Passwörter Ade (!?)
Sind Passkeys die Zukunft?

Ein gutes/sicheres Passwort hängt davon, wie viele Kombinationen mit den verwendeten Zeichen (Zahlen/Buchstaben etc.) möglich sind

1. Beispiel:
Nur Zahlen (10), davon werden beliebige 8 für das Passwort eingesetzt
Berechnung: 10^8 = 100.000.000 Kombinationen

2. Beispiel:
Zahlen (10), Buchstaben (26x2) ä,ö,ü,ß = 66, davon 8 eingesetzt
Berechnung: 66^8 = 3.6 x 10^14 Kombinationen (360.000.000.000.000)

Noch mehr Kombinationen mit Sonderzeichen !“§$%&/()=?

Zeitbedarf zum Knacken von Passwörtern mit einem normalen PC

Inhalte	Anzahl Stellen	Beispiel	Zeitbedarf
nur Zahlen	8	98657452	0,01 Sekunden
nur Zahlen	12	097654736212	2 Minuten
Zahlen + Buchstaben	8	h6t3rf2l	5 Minuten
mit Klein-/Großbuchstaben	8	H6t3rf2L	6 Minuten
mit Klein-/Großbuchstaben	12	H6t3rf2LxY45	165 Jahre
komb. mit Sonder-Zeichen	8	H6t%rf2$	8 Tage
Komb. mit Sonder-Zeichen	12	H6t%rf2$xY45	1 Mio. Jahre

Quelle: Mekodia

Problem:

- 12 stellige Passwörter mit Groß-/Kleinbuchstaben, Zahlen und Sonderzeichen sind schwer zu merken
- Die Eingabe ist aufwendig und fehleranfällig

Meine Empfehlung (1):

- Merksätze zur Passwortgenerierung festlegen

dPCFts2“xiM die PC Freunde treffen sich 2x im Monat
d1!2“MiJidD der 12. Monat im Jahr ist der Dezember

Bei diesem Beispiel wird die Zahl 2x eingegeben, davon 1x mit Shifttaste

Was sind Passkeys?

- Eine neue und sichere Methode zum Einloggen bei Online-Diensten, **ohne Passwörter** zu benutzen
- Bei der Passkey Einrichtung bei einem Online-Dienst wird dagegen ein **Schlüsselpaar** generiert
- Ein Schlüssel (**Private Key**) wird **lokal** gespeichert.
  Der 2. Schlüssel (**Public Key**) wird auf dem Server des Online-Anbieters gespeichert.

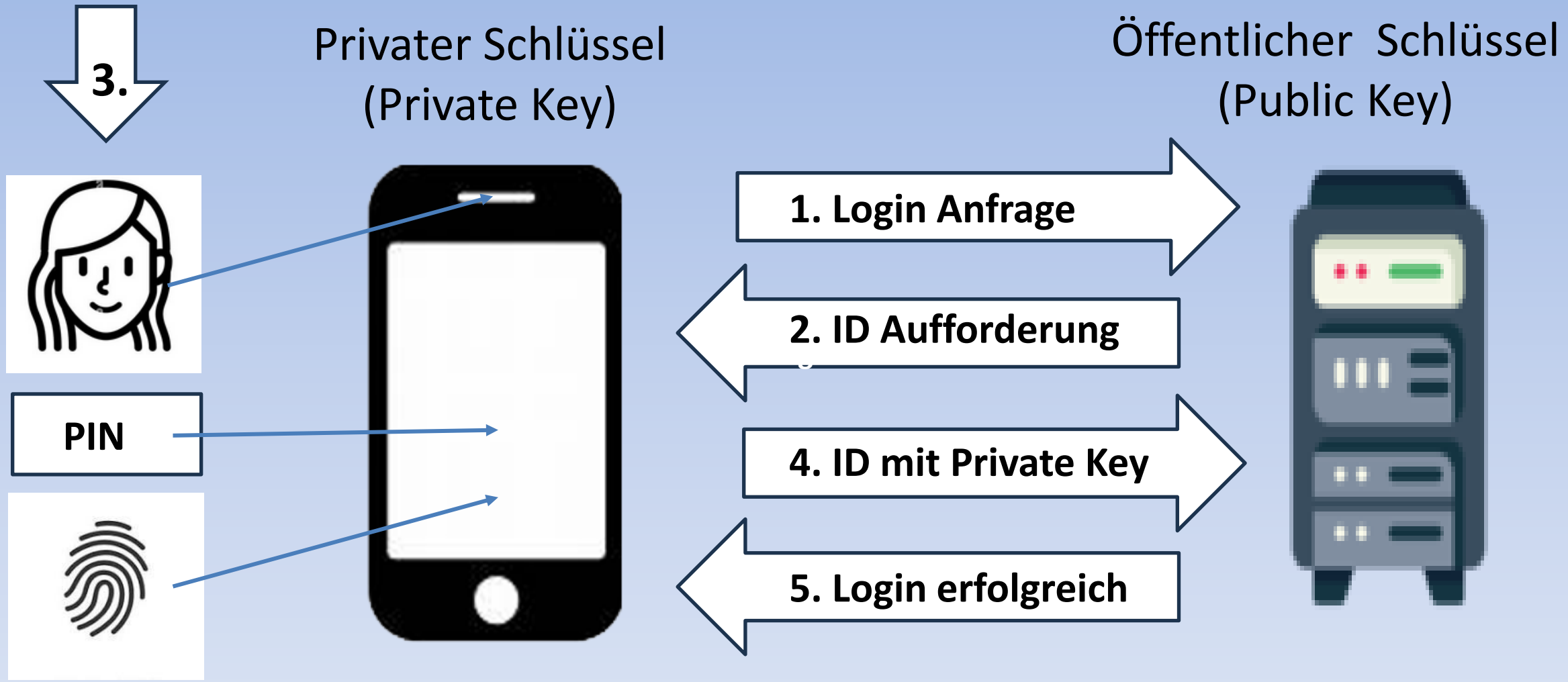
Was sind Passkeys? (Forts.)

