

OMNISECURE - Sandra Kostic

23. Januar 2024

Digitalisierung und Vertrauen

Tutorial - Usable Privacy and Security

Wie wird eine gute Benutzbare Sicherheit erreicht

Drei Designprinzipien



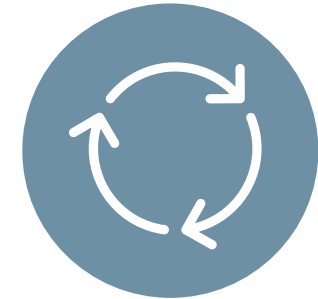
Frühe Einbeziehung der Nutzenden

- 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 Verfestung von Mockups / Klickdummies



Iterative Methoden nutzen

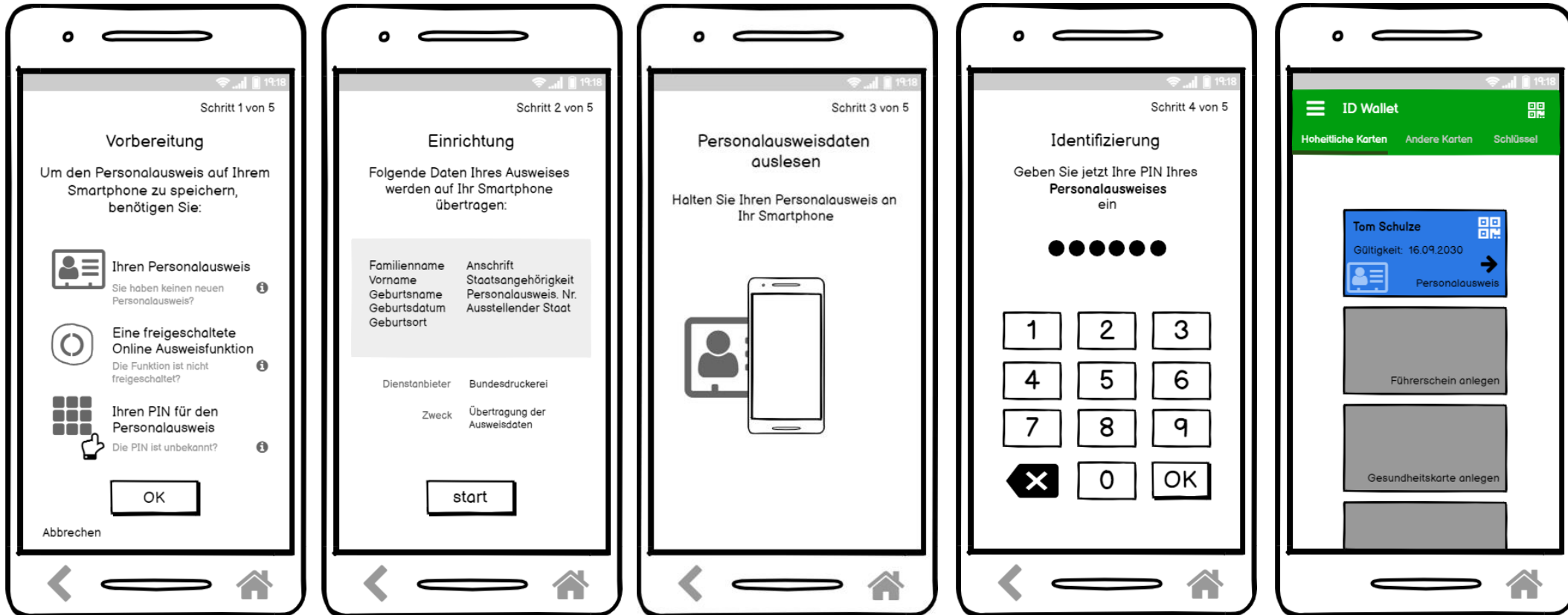
- Wiederholte Überarbeitung eines Mockups des Produktes mit Hilfe von Feedback der Nutzenden



