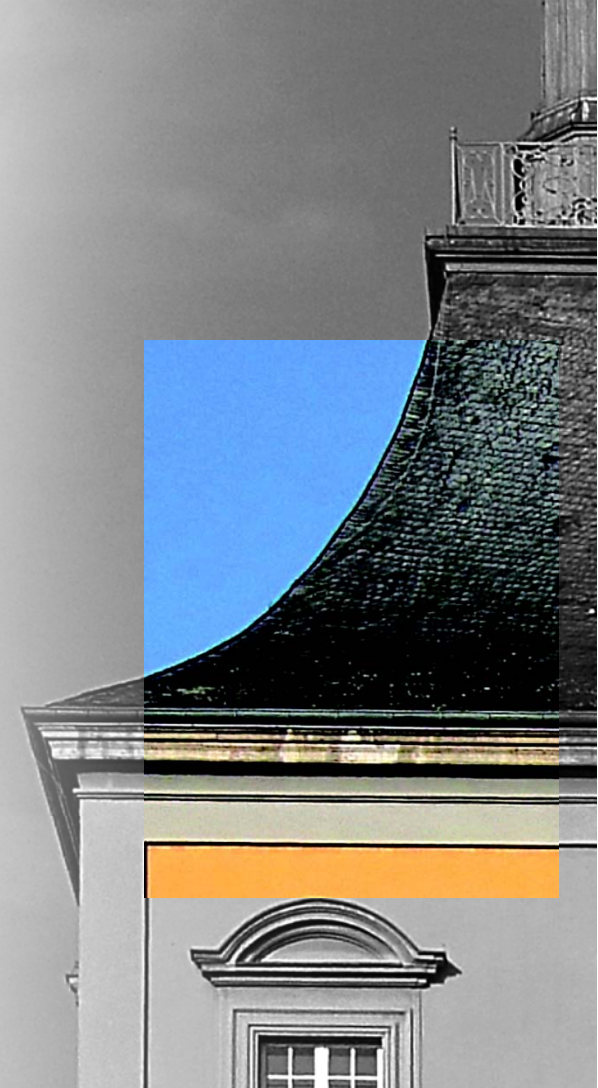


VORLESUNG
NETZWERKSICHERHEIT

SOMMERSEMESTER 2021
MO. 14-16 UHR




KAPITEL 7

AUTHENTIFIKATION IM WEB

BEGRIFFE

- Authentisierung
- Authentifizierung
- Autorisierung

- Authentisierung
 - (Aktiver) Nachweis, tatsächlich die Person zu sein, die man vorgibt zu sein.
- Authentifizierung
- Autorisierung

- Authentisierung
 - (Aktiver) Nachweis, tatsächlich die Person zu sein, die man vorgibt zu sein.
Beispiel: Ich bin Erika Mustermann und das ist mein Ausweis.
 - Authentifizierung
 - Autorisierung
- 



- Authentisierung
 - (Aktiver) Nachweis, tatsächlich die Person zu sein, die man vorgibt zu sein.
Beispiel: Ich bin Erika Mustermann und das ist mein Ausweis.
- Authentifizierung
 - Die im Rahmen der Authentisierung vorgelegten Nachweise werden überprüft.
- Autorisierung

- Authentisierung
 - (Aktiver) Nachweis, tatsächlich die Person zu sein, die man vorgibt zu sein.
Beispiel: Ich bin Erika Mustermann und das ist mein Ausweis.
- Authentifizierung
 - Die im Rahmen der Authentisierung vorgelegten Nachweise werden überprüft.
Beispiel: Überprüfung (durch eine vertrauenswürdige Instanz), z.B. Realität gegen Identitätsnachweis.
- Autorisierung



- Authentisierung
 - (Aktiver) Nachweis, tatsächlich die Person zu sein, die man vorgibt zu sein.
Beispiel: Ich bin Erika Mustermann und das ist mein Ausweis.
- Authentifizierung
 - Die im Rahmen der Authentisierung vorgelegten Nachweise werden überprüft.
Beispiel: Überprüfung (durch eine vertrauenswürdige Instanz), z.B. Realität gegen Identitätsnachweis.
- Autorisierung



- Authentisierung
 - (Aktiver) Nachweis, tatsächlich die Person zu sein, die man vorgibt zu sein.
Beispiel: Ich bin Erika Mustermann und das ist mein Ausweis.
- Authentifizierung
 - Die im Rahmen der Authentisierung vorgelegten Nachweise werden überprüft.
Beispiel: Überprüfung (durch eine vertrauenswürdige Instanz), z.B. Realität gegen Identitätsnachweis.
- Autorisierung
 - Zuteilung von Zugriffsrechten nach erfolgreicher Authentifizierung.

- Authentisierung
 - (Aktiver) Nachweis, tatsächlich die Person zu sein, die man vorgibt zu sein.
Beispiel: Ich bin Erika Mustermann und das ist mein Ausweis.
- Authentifizierung
 - Die im Rahmen der Authentisierung vorgelegten Nachweise werden überprüft.
Beispiel: Überprüfung (durch eine vertrauenswürdige Instanz), z.B. Realität gegen Identitätsnachweis.
- Autorisierung **für uns an dieser Stelle nicht weiter relevant.**
 - Zuteilung von Zugriffsrechten nach erfolgreicher Authentifizierung.
Beispiel: Zugriff auf Webinhalte / Systemressourcen / Aktionen.