- Das Login erfolgt durch Verwendung **biometrischer Daten** (Gesichtserkennung, Fingerabdruck) oder auch nur durch Eingabe der **Geräte-Pin**

Anmerkung:

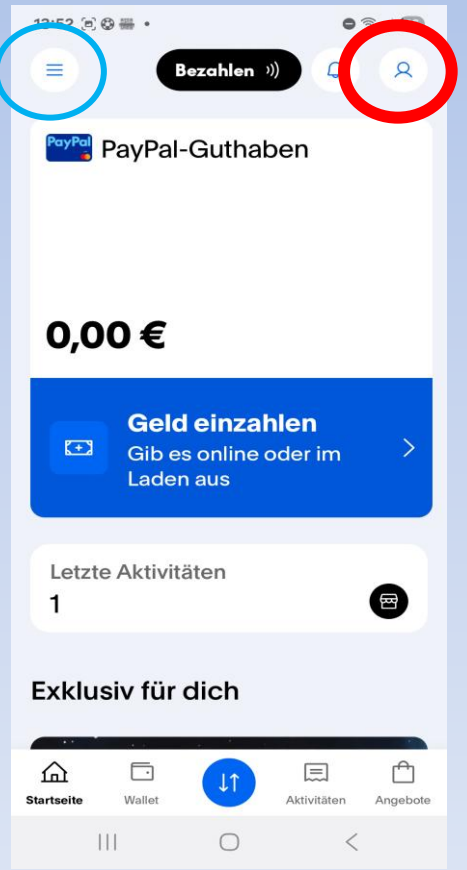
Der Private Key ist gerätegebunden. D.h. Ein Login kann nur mit dem Gerät erfolgen, auf dem der Private Key gespeichert ist