**Frühe
Einbeziehung
der
Nutzenden**

Wallet Klick-Dummy

Low-Fidelity Prototyp



1. Designprinzip



Frühe Einbeziehung der Nutzenden



Frühe
Einbeziehung
der
Nutzenden

Wallet Klick-Dummy

Low-Fidelity Prototyp





Frühe Einbeziehung der Nutzenden

Wallet Klick-Dummy

Low-Fidelity Prototyp





**Studien
durchführen
und das
Verhalten von
echten
Nutzenden
evaluieren**



Studien durchführen und das Verhalten von echten Nutzenden evaluieren

Übersicht zur Studie

Evaluierung des Konzepts

Zusammenfassung

- Insgesamt ca. 60 Personen mit Hilfe von qualitativen Interviews befragt
 - Altersverteilung zwischen 18-56 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



Studien durchführen und das Verhalten von echten Nutzenden evaluieren

Aktuelle Ergebnisse und Herausforderungen

Vertrauen in digitale Identitäten

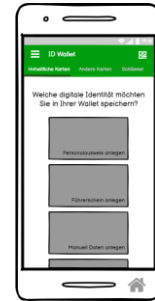
- **Nutzende wollen wissen, wer der Anbieter des Dienstes ist**
- Äußerst relevant für das Vertrauen in die Anwendung, besonders bei sensiblen Daten
 - Ist es ein deutscher Anbieter?
 - Sind die Server in Deutschland?
 - Gilt die DSGVO?
 - *Ist der Staat involviert?*



Studien durchführen und das Verhalten von echten Nutzenden evaluieren

Studienergebnisse

Evaluierung des Konzepts



Studie aus 2020

16 von 16
vertrauten dem
Konzept

9 Personen
Betreiber sollte der
Staat sein

7 Personen
Betreiber sollte ein
Unternehmen sein



**Iterative
Methoden
nutzen**



Iterative
Methoden
nutzen

Studienergebnisse

Aus 2022



Studie aus 2022

12 von 12
vertrauten dem
Konzept

11 Personen
Betreiber sollte der
Staat sein

1 Personen
Betreiber sollte ein
Unternehmen sein



Studie aus Nov.
2022

16 von 16
vertrauten dem
Konzept

13 Personen
Betreiber sollte der
Staat sein

3 Personen
Betreiber sollte ein
Unternehmen sein

Exakte
Wiederholung
aus 2020 !

