



Das Ende des Passworts?

Ein Überblick über Passkeys und den Stand der Forschung

November 2025

Internetkriminalität

Das Zeitalter des Passworts neigt sich dem Ende zu

Das Passwort ist die Versicherung im Netz – vor modernen An

ada-Magazin

Das Ende der Passwörter ist nah

nd fast immer nutzlos, weil sie leicht zu
ie passend, dass mehrere Start-ups an der
Passworts arbeiten.

DIGITALE SICHERHEIT

Ende des Passworts – So schützen Google, Apple und Microsoft bald unsere Daten



Von **Thomas Heuzeroth**
Wirtschaftsredakteur

Veröffentlicht am 05.05.2022 | Lesedaue

Cyberkriminalität

Apple und Co wollen Passwort ersetzen: Anmelden mit Passkeys

Berlin. Viele sind mit ihren Zugangsdaten im Netz leichtsinnig. Eine Allianz um Google und Apple will das Anmelden vereinfachen – so geht's.



Von Maik Henschke, Redakteur im Ressort Ratgeber/Wissen
27.01.2023, 06:21 Uhr

Berliner Morgenpost

Handelsblatt



A word cloud centered around the term "Passkeys". The words are arranged in a circular pattern, with "Passkeys" being the largest and most central. Other prominent words include "FIDO2", "U2F", "CTAP", "Attestation", "Yubikey", "Hardware Token", "Relying Party", "UAF", "WebAuthn", "Security Key", "MFA", "FIDO Alliance", "Passwordless Authentication", and "Platform Authenticator". The background features a repeating pattern of large, light gray circular shapes.

FIDO2

Yubikey

Hardware Token

CTAP

Attestation

Relying Party

U2F

Passkeys

Platform Authenticator

UAF

WebAuthn

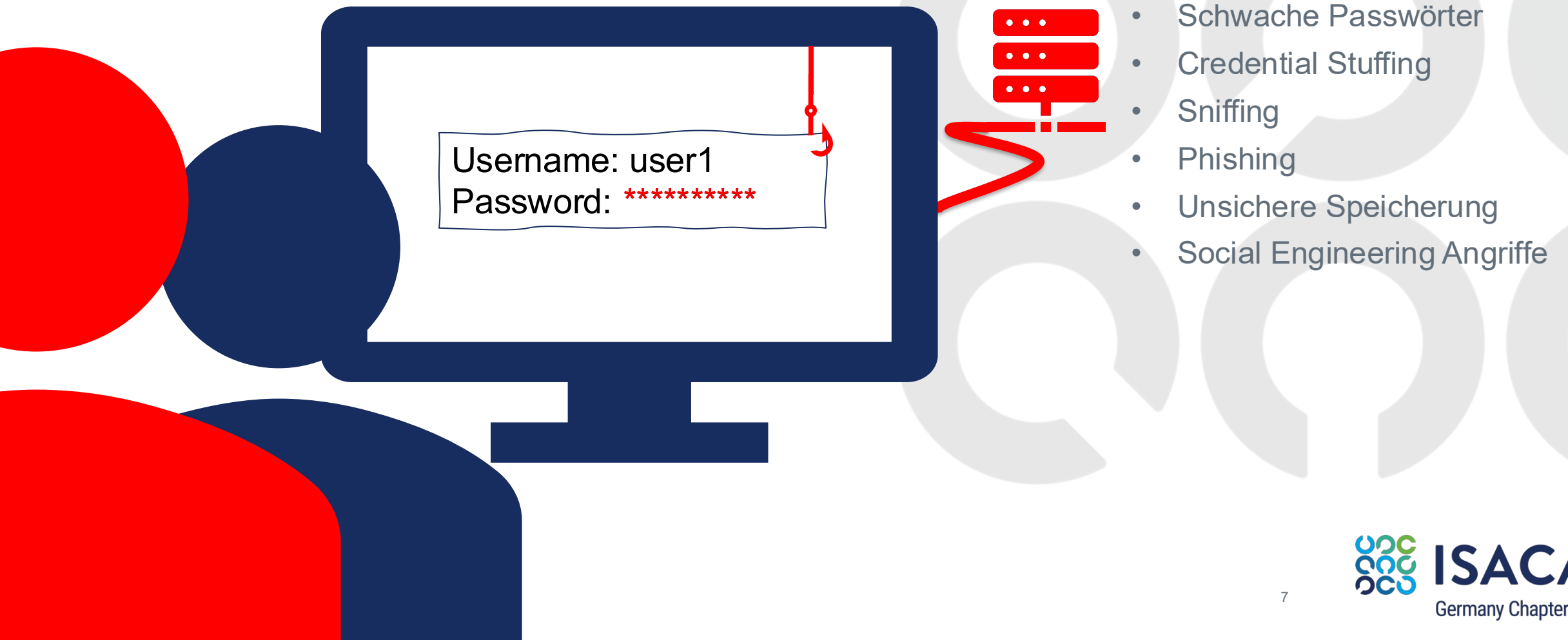
Security Key

MFA

Passwordless Authentication

FIDO Alliance

Bedrohungen für passwort-basierte Authentifizierung



Fast IDentity Online

- ein offener weltweiter Branchenverband
- Mitglieder wie Google, Microsoft, Meta und Apple



Registrierung

mit Security Key

Sign in

Username*

Password*

Not registered? [Click here](#) to create a new account.

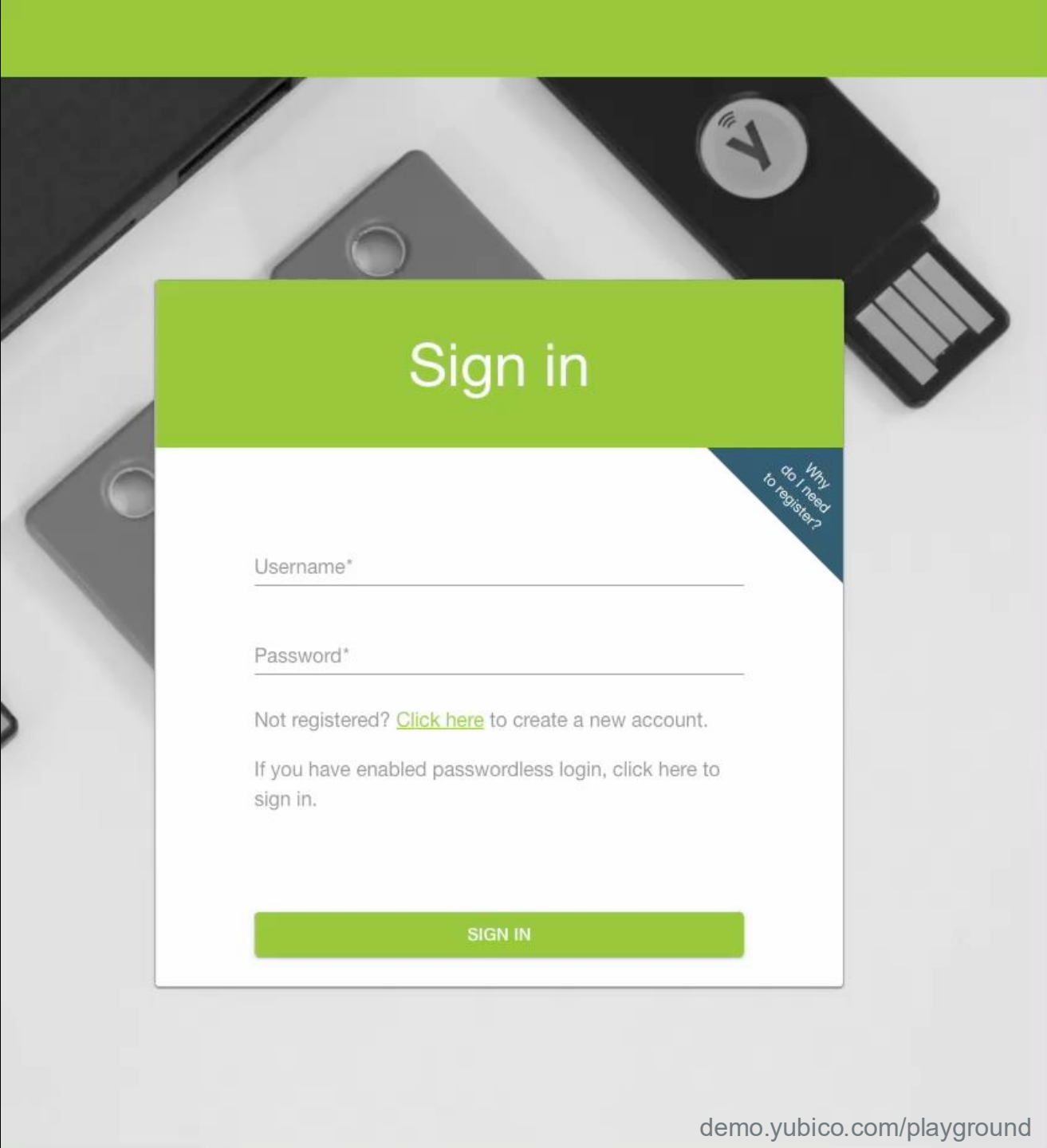
If you have enabled passwordless login, click here to sign in.

SIGN IN

Why
do I need
to register?