- Der Begriff „Authentifikation“ fasst die notwendigen Aktivitäten zusammen:
 - Eine Person authentisiert sich...
 - und wird anschließend authentifiziert.
- Im Englischen leichter:
 - Authentikation
 - To authenticate (oneself)
 - To authenticate (others)
 - Authorization
 - To authorize (others)

AUTHENTIFIKATION IM WEB

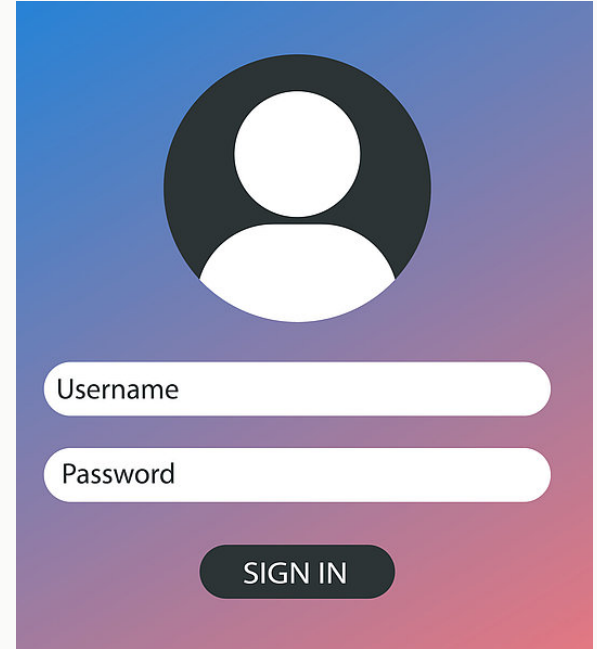
Vereinzelt vielleicht mit Multifactor Authentication(MFA)

mehr dazu später

Authentifikation in beinahe jeder Anwendung:

Username + Passwort

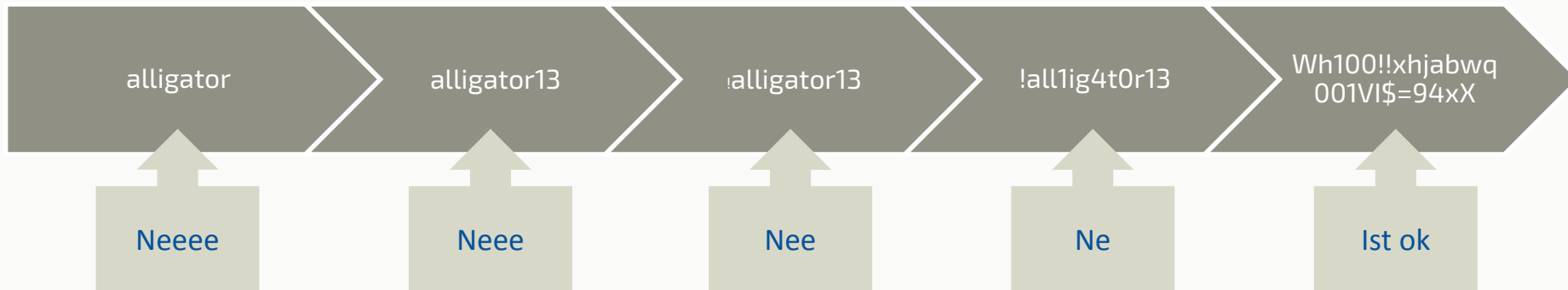
Idealer Ansatz?



https://www.der-niedergelassene-arzt.de/fileadmin/_processed_/d/6/csm_shutterstock_1231813309_AnyaPL_d86160ce41.jpg

PROBLEM 1: PASSWÖRTER

Man muss sich ein Passwort überlegen UND merken



PROBLEM 2: (VIELE) PASSWÖRTER

Man muss sich VIELE Passwörter überlegen UND merken



Password-Manager? Kann helfen



ABER: Muss erst installiert und eingerichtet werden



Mehr Sicherheit
sollte nicht
durch mehr
Aufwand
geschehen

Jeglicher
Mehraufwand
ist für den
Endverbraucher
abschreckend.

PROBLEM: PASSWÖRTER SPEICHERN

Passwörter basieren auf einem Shared Secret



Nutzer:
Kennt Passwort
für sein Konto



Server:
Speichert
Passwort für
entsprechendes
Konto



Angriff auf Server
bietet Möglichkeit
Passwort des Nutzers
zu erhalten.