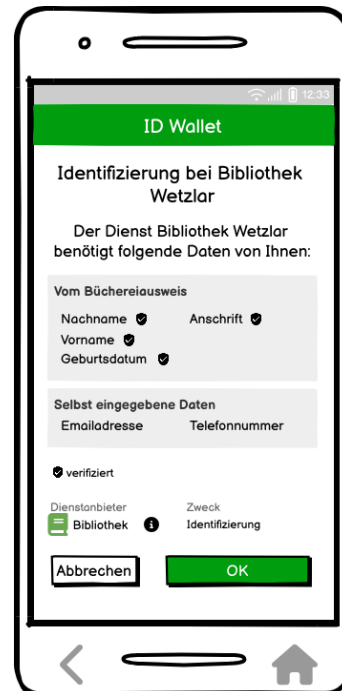


Iterative
Methoden
nutzen

Quantitativen Studie

Aufbau

— **Wallet Konzept wurde vorgestellt
ohne Hinweis auf hoheitliche IDs**



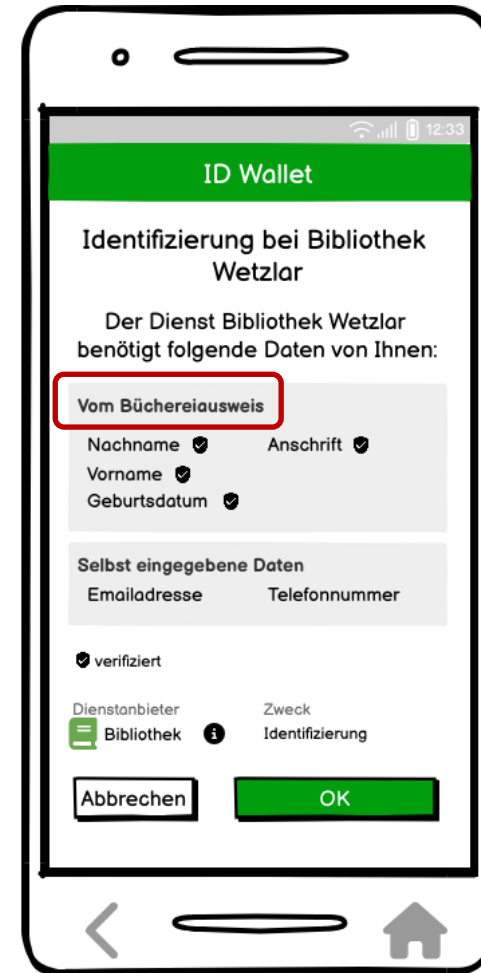


Iterative
Methoden
nutzen

Quantitativen Studie

Aufbau

Wallet Konzept wurde vorgestellt
ohne Hinweis auf hoheitliche IDs



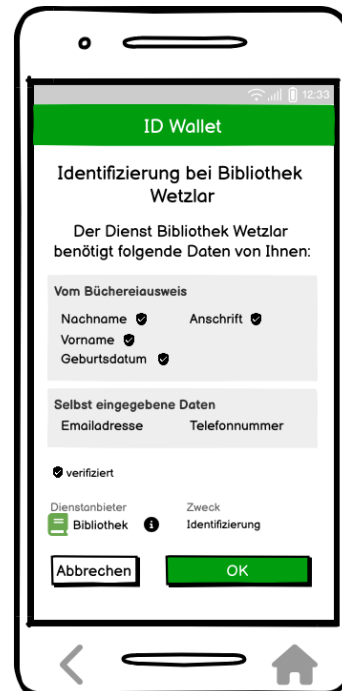


Iterative
Methoden
nutzen

Quantitativen Studie

Aufbau

Wallet Konzept wurde vorgestellt
ohne Hinweis auf hoheitliche IDs



Genannte Betreiber nach Präferenzen sortieren

(1= höchste Priorität; 7=niedrigste Priorität)

- **Bekanntes** *deutsches* Privatunternehmen
- **Bekanntes** nicht-deutsches Privatunternehmen
- Unbekanntes *deutsches* Privatunternehmen
- Unbekanntes nicht-deutsches Privatunternehmen
- Community-Projekt Open Source
- Deutsche Regierung
- Bekannte Gruppierung (z.B. der Chaos Computer Club (CCC), etc.)
- Anderer (Freifeld)

Quantitativen Studie

Studienergebnisse

Rückmeldungen von 306 Teilnehmenden im Dezember 2023

Reihenfolge	Name des Betreibers	Durschnitt
1	Bekanntes <i>deutsches</i> Privatunternehmen	2,5
2	Deutsche Regierung	3,2
3	Bekannte Gruppierung (z.B. CCC)	3,3
4	Bekanntes nicht-deutsches Privatunternehmen	3,9
5	Community-Projekt Open Source	4,6
6	Unbekanntes <i>deutsches</i> Privatunternehmen	4,7
7	Unbekanntes nicht-deutsches Privatunternehmen	5,8