Authentifizierung

mit Security Key



Sign in

Username*

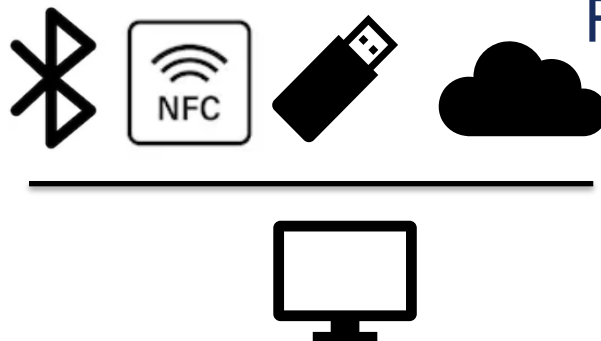
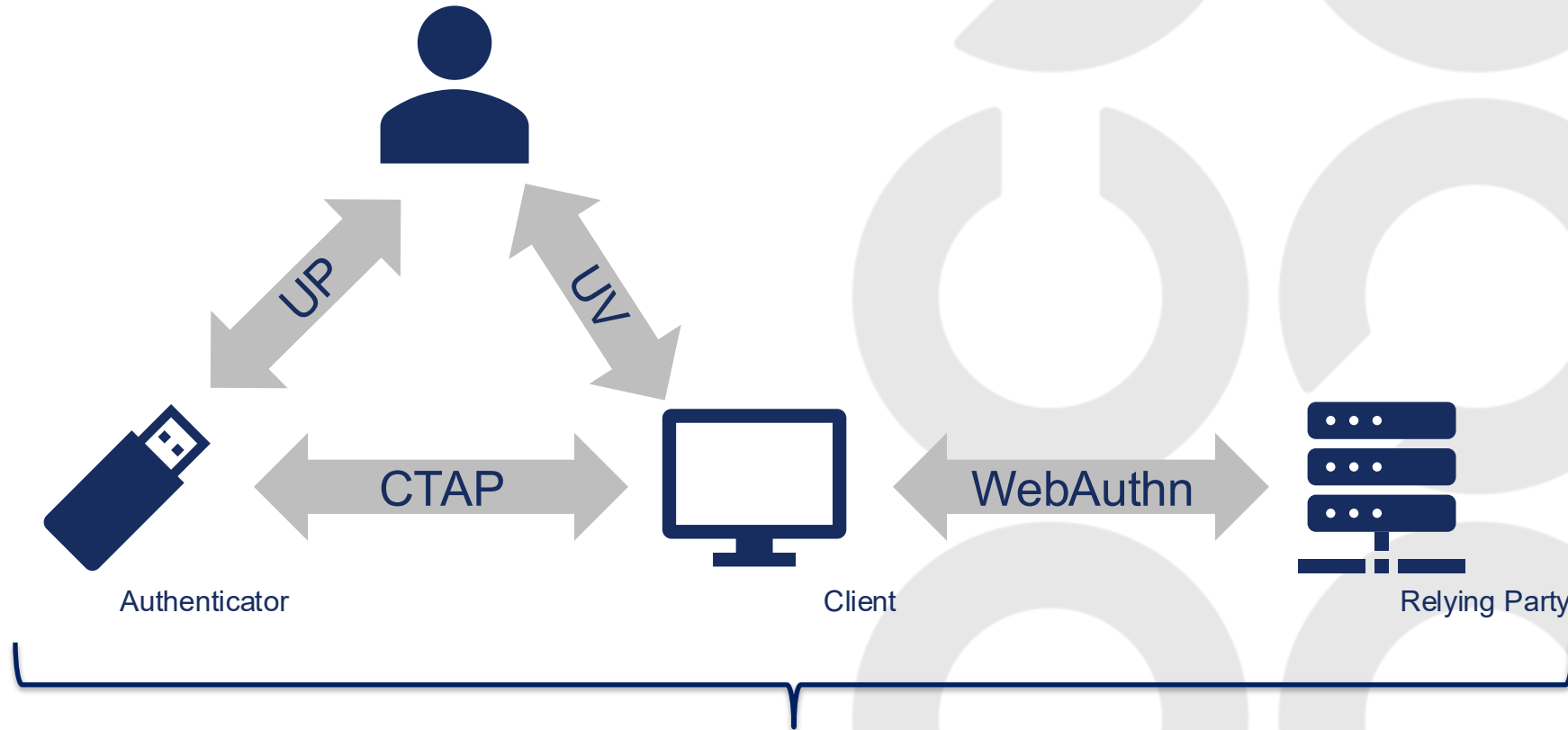
Password*

Not registered? [Click here](#) to create a new account.

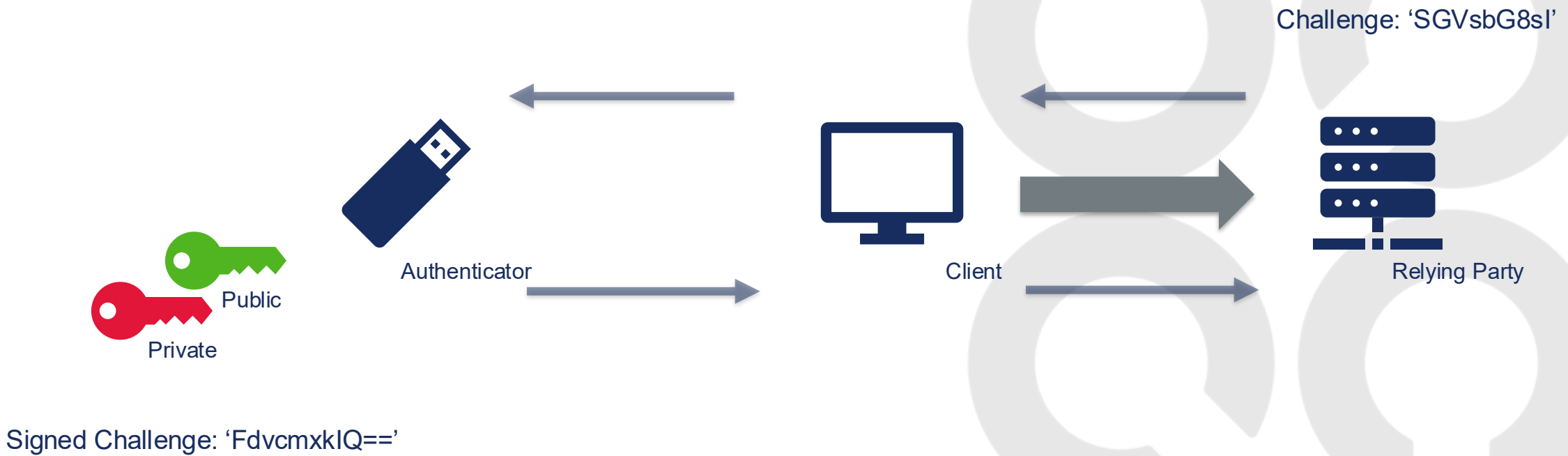
If you have enabled passwordless login, click here to sign in.

SIGN IN

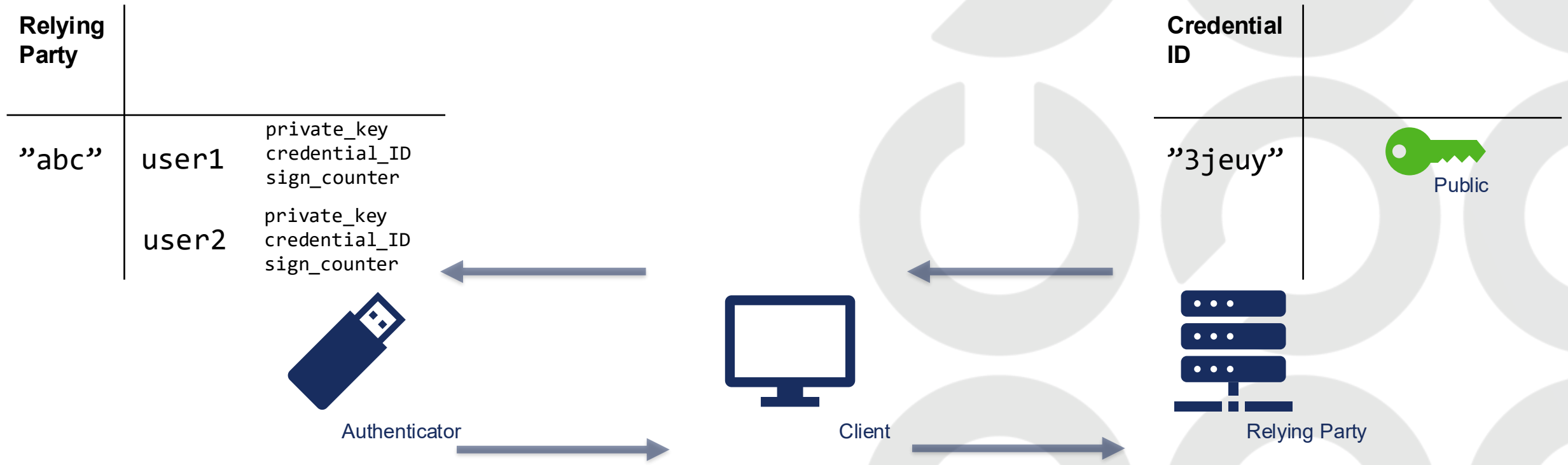
Why do I need to register?