PROBLEM: PASSWÖRTER SPEICHERN

Passwörter basieren auf einem Shared Secret



Nutzer:
Kennt Passwort
für sein Konto



Server:
Speichert
Passwort für
entsprechendes
Konto



Hashes in der
Serverdatenbank
verhindern
„einfachen“ Zugriff

PROBLEM: PASSWÖRTER SPEICHERN

Passwörter basieren auf einem Shared Secret



Nutzer:
Kennt Passwort
für sein Konto

Aber es bleibt ein Shared Secret



Server:
Speichert
Passwort für
entsprechendes
Konto



Hashes in der
Serverdatenbank
verhindern
„einfachen“ Zugriff

MULTIFACTOR-AUTHENTIFIKATION

- Unterschiedliche Faktoren bei der Authentifikation sollen die Sicherheit erhöhen
 - Wissen
 - Besitz
 - Inhärenz

MULTIFACTOR-AUTHENTIFIKATION

- Unterschiedliche Faktoren bei der Authentifikation sollen die Sicherheit erhöhen
 - ~~Wissen~~
 - Besitz
 - ~~Inhärenz~~

Im Web häufig „Google Authenticator“ als 2-FA eingesetzt.

GOOGLE AUTHENTICATOR

✕ Cancel

Setup Google Authenticator



Get the Authenticator App from the Google Play Store (Android) or iTunes App Store (iOS).



Choose Scan a barcode.



Can't scan it?

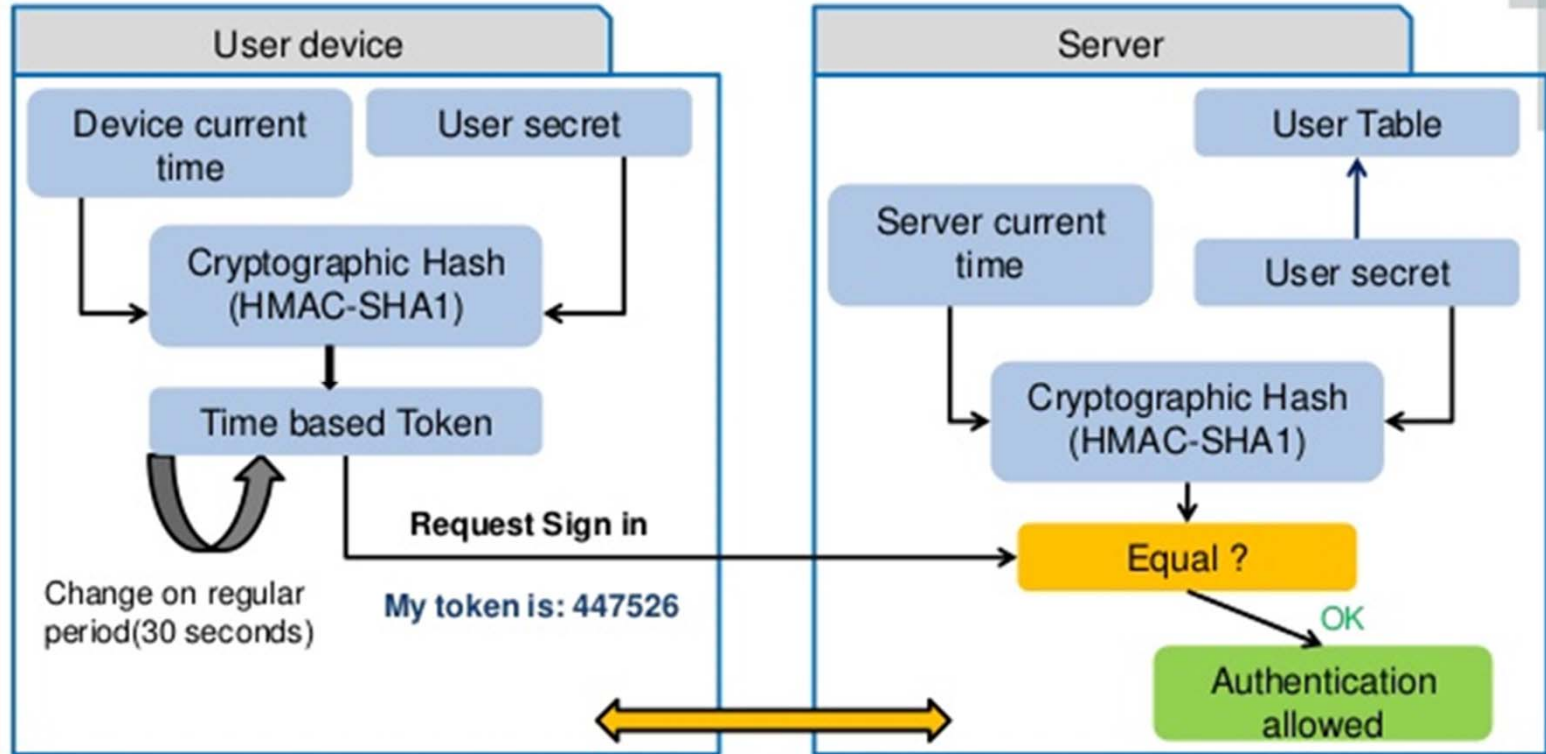
Set up Authenticator. Enter the six-digit code that you see in the app.