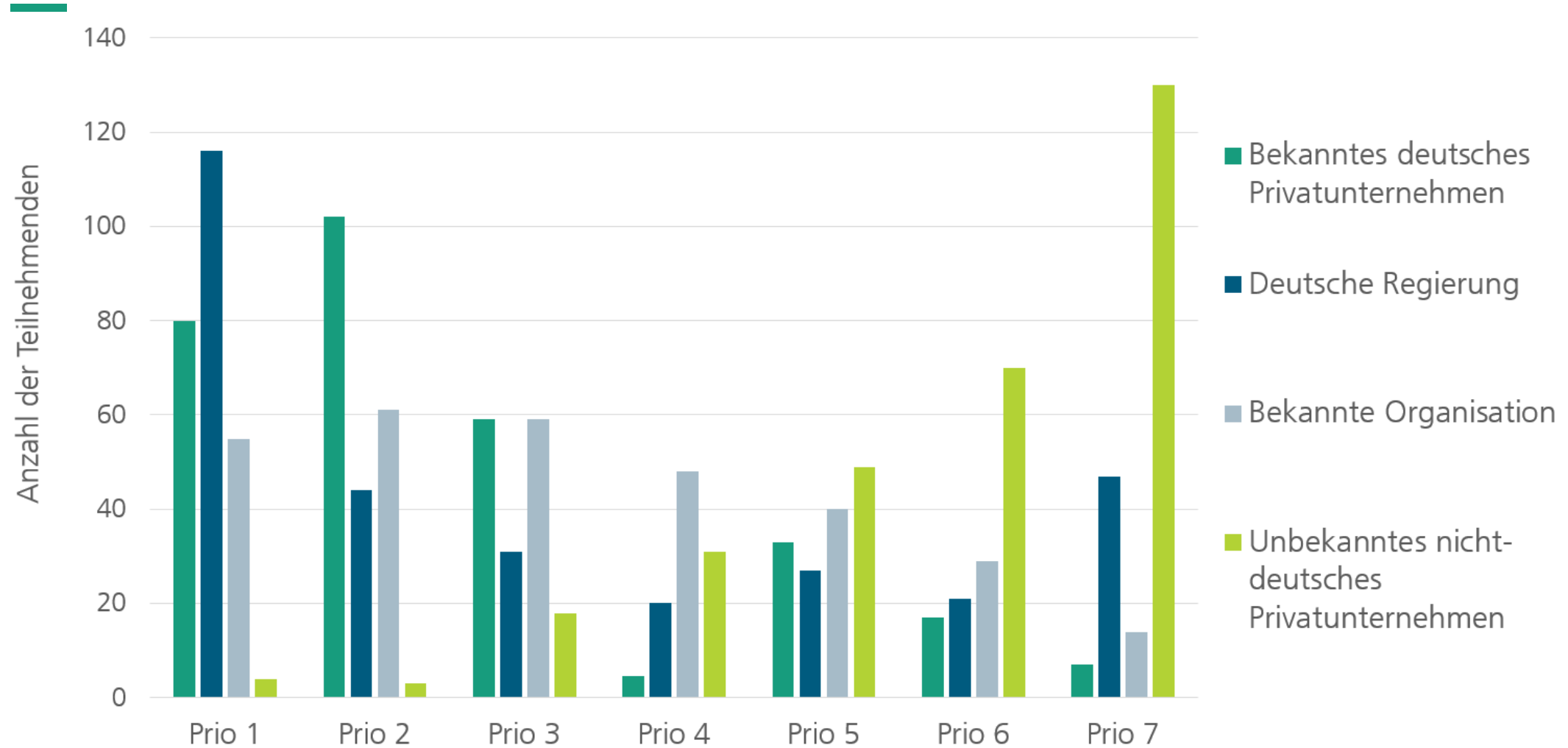




Iterative
Methoden
nutzen

Quantitativen Studie

Studienergebnisse

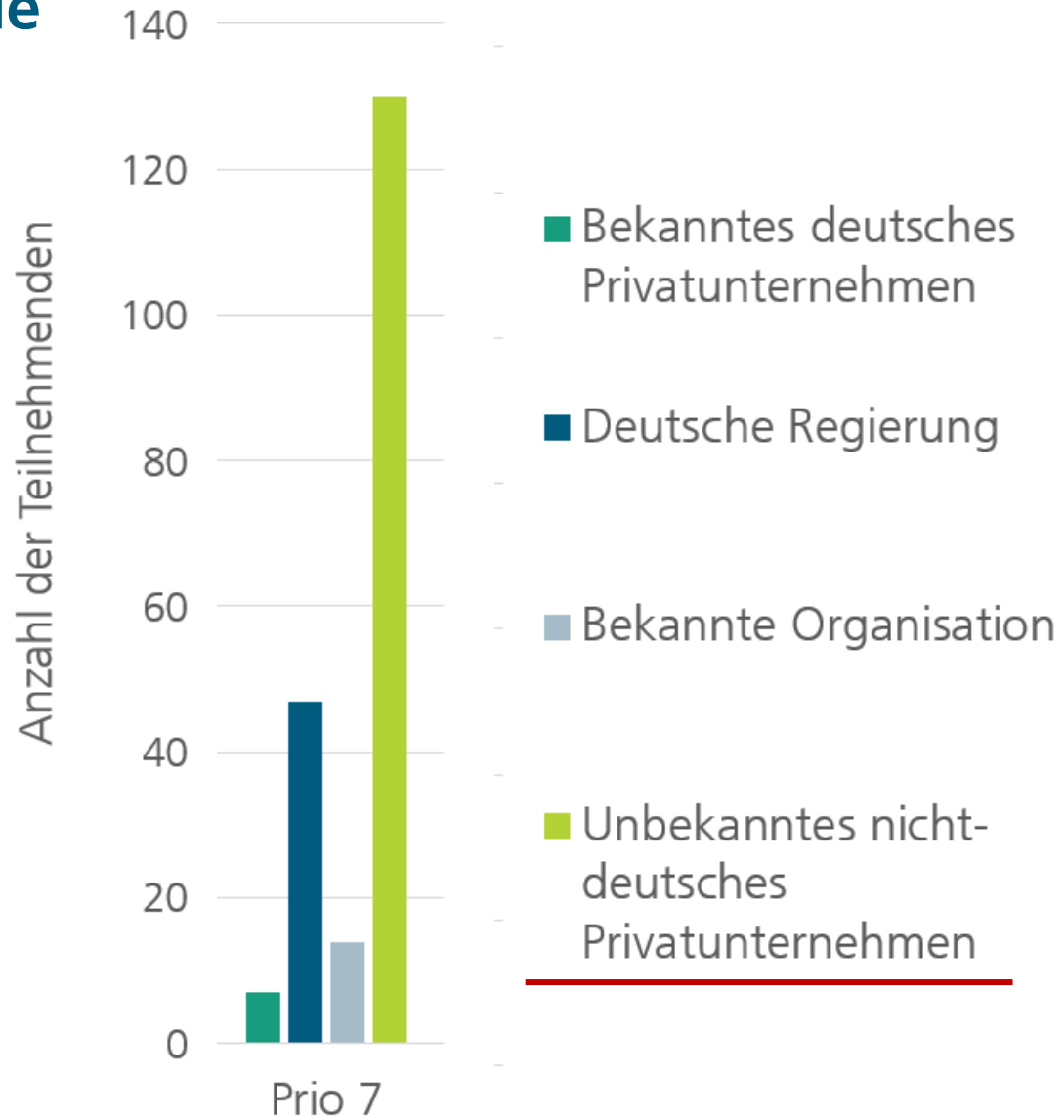




Iterative
Methoden
nutzen

Quantitativen Studie

Studienergebnisse

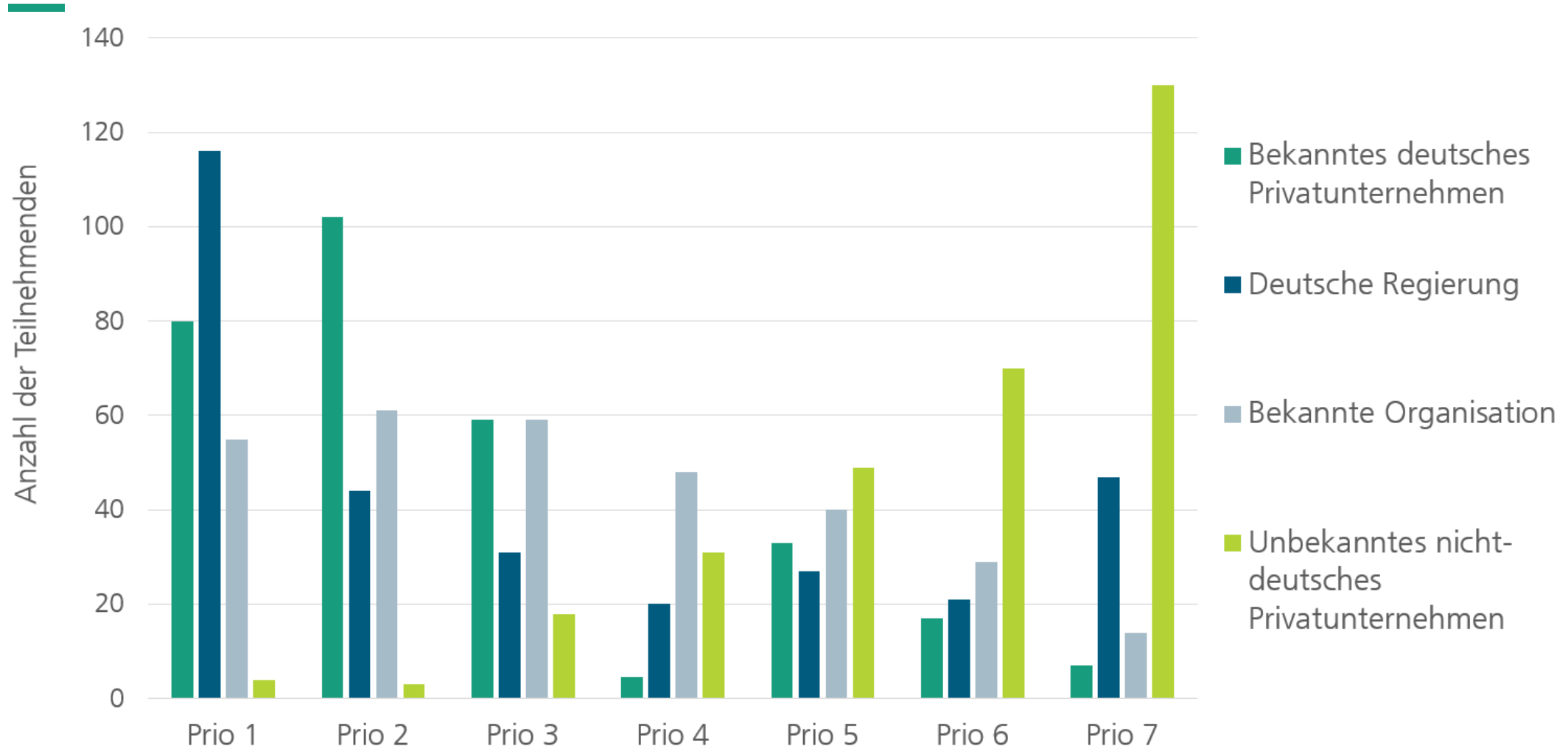




Iterative
Methoden
nutzen