UP: User Presence
UV: User Verification
CTAP: Client To
Authenticator Protocol



Speicherung

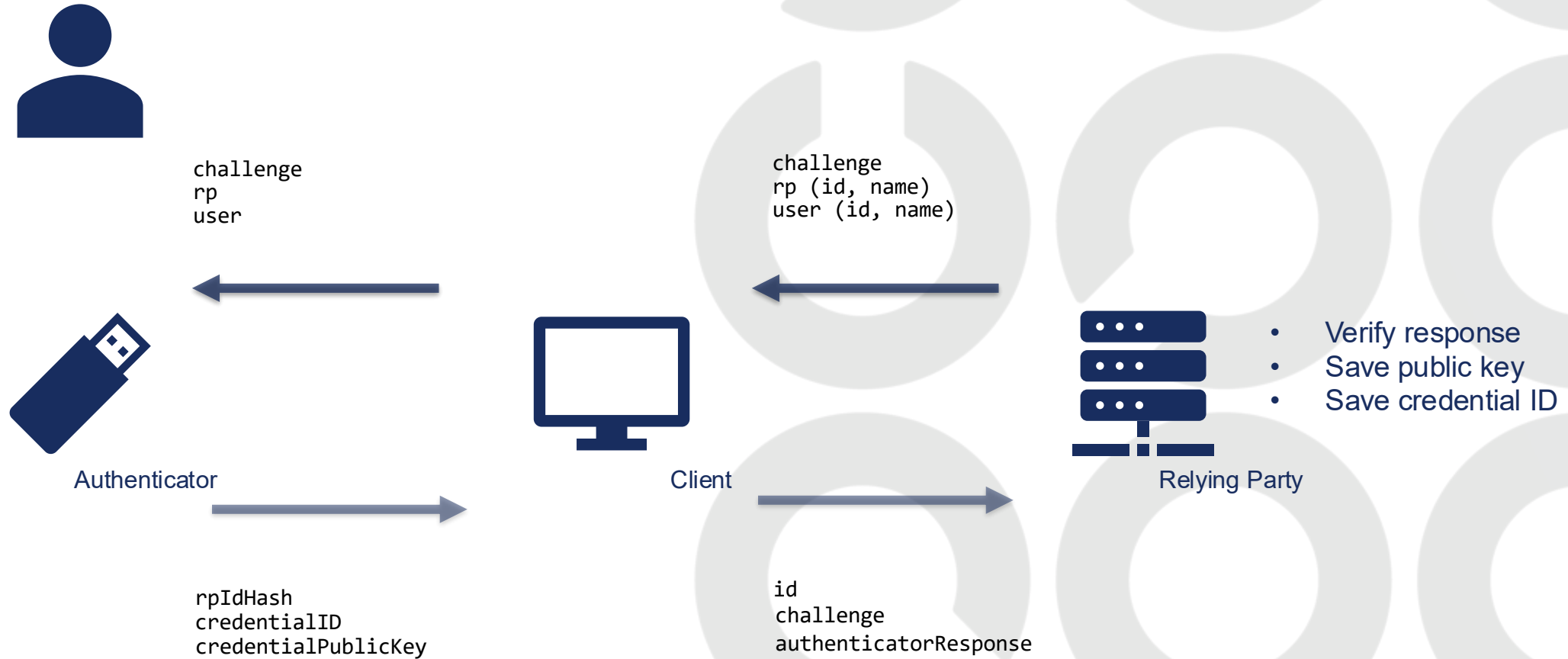


Registration

Credential Stuffing

Schwache Passwörter
Sniffing & Phishing
Unsichere Speicherung
Social Engineering Angriffe

- Validate request
- Generate key pair



Registration

- Credential Stuffing
- Schwache Passwörter**
- Sniffing & Phishing
- Unsichere Speicherung
- Social Engineering Angriffe

Schwache Passwörter

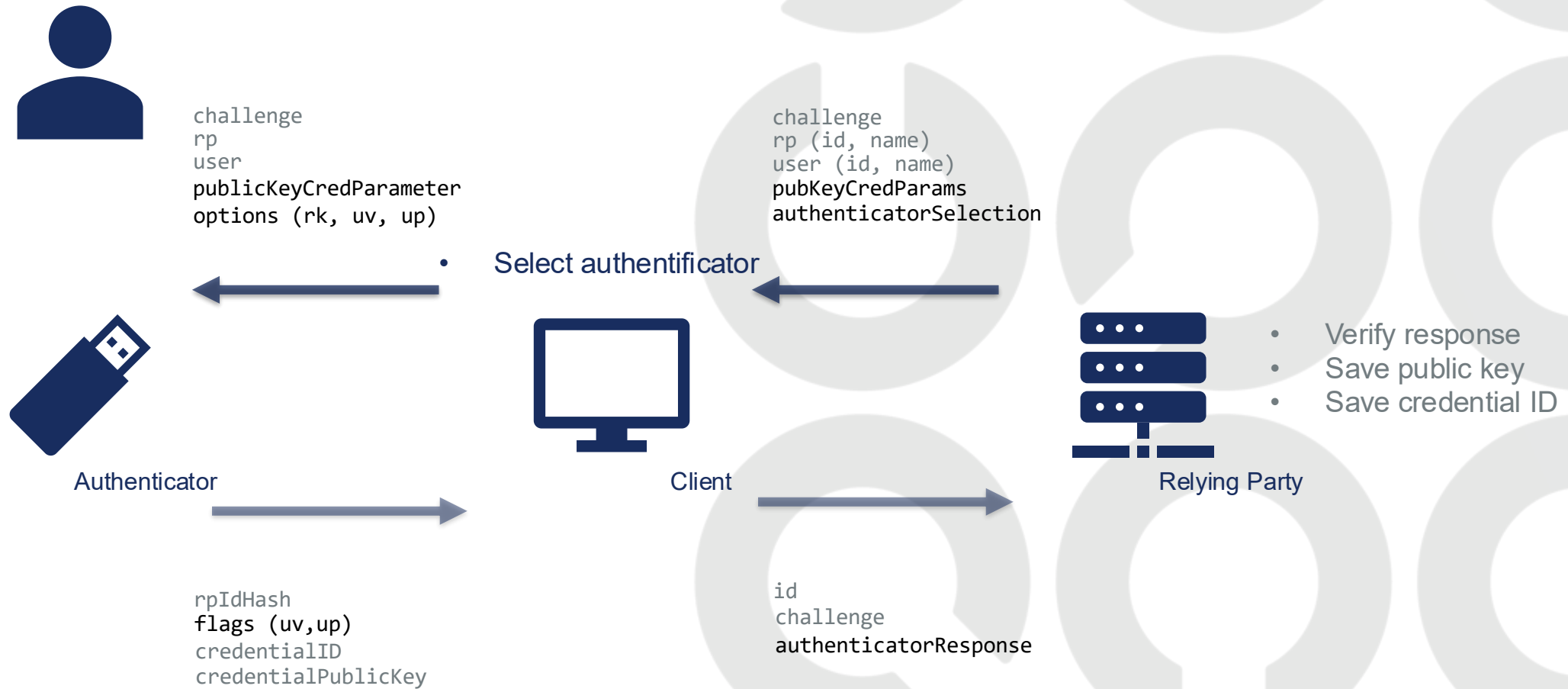
- Sniffing & Phishing
- Unsichere Speicherung
- Social Engineering Angriffe

- Sniffing & Phishing
- Unsichere Speicherung
- Social Engineering Angriffe

Unsichere Speicherung Social Engineering Angriffe

Social Engineering Angriffe

- Validate request
- Choose algorithm
- Verify user (presence)
- Generate key pair



Registration

Credential Stuffing

Schwache Passwörter

Sniffing & Phishing

Unsichere Speicherung

Social Engineering Angriffe

- Validate request
- Choose algorithm
- Verify user (presence)
- **Check existing credentials**
- Generate key pair



challenge
rp
user
publicKeyCredParameter
excludeList
options (rk, uv, up)



Authenticator

rpIdHash
flags (uv, up)
credentialID
credentialPublicKey

• Select authenticator



Client

challenge
rp (id, name)
user (id, name)
pubKeyCredParams
authenticatorSelection
excludeCred

id
challenge
authenticatorResponse



Relying Party

- Verify response
- Save public key
- Save credential ID

Authentication

Credential Stuffing

Schwache Passwörter
Sniffing & Phishing
Unsichere Speicherung
Social Engineering Angriffe

- Validate inputs
- Generate signature



Authenticator

challenge
rpId



credentialId
signature (authData)



Client

challenge



id
signature



Relying Party

- Get public key
- Verify signature

Authentication

Credential Stuffing

Schwache Passwörter

Sniffing & Phishing

Unsichere Speicherung

Social Engineering Angriffe



challenge
rpId



Authenticator



```
credential (id, type, transport)
authData
  credentialId
  credentialPublicKey
signature (authData)
```