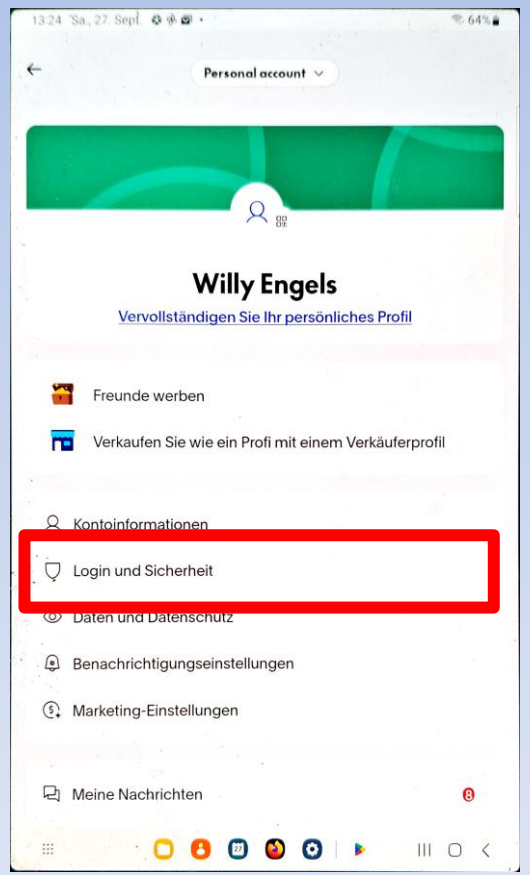
Passkeys

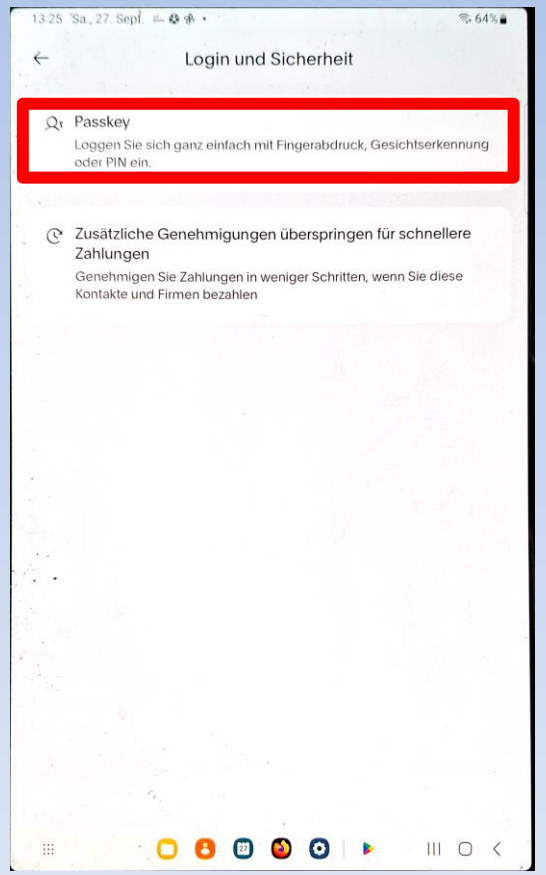

3.
Privater Schlüssel
(Private Key)
Öffentlicher Schlüssel
(Public Key)
PIN
1. Login Anfrage
2. ID Aufforderung
4. ID mit Private Key
5. Login erfolgreich

Einrichtung eines Login mit Passkey

Beispiel: PayPal mit Android Phone







Nächster Menü Punkt

„Passkey erstellen“
Fingerabdruck scannen

Fertig!

Vorteile von Passkeys

Hohe Sicherheit: Können nicht gestohlen oder erraten werden.

Phishing-Schutz: können nicht von gefälschten Webseiten abgegriffen werden

Benutzerfreundlichkeit: Keine komplexen Passwörter mehr
Einfache Anmeldung u.a. mit Fingerabdruck

Einrichtung: schnell und automatisiert

Quelle: BSI

Nachteile von Passkeys

Wiederherstellung bei Gerätverlust: Nur möglich, wenn ein Sicherungsstick eingerichtet wurde oder der Private Key in einer Cloud hinterlegt wurde

Begrenzte Akzeptanz: Verfahren steht erst am Anfang. Noch bieten relativ wenige Online-Dienste ein Login mit Passkeys an

Quelle: BSI

Nachteile von Passkeys (Forts.)

Eigene Meinung in Bezug auf PC-Anwendung:

Etwas umständlich, wenn kein Fingerabdruck-Sensor vorhanden

Mehrstufiges Vorgehen mit Smartphone Schlüssel
Ausführliche (DeepSeek) generierte Anleitung auf unserer Homepage, am Beispiel PayPal

Passkeys

Weitergehende Informationen

Ausführliche und leicht verständliche Information vom BSI
(**Bundesamt für Sicherheit in der Informationstechnik)**

www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Passkeys/passkeys-anmelden-ohne-passwort_node.html

Ein Vergleich mit Autos

Passwörter sind die Verbrenner
Passkeys die Elektro-Mobile

Exkurs PIN

75846375869701143340787664563

56835121125710787664563789054

56745389641354265711365807330