Enter Code

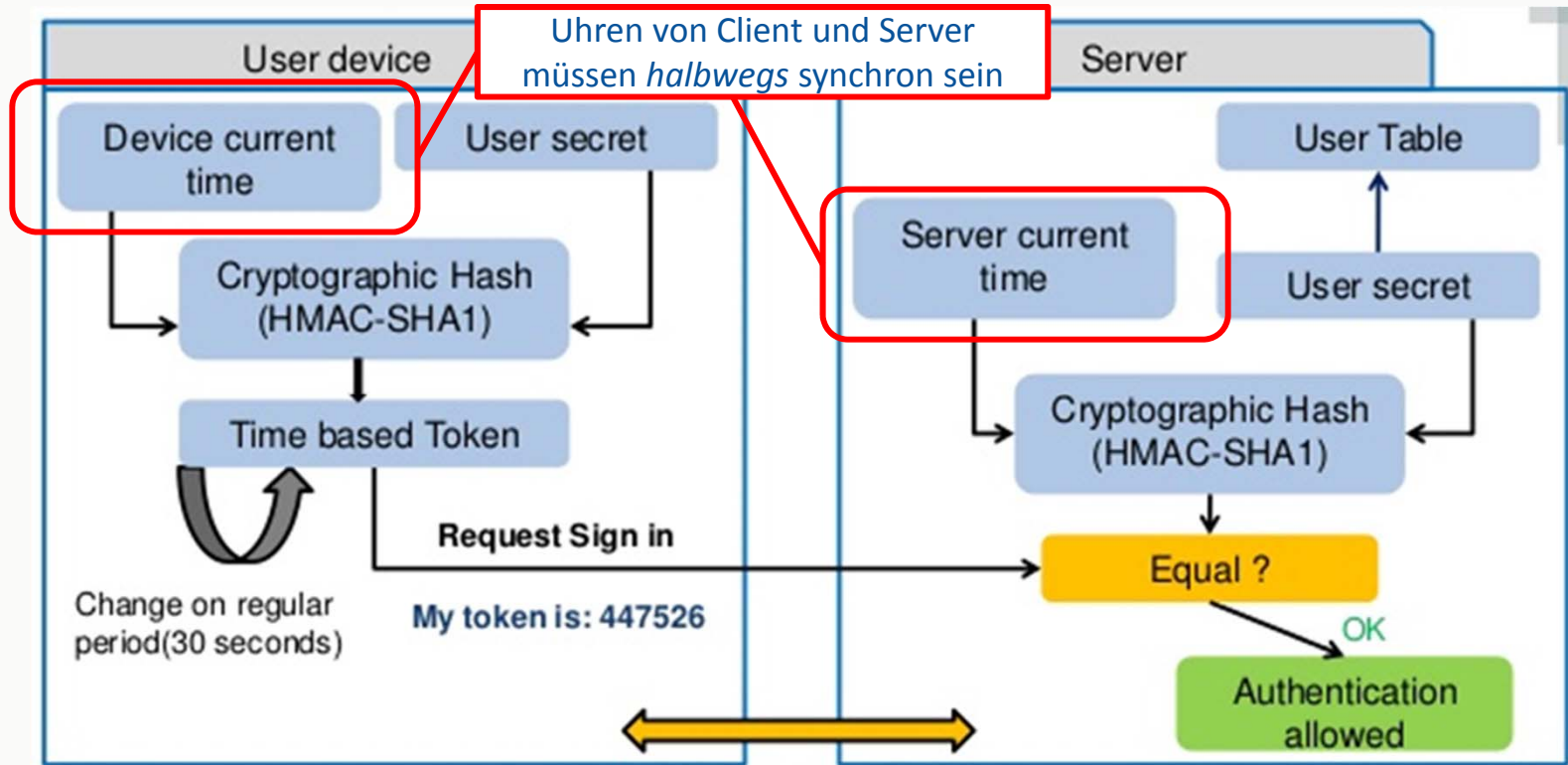
Verify

zxyl.com

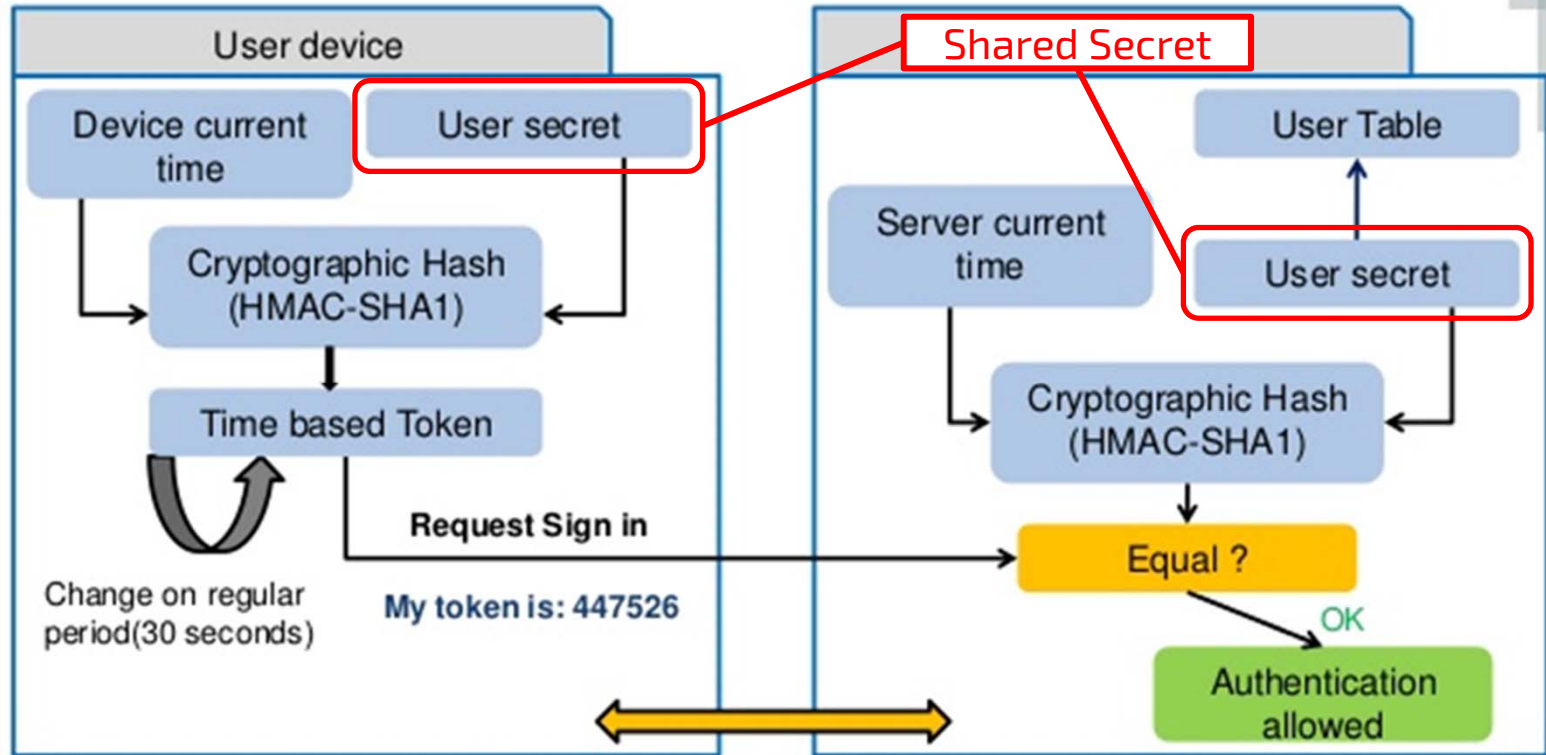
GOOGLE AUTHENTICATOR



GOOGLE AUTHENTICATOR



GOOGLE AUTHENTICATOR



GOOGLE AUTHENTICATOR

- Streng genommen ist Google Authenticator **KEIN** Multifactor sondern einfach ein zweites Passwort (Shared Secret)

... wobei dieses im Klartext auf dem Server hinterlegt sein muss!

WIE KANN MAN DIESE PROBLEME LÖSEN?

Neuer Ansatz mit folgenden Eckpunkten:

Nutzer soll sich nichts
merken müssen

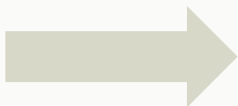
Kein Shared Secret
verwenden

Kein (erheblicher)
Mehraufwand im Vergleich
zu einem Passwort

WIE KANN MAN DIESE PROBLEME LÖSEN?

Neuer Ansatz mit folgenden Eckpunkten:

Nutzer soll sich nichts
merken müssen



"Something you know"



"Something you have/are"



Kein Shared Secret
verwenden

Kein (erheblicher)
Mehraufwand im Vergleich
zu einem Passwort

WIE KANN MAN DIESE PROBLEME LÖSEN?

Neuer Ansatz mit folgenden Eckpunkten:

Nutzer soll sich nichts
merken müssen



"Something you know"



"Something you have/are"



Kein Shared Secret
verwenden



Public Key + Private Key



Kein (erheblicher)
Mehraufwand im Vergleich
zu einem Passwort

WIE KANN MAN DIESE PROBLEME LÖSEN?

Neuer Ansatz mit folgenden Eckpunkten:

Nutzer soll sich nichts merken müssen



"Something you know"



"Something you have/are"



Kein Shared Secret verwenden



Public Key + Private Key



Kein (erheblicher) Mehraufwand im Vergleich zu einem Passwort



Authentisierung durch simple Aktion



FAST IDENTITY ONLINE(FIDO)

Unter anderem
auch das BSI

FIDO-Allianz:

Zusammenschluss von zahlreichen
Unternehmen und Organisationen

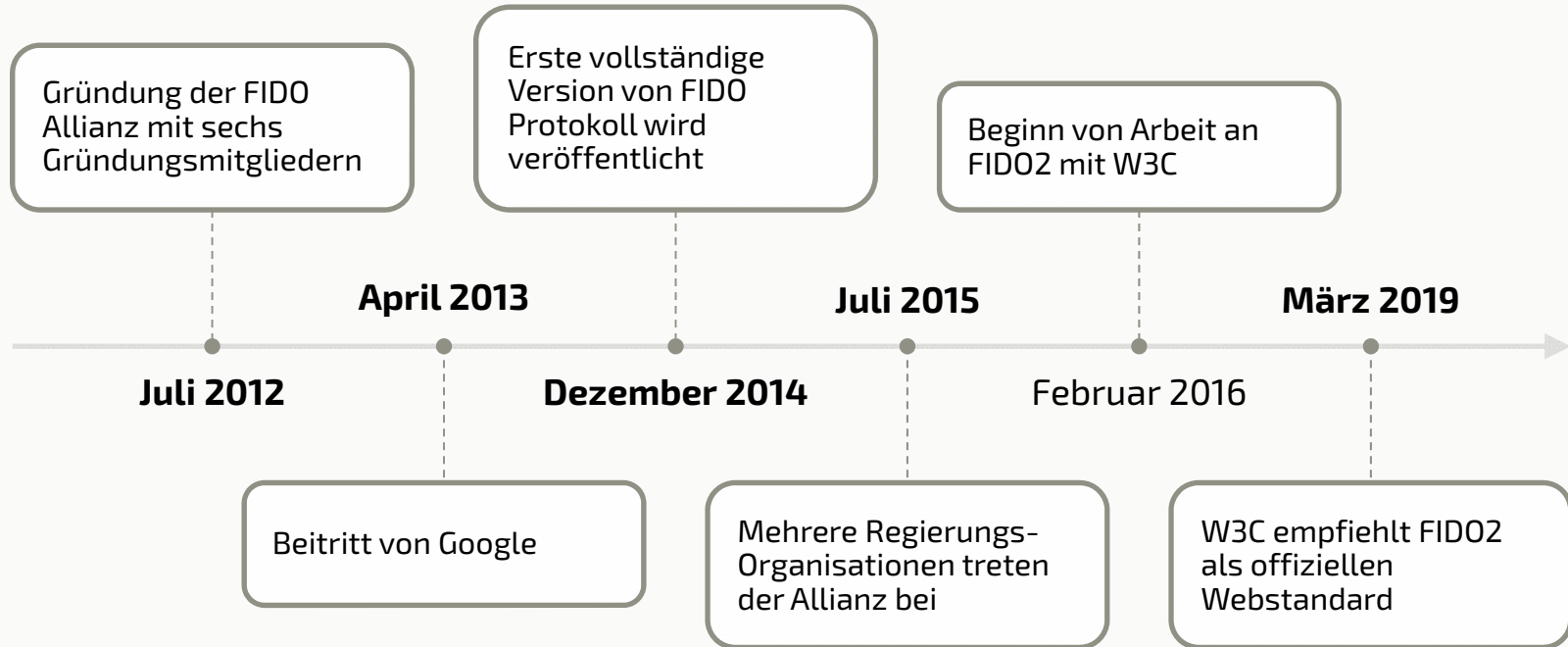
Ziel:

Entwicklung und Verbreitung von
offenen, frei verfügbaren Standards zur
Authentifizierung



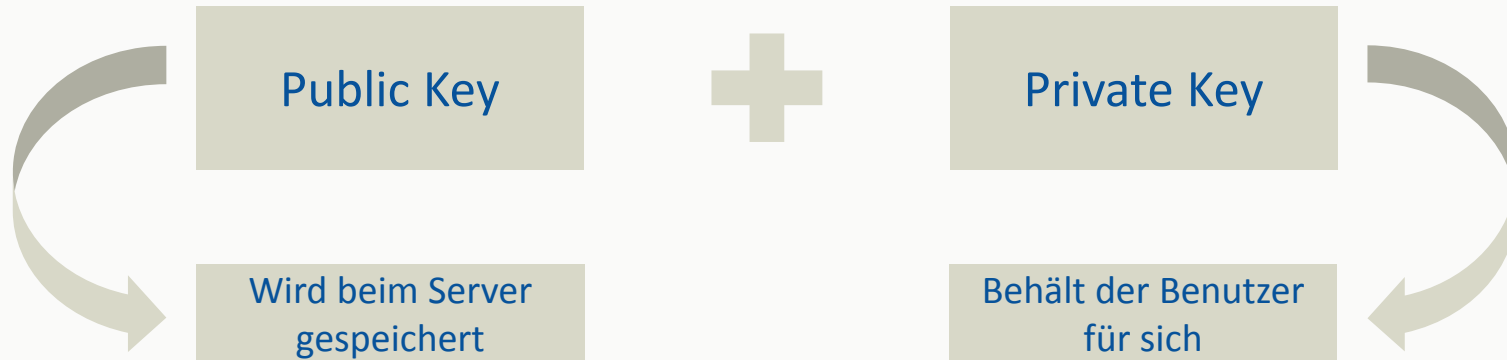
<https://www.iclarified.com/74436/apple-joins-fido-alliance-as-board-member>