Client

challenge



```
id
authData
signature
```



Relying Party

- Get public key
- Verify signature

Authentication

Credential Stuffing

Schwache Passwörter

Sniffing & Phishing

Unsichere Speicherung

Social Engineering Angriffe



clientDataHash
rpId



Authenticator



credential (id, type, transport)
authData
rpIdHash
flags
credentialId
credentialPublicKey
signature (authData)
user

challenge



Client



id
authData
signature
user



Relying Party

- Verify response
- Get public key
- Verify signature

Authentication

Credential Stuffing

Schwache Passwörter

Sniffing & Phishing

Unsichere Speicherung

Social Engineering Angriffe

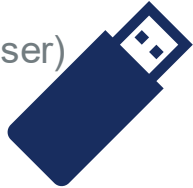


clientDataHash
rpId
allowlist
options (up,uv)

- Select authenticator

challenge
allowCredentials (id, type, transport)

- Validate inputs
- Select credentials (by user)
- Verify user (presence)
- Generate signature



Authenticator



Client



Relying Party

- Verify response
- Get public key
- Verify signature

credential (id, type, transport)
authData
rpIdHash
flags
credentialId
credentialPublicKey
signature (authData)
user

id
authData
signature
user

Authentication

Credential Stuffing
Schwache Passwörter
Sniffing & Phishing
Unsichere Speicherung
Social Engineering Angriffe



clientDataHash
rpId
allowlist
options (up,uv)

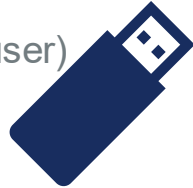
clientData
type
challenge
origin
crossOrigin
tokenBinding

challenge
allowCredentials (id, type, transport)

- Create clientData
- Select authenticator



- Validate inputs
- Select credentials (by user)
- Verify user (presence)
- Generate signature



Authenticator



Client



Relying Party

- Verify response
- Get public key
- Verify signature

credential (id, type, transport)
authData
rpIdHash
flags
credentialId
credentialPublicKey
signature (authData, clientDataHash)
user

id
authData
clientData
signature
user



Authentication

Credential Stuffing
Schwache Passwörter
Sniffing & Phishing
Unsichere Speicherung
Social Engineering Angriffe

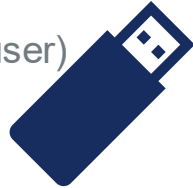


clientData
type
challenge
origin
crossOrigin
tokenBinding

clientDataHash
rpId
allowlist
options (up,uv)

- Create clientData
- Select authenticator

challenge
allowCredentials (id, type, transport)



Authenticator



Client



Relying Party

- Verify response
- Get public key
- Verify signature
- Check counter

credential (id, type, transport)
authData
rpIdHash
flags
signCount
credentialId
credentialPublicKey
signature (authData, clientDataHash)
user

id
authData
clientData
signature
user

- Validate inputs
- Select credentials (by user)
- Verify user (presence)
- **Increase counter**
- Generate signature

Registration

Credential Stuffing
Schwache Passwörter
Sniffing & Phishing
Unsichere Speicherung
Social Engineering Angriffe

- Validate request
- Choose algorithm
- Verify user (presence)
- Check existing credentials
- Generate key pair



Authenticator

clientDataHash
rp
user
publicKeyCredParameter
excludeList
options (rk, uv, up).



rpIdHash
flags (uv, up)
credentialID
credentialPublicKey

clientData
type
challenge
origin
crossOrigin
tokenBinding

Create clientData
Select authenticator



Client

challenge
rp (id, name)
user (id, name)
pubKeyCredParams
authenticatorSelection
excludeCred



id
clientData
type
challenge
origin
crossOrigin
tokenBinding
authenticatorResponse



Relying Party

- Verify response
- Save public key
- Save credential ID

Registration

Credential Stuffing
Schwache Passwörter
Sniffing & Phishing
Unsichere Speicherung
Social Engineering Angriffe

- Validate request
- Choose algorithm
- Verify user (presence)
- Check existing credentials
- Generate key pair
- Set counter to 0



Authenticator

clientDataHash
rp
user
publicKeyCredParameter
excludeList
options (rk, uv, up).



authData
rpIdHash
flags (uv, up)
signCount
credentialID
credentialPublicKey



clientData
type
challenge
origin
crossOrigin
tokenBinding

Create clientData
Select authenticator



Client

challenge
rp (id, name)
user (id, name)
pubKeyCredParams
authenticatorSelection
excludeCred

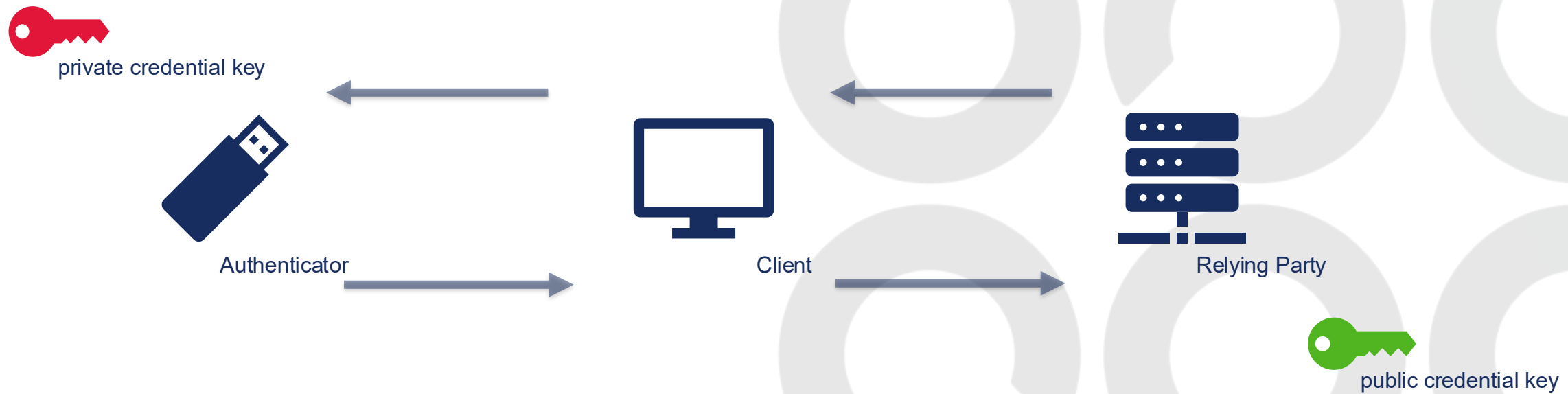


id
clientData
type
challenge
origin
crossOrigin
tokenBinding
authData

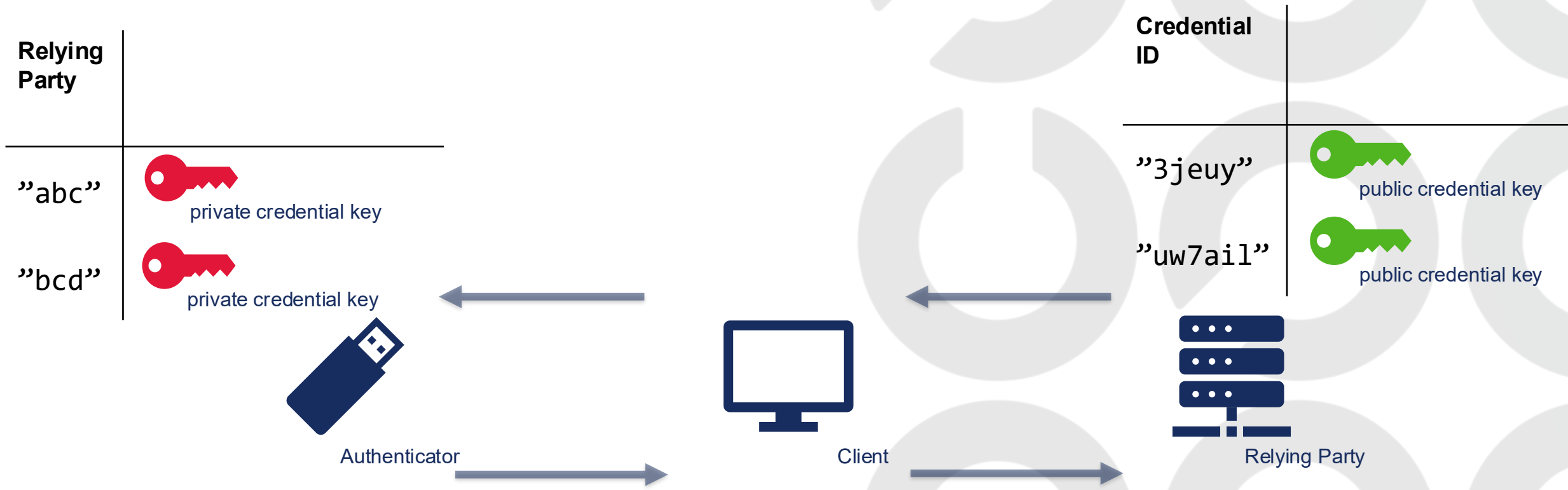


Relying Party

- Verify response
- Set counter to 0
- Save public key
- Save credential ID



Attestation



- Basic attestation
- Self attestation
- Attestation CA
- No attestation
- Anonymized CA
- Enterprise Attestation

private credential key



private attestation key



Authenticator



Client



Metadata Service



Relying Party

public credential key



public attestation key



Metadata BLOB

aaguid

Registration

Credential Stuffing
Schwache Passwörter
Sniffing & Phishing
Unsichere Speicherung
Social Engineering Angriffe