Quantitativen Studie

Studienergebnisse

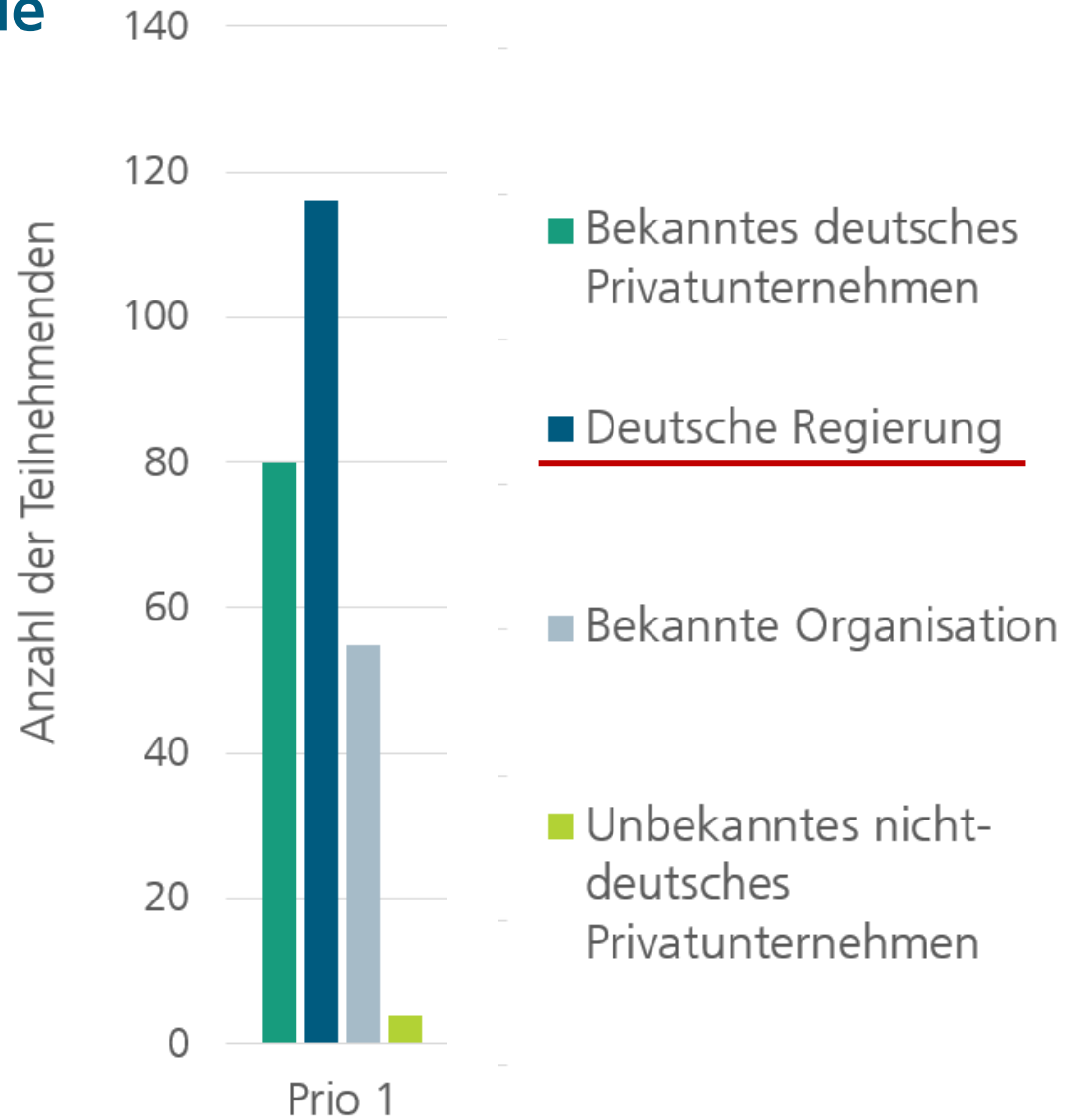




Iterative
Methoden
nutzen

Quantitativen Studie

Studienergebnisse



Zusammenfassung

Welche Erkenntnisse lassen sich durch die Einbeziehung von Nutzenden ermitteln

- Ermittlung von Anforderungen an die Nutzerfreundlichkeit und Sicherheit
- Rückmeldung zum Betreibermodell
 - Präferenzen zu bestimmten Betreibermodellen
 - Bekannte Unternehmen haben eine hohe Relevanz
 - Staat bleibt ein großer und starker Vertrauens- und Akzeptanzfaktor (gleich, welche Identitäten eingesetzt werden)



Interdisziplinären Austausch zum Beginn eines Projekts

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
Breite Str. 12,
14199 Berlin,
Germany

Sitz des Instituts:
Lichtenbergstraße 11
85748 Garching near Munich,
Germany

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



Fraunhofer-Institut für Angewandte
und Integrierte Sicherheit AISEC