FIDO2 - HISTORIE

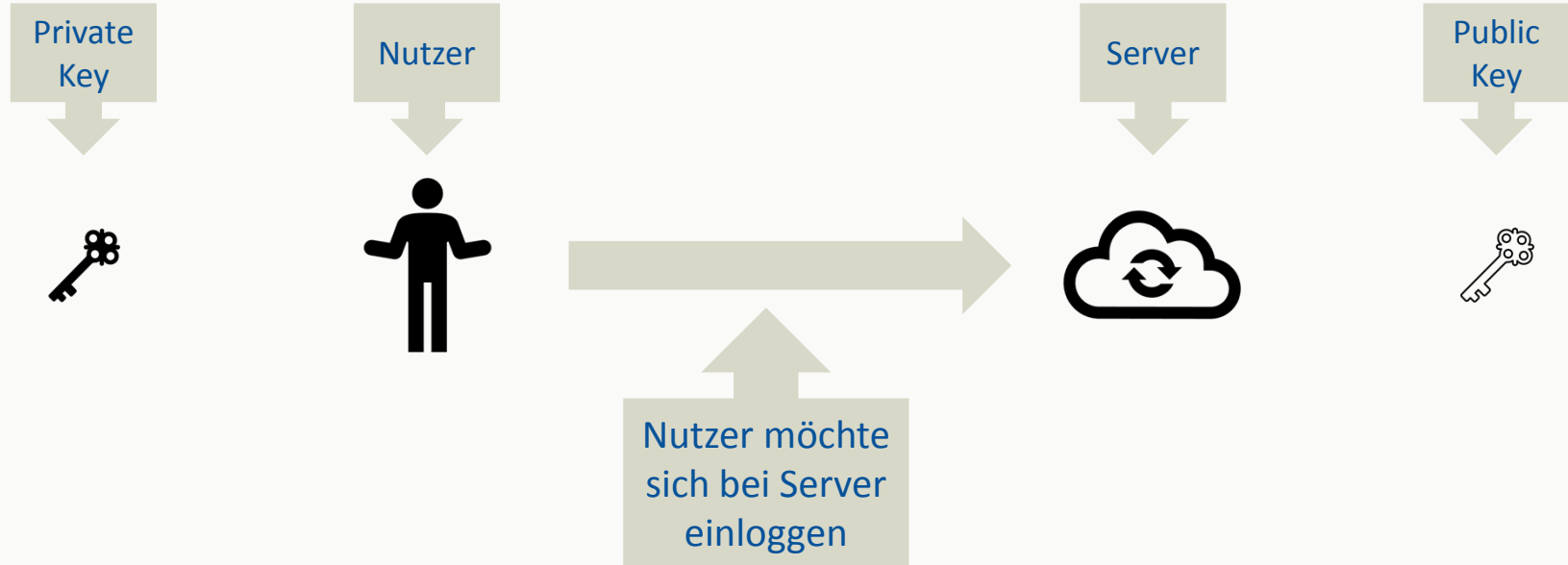


FUNKTIONSWEISE - REGISTRATION

Für jede Registrierung bei einem Webserver wird ein Key Pair erstellt.



FUNKTIONSWEISE - LOGIN



FUNKTIONSWEISE - LOGIN

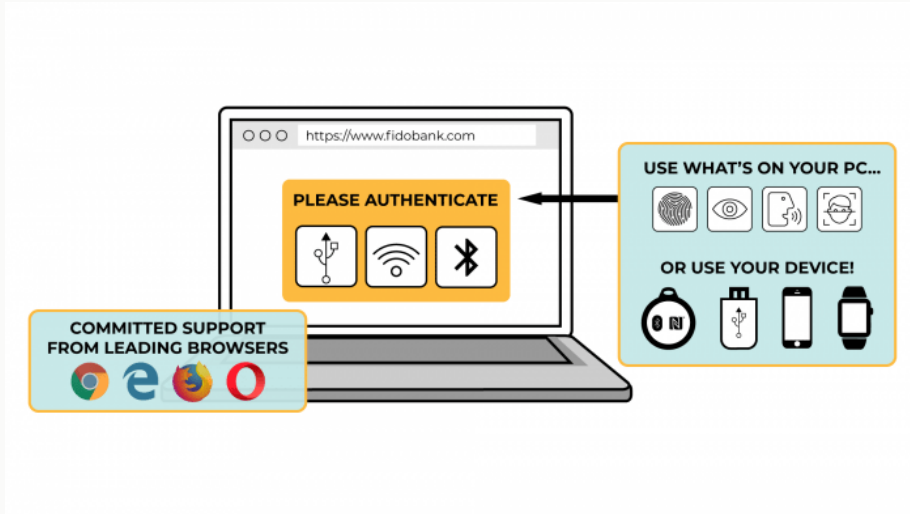


FUNKTIONSWEISE - LOGIN





WO WIRD DER PRIVATE KEY GESPEICHERT?



<https://blog.mtrix.de/blog/passwortlose-authentifizierung-fido2-und-webauthn>

Smartphone

Externer Authenticator
Bei Login mit Gerät verbinden zB
über USB oder NFC



Trusted Platform
Module Chip(TPM)

WAS GENAU UMFASST JETZT FIDO2?