- Validate request
- Choose algorithm
- Verify user (presence)
- Check existing credentials
- Generate key pair
- Set counter to 0



Authenticator

clientDataHash
rp
user
publicKeyCredParameter
excludeList
options (rk, uv, up).



authData
rpIdHash
flags (uv, up)
signCount
credentialID
credentialPublicKey



clientData
type
challenge
origin
crossOrigin
tokenBinding

Create clientData
Select authenticator



Client

challenge
rp (id, name)
user (id, name)
pubKeyCredParams
authenticatorSelection
excludeCred



id
clientData
type
challenge
origin
crossOrigin
tokenBinding
authData

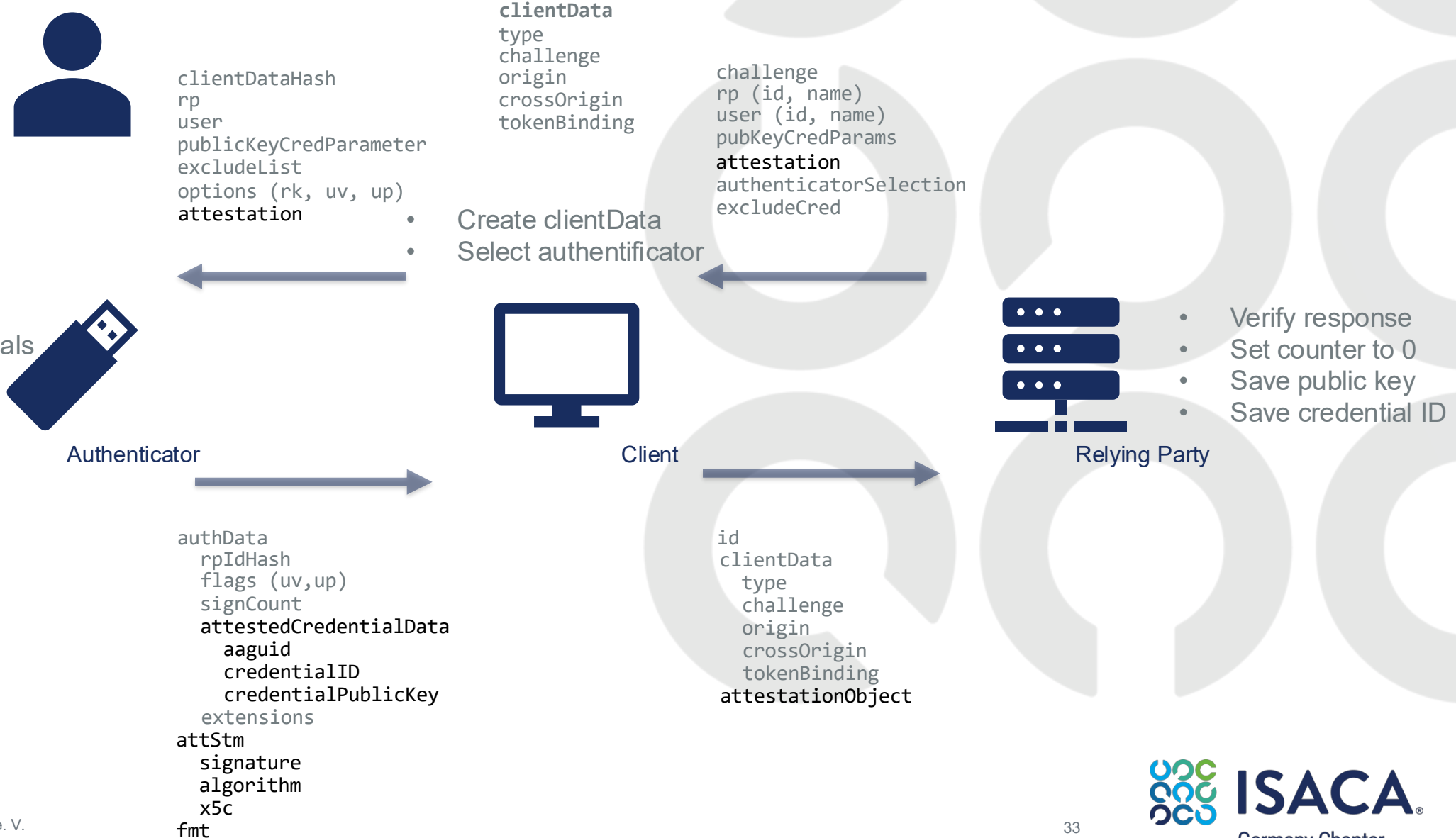


Relying Party

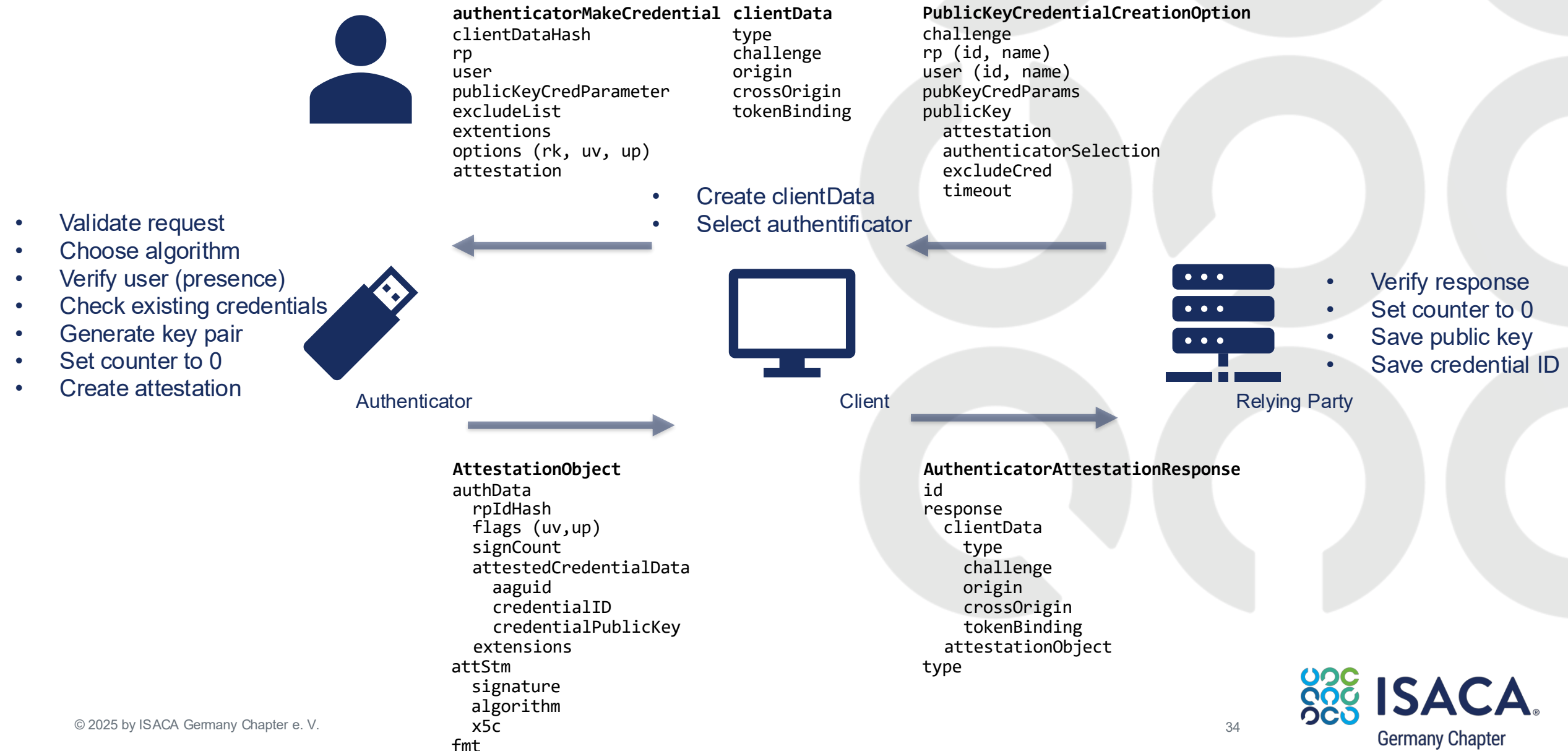
- Verify response
- Set counter to 0
- Save public key
- Save credential ID

