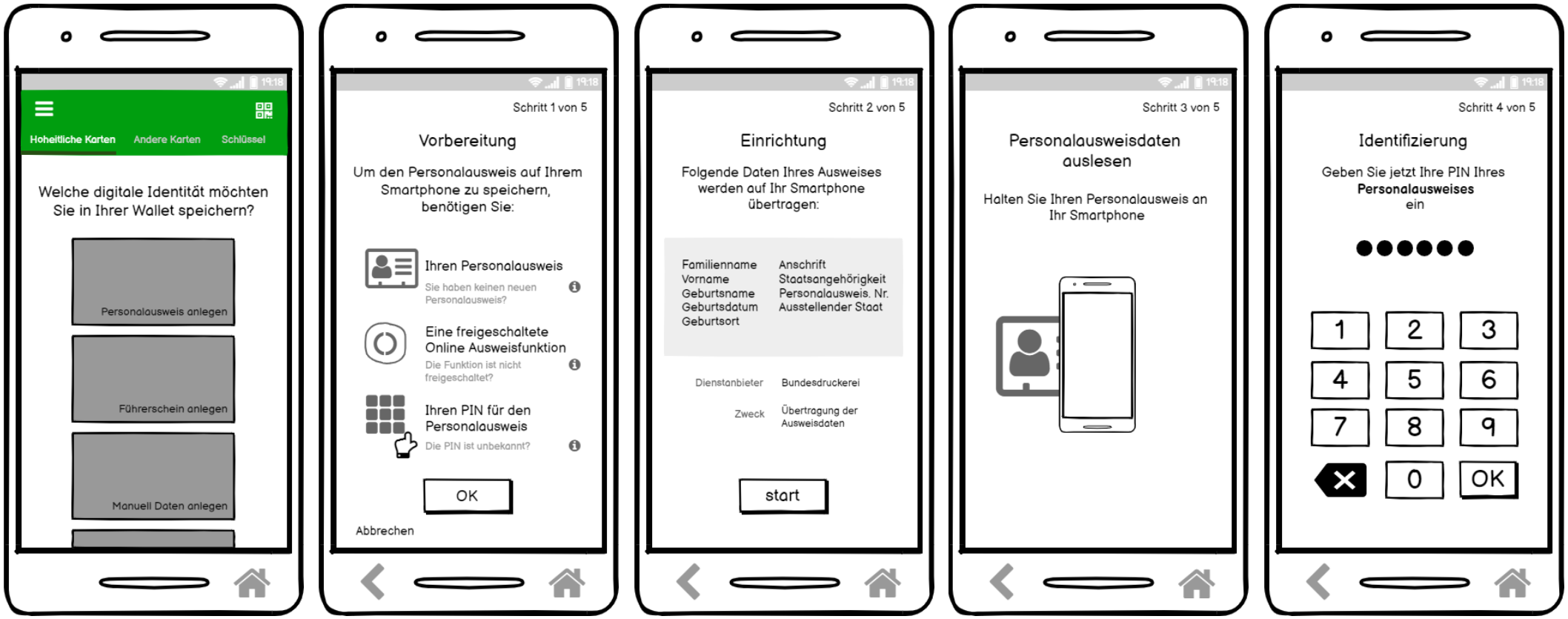
Wallet Mockup

Aktuelle Recherchen

Fraunhofer AISEC

Wallet Mockup

Aktuelle Recherchen



Fraunhofer AISEC

Aktuelle Ergebnisse und Herausforderungen
bei digitalen Identitäten

Passwort

- Nutzende begrüßen einen separaten Schutzmechanismus der App (PIN, Passwort, Biometrie)
  - Bei häufiger Eingabe wurde ein biometrisches Mittel zur Entsperrung der App bevorzugt

NFC Schnittstelle

- Nutzenden ist nicht immer klar, dass ein direkter Kontakt benötigt wird.
  - Teilweise wurde beschrieben, dass eine Fotografie der Karte gemacht wird

Aktuelle Ergebnisse und Herausforderungen
bei digitalen Identitäten

Einsatz

- Digitaler als auch physischer Einsatz der Karte wird gewünscht
  - Digitale Identität soll stehts nur einen Zusatz darstellen und nicht die physische Karte ersetzen
  - Es wird immer eine Rückfalllösung gewünscht
  - Direktes Feedback beim Einsatz der physischen Karte wird gutgeheißen

- Ein Vor-Ort Einsatz der digitalen Identität wurde mit Hilfe von QR Codes ermöglicht
  - Nutzende zeigten in Studien keine Probleme beim Einsatz der QR Code
  - Nutzende sind mit QR Code auf Grund der Pandemie gut vertraut (z.B. Impfzertifikate)

Aktuelle Ergebnisse und Herausforderungen
bei digitalen Identitäten

„Familien Funktion“

- Nutzende wünsche sich die Möglichkeit der Verwaltung von Daten mehrerer Personen
  - Oft wurde ein Vergleich zur Covid Pass App gezogen

Backup

- Nutzende wünschen sich die Möglichkeit eines Backups
  - Es werden oft Sorgen zum Verlust des Smartphones geäußert
  - Damit eingehend wird auch oft ein leerer Akkustand oder fehlendes Internet als Problem erwähnt

Empfehlungen
bei digitalen Identitäten

Verständnis, Akzeptanz und Vertrauen sollte der Fokus sein

- Betonung einer offiziellen App für Deutschland bereits beim Onboarding

Nachvollziehbare Rechteverwaltung

- Betonung der Kontrolle der Nutzenden
- Welche Rechte habe ich?
- Was passiert mit meinen Daten?
- Wer kann welche Daten einsehen?
  - Deutlich machen, dass eine Arzt*in nicht alle Daten der Patient*in einsehen kann, sondern nur einen bestimmten Satz Daten
- Wie lange können diese Daten eingesehen werden?
- Können geteilte Daten wieder zurückgezogen werden?

Empfehlungen
bei digitalen Identitäten

Verständlicher Einsatz der Passwörter

- Unterschied deutlich machen zwischen der PIN / dem Kennwort zur Schutz der App und der PIN für die Karte

Datenschutz und Datensicherheit

- Betonung der Sicherheit
  - Daten sind geschützt trotz verlorenem Smartphone
  - Verschlüsselte Kommunikation
  - Einsatz von Schlosssymbolen
- Betonung der DSGVO

Barrierefreiheit

- z.B. Beachtung von Farbkontrasten und Einsatz von leichter Sprache