Protokoll für Kommunikation zwischen
Client und Authenticator



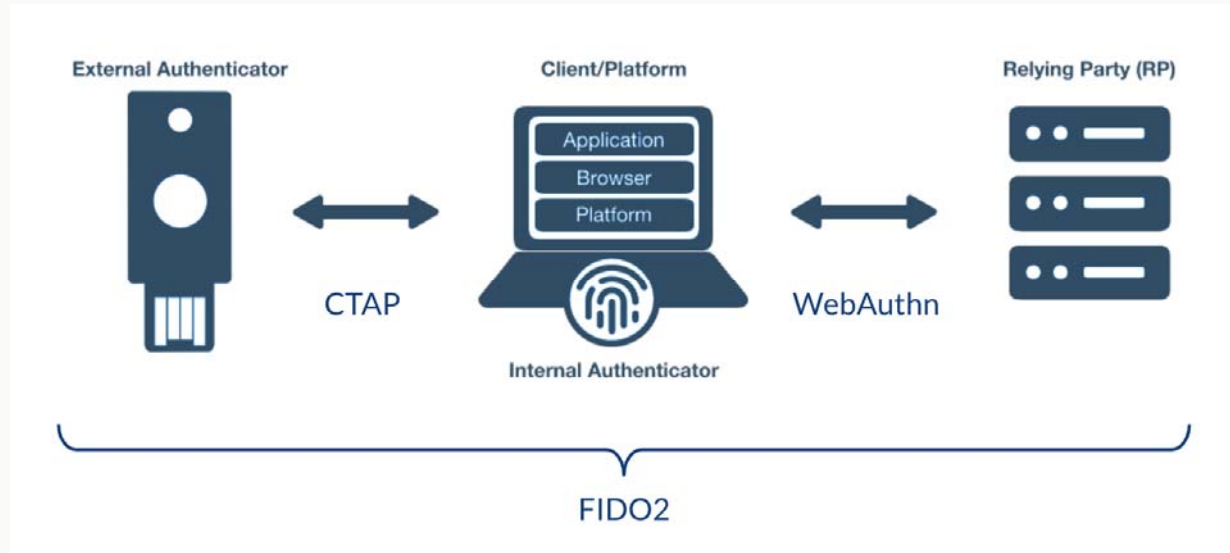
Client to Authenticator
Protocol(CTAP)



WebAuthn



API für Authentifizierung zwischen
Client und Server



<https://www.inovex.de/de/blog/fido2-webauthn-in-practice/>

POTENTIELLE PROBLEME

„Normale“
Endverbraucher
verstehen
möglicherweise
den Mehrwert
nicht.



"Mein Passwort Alligator13 ist so trivial
da kommt eh keiner drauf :D"

"Noch ein extra Gerät, dass auch noch
Geld kostet???"

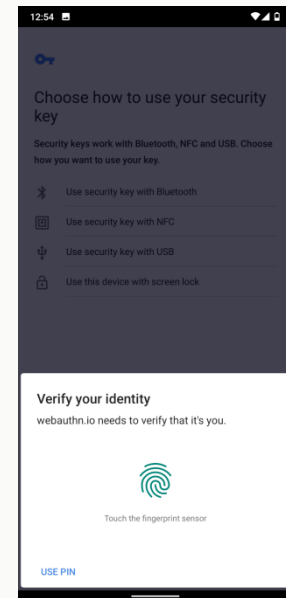
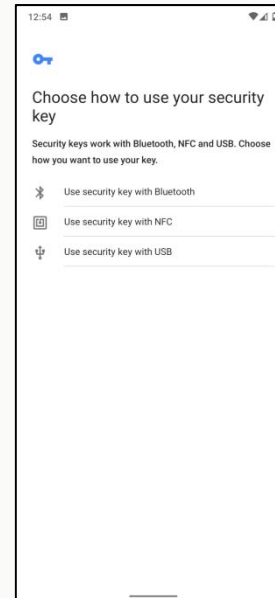
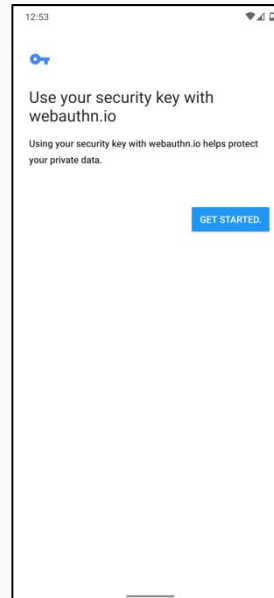
"Und wenn ich den Key verliere???
Passwort würde ich nie vergessen!"



POTENTIELLE ENABLER

„Mit Fingerabdruck ist das ja voll easy“

„Normale“
Endverbraucher
verstehen
möglicherweise
den Komfort!



FIDO-Allianz hat mittlerweile über 250 Mitglieder

Einige Websites ermöglichen
FIDO-Authentifizierung bereits



Chancen stehen gut, dass nach und nach weitere
Websites FIDO-Support anbieten werden

ZUSAMMENFASSUNG

Shared Secrets bringen
Probleme mit sich



FIDO2 löst diese mit
Public-Key-Pair Ansatz



Mehr und mehr
Unterstützung für FIDO2

Vielen Dank für die Aufmerksamkeit!

Fragen?

Nächste Vorlesung:

- Montag, 19. Juli 2021

Nächste Übung:

- Dienstag, 13. Juli 2021 – 16 Uhr
- Abgabe des Übungszettels 11 bis morgen – 16 Uhr
- Klausurtermine (vorläufig):
 - 1. Klausurtermin: 5. August 2021 im Zeitraum 10 – 13 Uhr
 - 2. Klausurtermin: 30. September 2021 im Zeitraum 10 – 13 Uhr