Registration

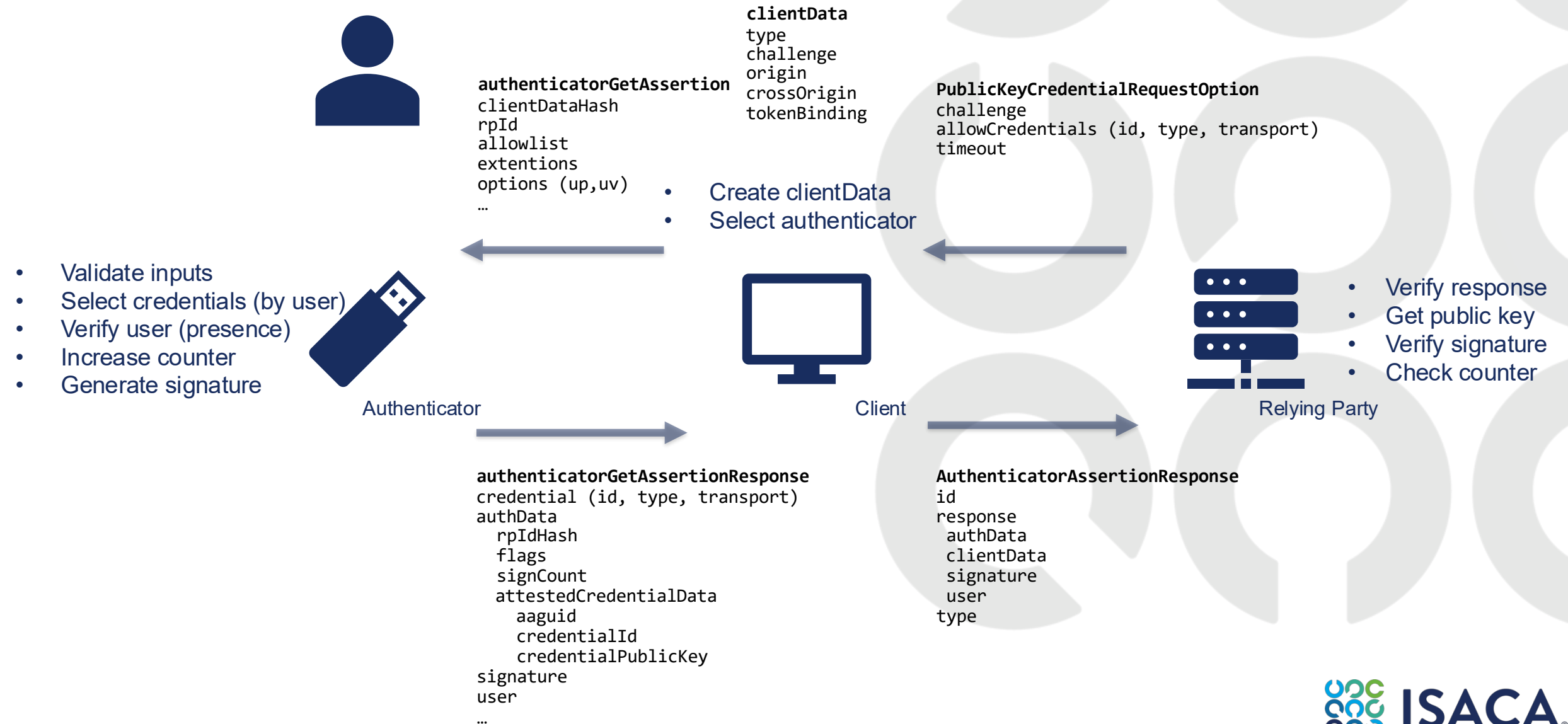
- Validate request
- Choose algorithm
- Verify user (presence)
- Check existing credentials
- Generate key pair
- Set counter to 0
- Create attestation



Registration



Authentication





A word cloud featuring various terms related to authentication and security. The words are arranged in a circular pattern, with some appearing more prominently than others. The terms include:

- FIDO2
- Yubikey
- Hardware Token
- CTAP
- U2F
- Attestation
- Relying Party
- Passkeys
- Platform Authenticator
- UAF
- WebAuthn
- Security Key
- Passwordless Authentication
- MFA
- FIDO Alliance

Standards und Protokolle

- FIDO2
 - CTAP
 - WebAuthn
- UAF
- U2F

Passkeys

Authenticator - Typen

- Platform Authenticator
- Roaming Authenticator
 - Yubikey
 - Hardware Token
 - Security Key

Authentifizierungsarten

- Password-based Authentication
- Passwordless Authentication
- MFA

Standards und Protokolle

- FIDO2
 - CTAP
 - WebAuthn
- UAF
- U2F

Schlüsselarten

- Discoverable credentials / resident keys **Passkeys**
- Non-discoverable credentials

Authenticator - Typen

- Platform Authenticator
- Roaming Authenticator
 - Yubikey
 - Hardware Token
 - Security Key

Authentifizierungsarten

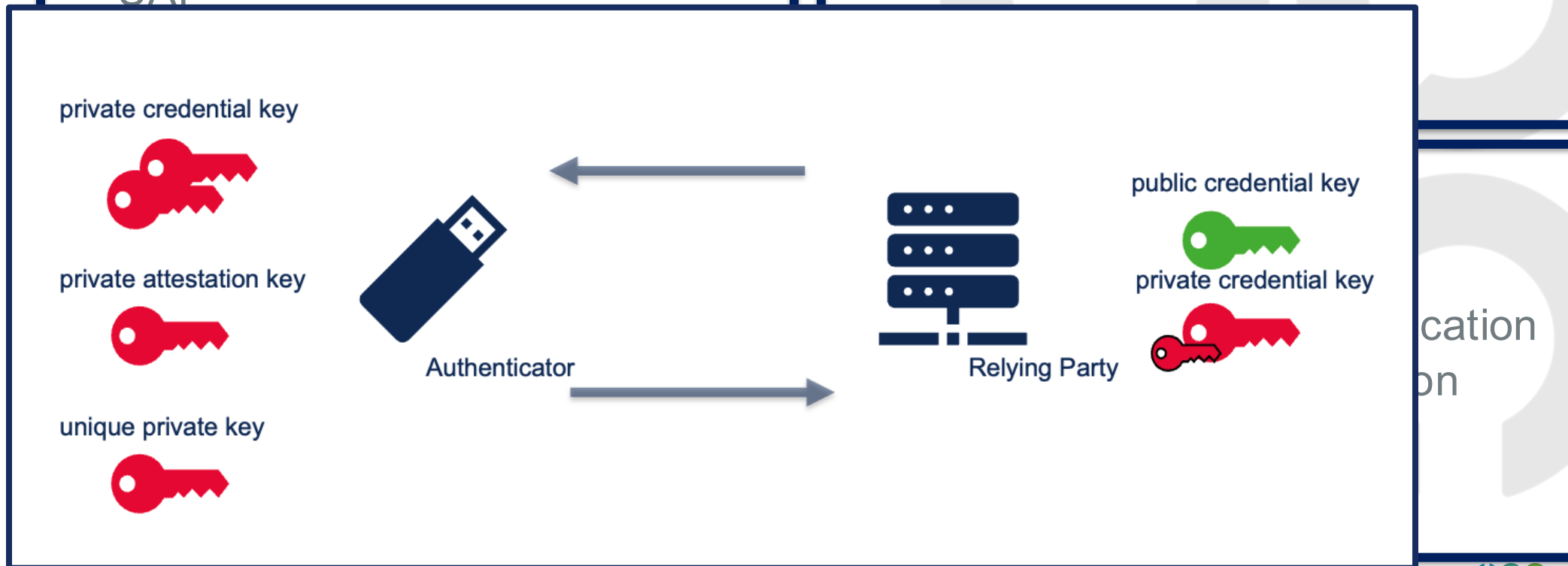
- Password-based Authentication
- Passwordless Authentication
- MFA

Standards und Protokolle

- FIDO2
 - CTAP
 - WebAuthn
- UAF

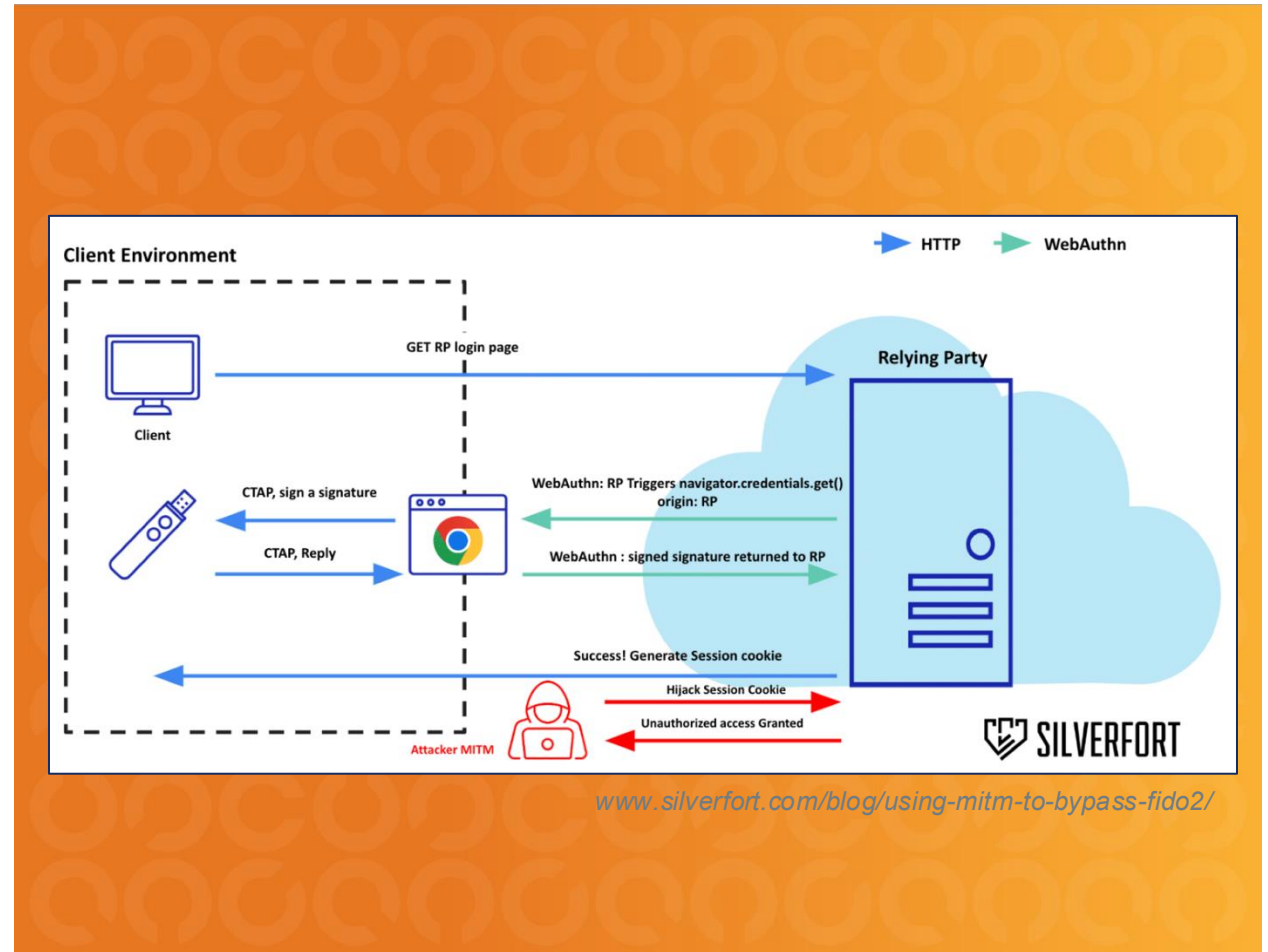
Schlüsselarten

- Discoverable credentials / resident keys
- Non-discoverable credentials



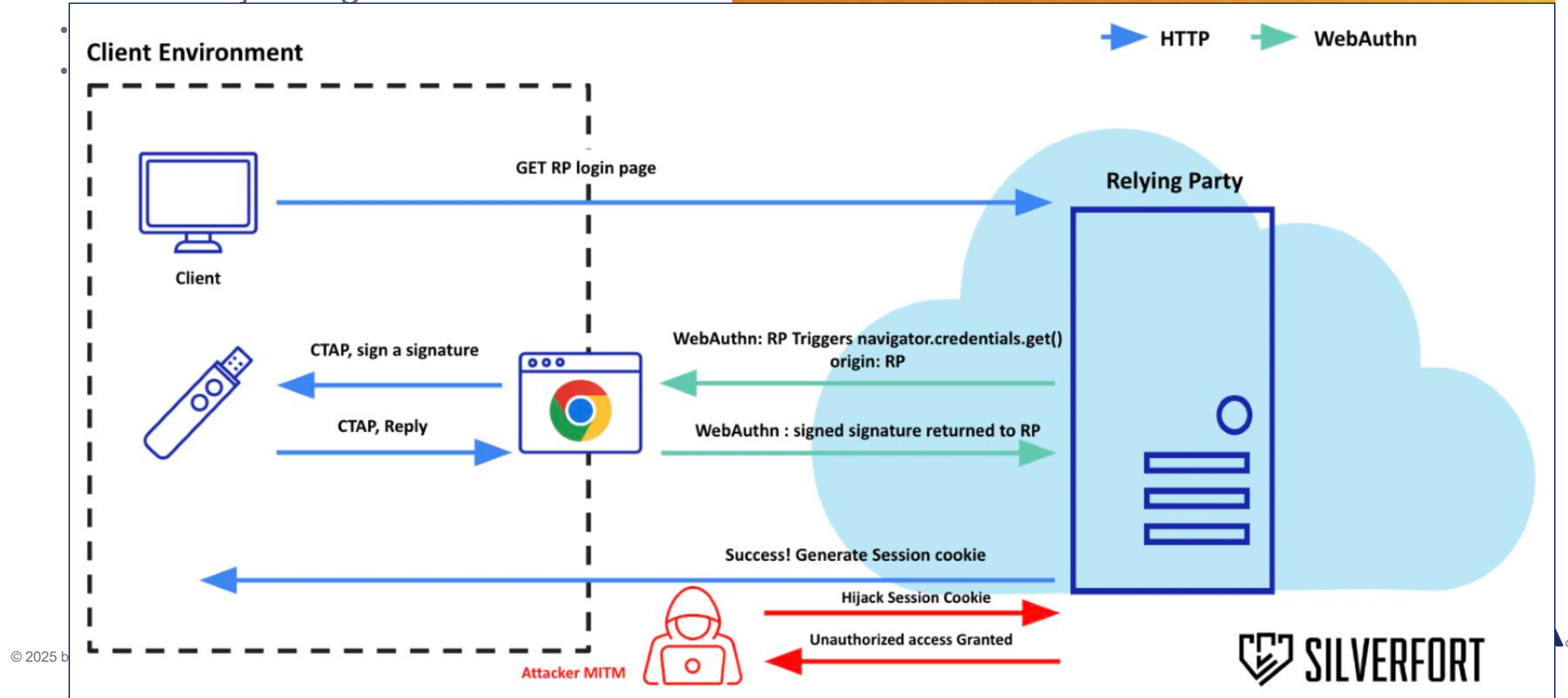
Schwachstellen bei Nutzung von FIDO2

- Session Hijacking
 - Silverfort
 - Veröffentlicht am 06.05.2024



Schwachstellen bei Nutzung von FIDO2

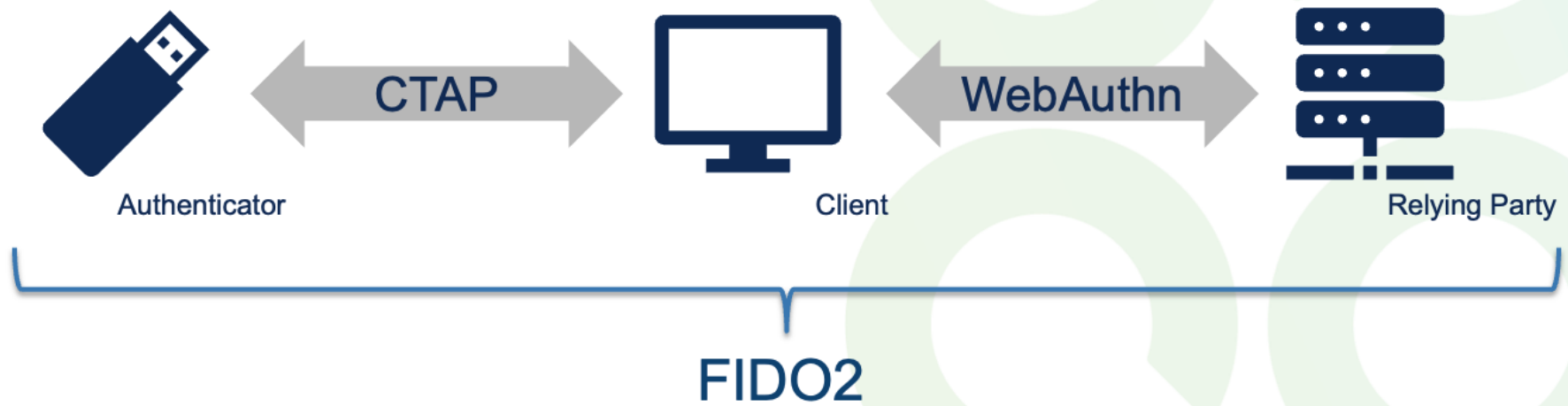
- Session Hijacking

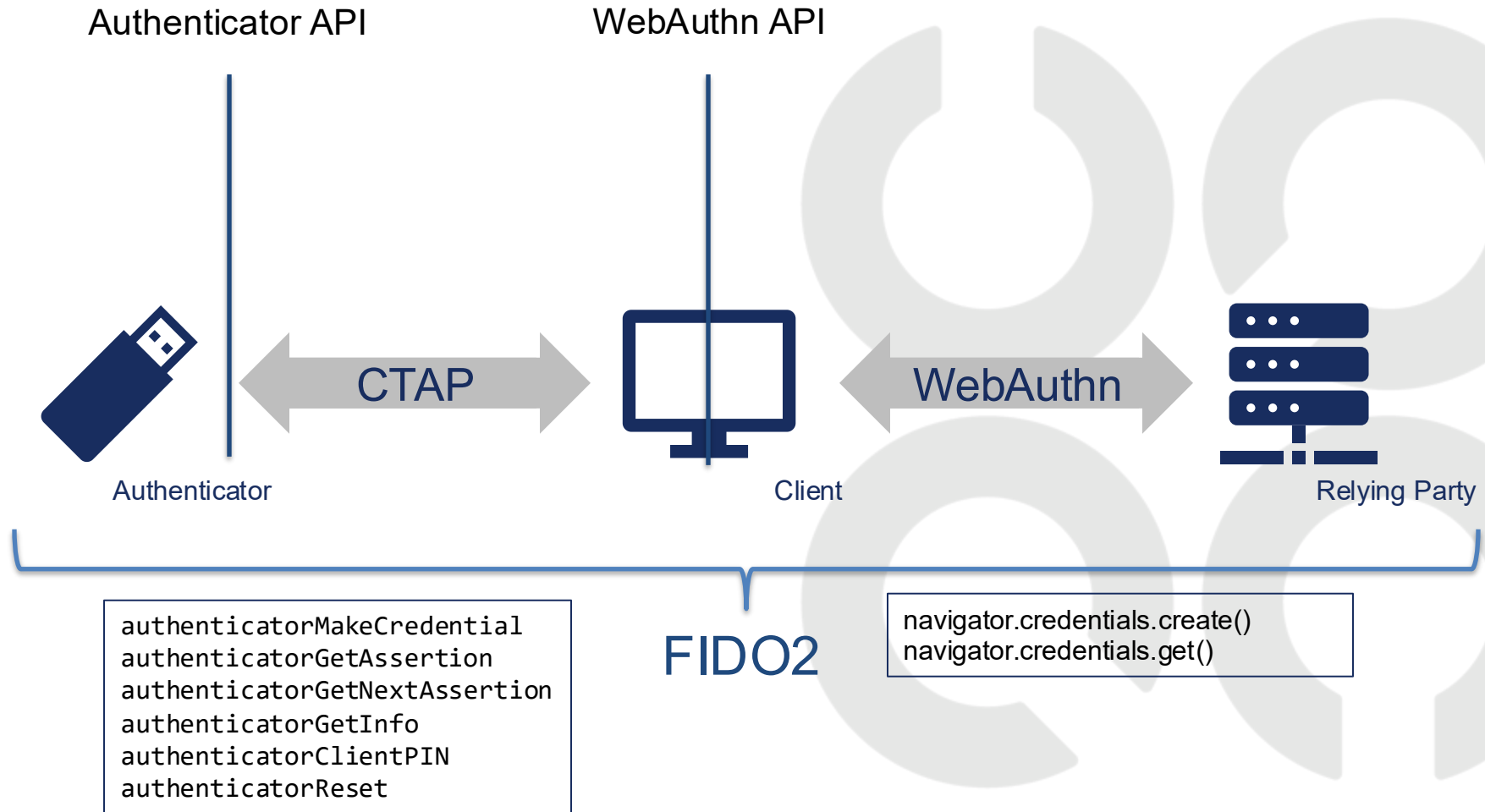


Schwachstellen bei Nutzung von FIDO2

- CTRAPS:
CTAP Client Impersonation and API Confusion
 - Marco Casagrande, Daniele Antonioli
 - Veröffentlicht am 03.12.2024
 - CVE-2024-35311 (Yubico)

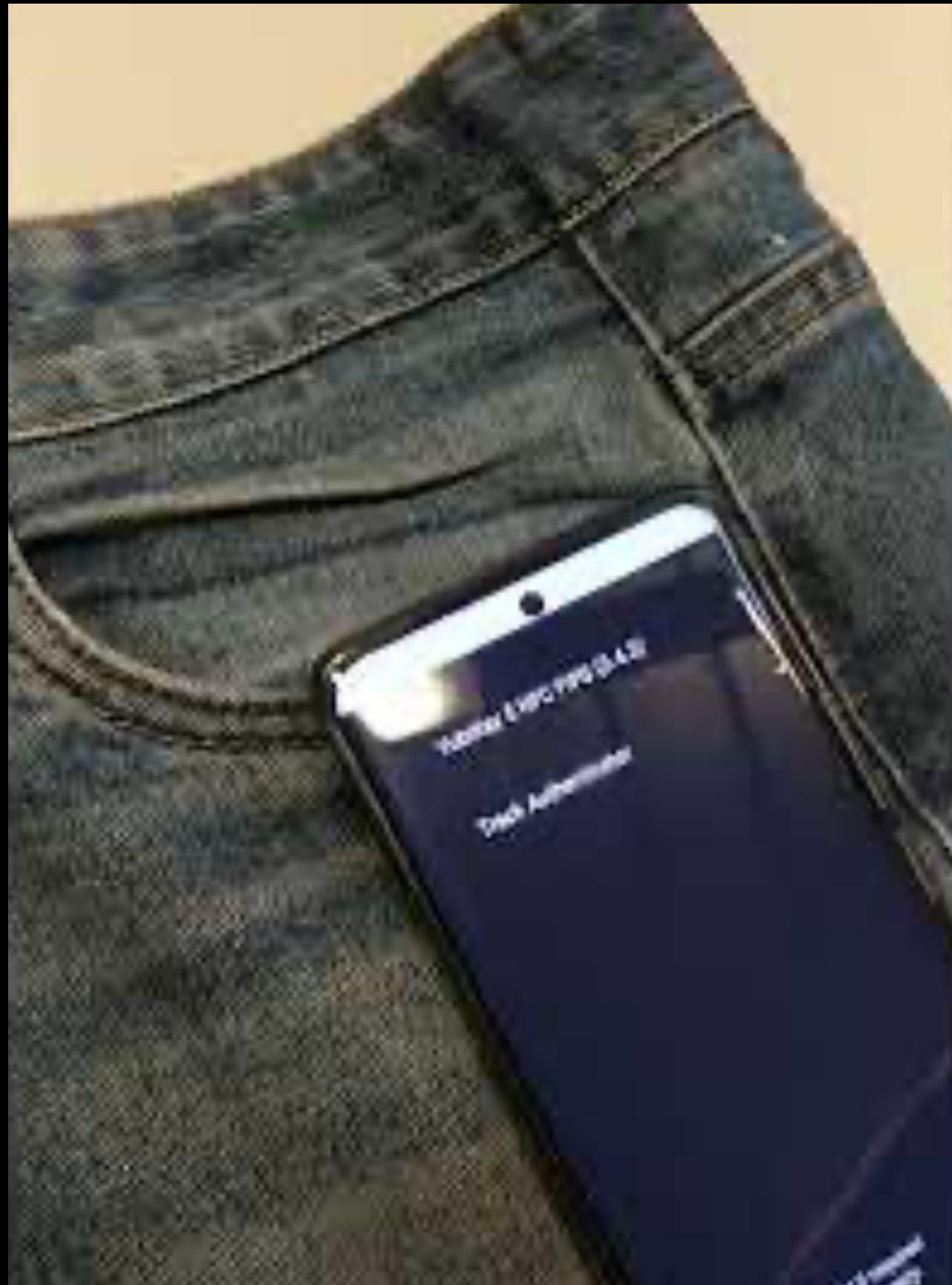






CTRAPS

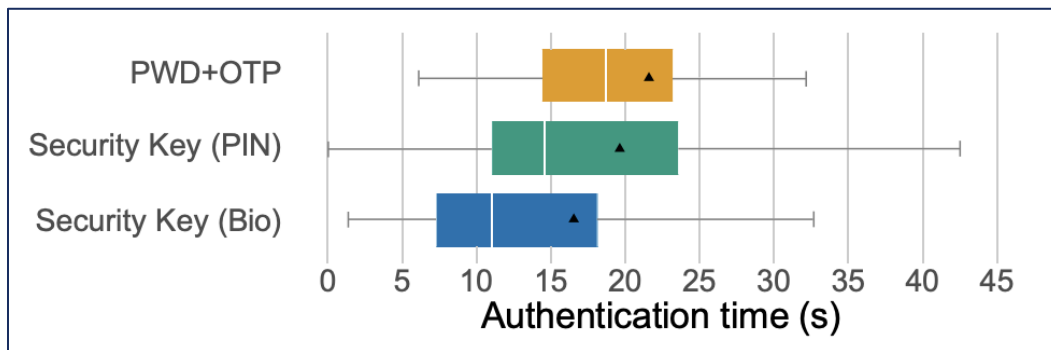
Credential Discovery



<https://www.youtube.com/watch?v=9n4YxWikAe8>

FIDO2 in der Praxis

- Geringerer Zeitaufwand für Authentifizierung
- Höhere Erfolgsrate bei der Authentifizierung mit Passkeys
- Erfolgreiche Phishing reduziert



<https://www.usenix.org/system/files/soups2025-lassak.pdf>



<https://fidoalliance.org/wp-content/uploads/2025/10/FIDO-Passkey-Index-October-2025.pdf>

FIDO2 in der Praxis

- Passkeys bieten hohe Sicherheit
- Trotz breiter OS-Unterstützung langsame Adoption in Unternehmen

32 Interviews mit

- FIDO Experten
- IAM Experten
- Organisationen (hauptsächlich CISOs)



Hürden bei der Einführung von Passkeys



Internetkriminalität

Das Zeitalter des Passworts neigt sich dem Ende zu

Das Passwort ist die Versicherung im Netz – vor modernen An

ada-Magazin

Das Ende der Passwörter ist nah

nd fast immer nutzlos, weil sie leicht zu
ie passend, dass mehrere Start-ups an der
Passworts arbeiten.

DIGITALE SICHERHEIT

Ende des Passworts – So schützen Google, Apple und Microsoft bald unsere Daten



Von **Thomas Heuzeroth**
Wirtschaftsredakteur

Veröffentlicht am 05.05.2022 | Lesedaue

Cyberkriminalität

Apple und Co wollen Passwort ersetzen: Anmelden mit Passkeys

Berlin. Viele sind mit ihren Zugangsdaten im Netz leichtsinnig. Eine Allianz um Google und Apple will das Anmelden vereinfachen – so geht's.

Handelsblatt

Eine Zukunft mit weniger Passwörtern – nicht ohne.



ISACA®

Germany Chapter

Das Ende des Passworts?

Ein Überblick über Passkeys und den Stand der Forschung

November 2025