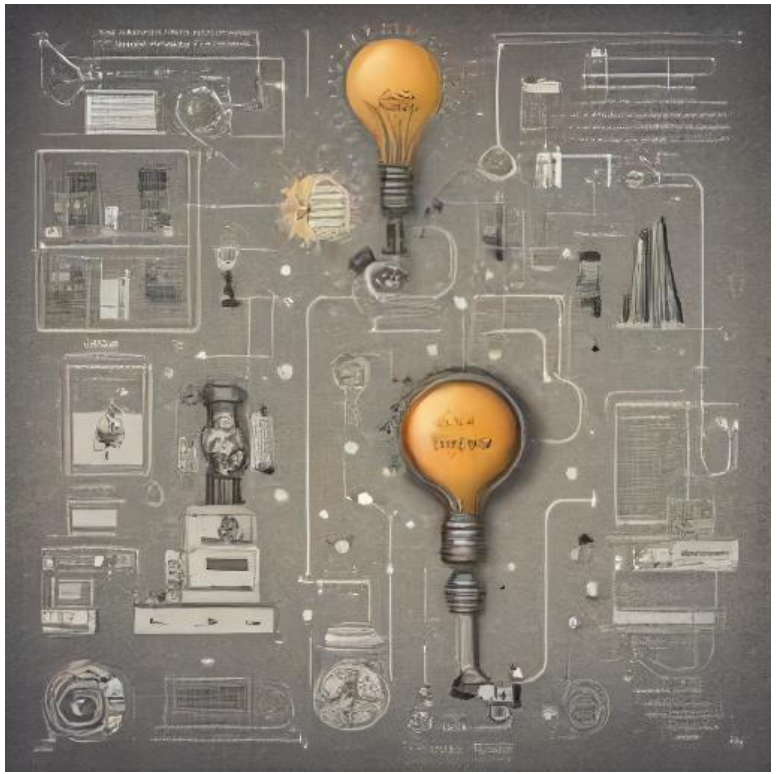
A-SIT

Innovationen im Bereich ID Austria

Dr. Arne Tauber

Um was geht es heute?

- A-SIT / EGIZ stehen für Technologiebeobachtung und Innovation
- Zwei ausgewählte Themen
  - Usability
    - Passkeys
  - Privacy
    - Stammzahl-basierte Pseudonyme



Passkeys

sozialversicherung.at

SV-TRÄGER

Meine SV

Suchbegriff eingeben

Österreichische Sozialversicherung

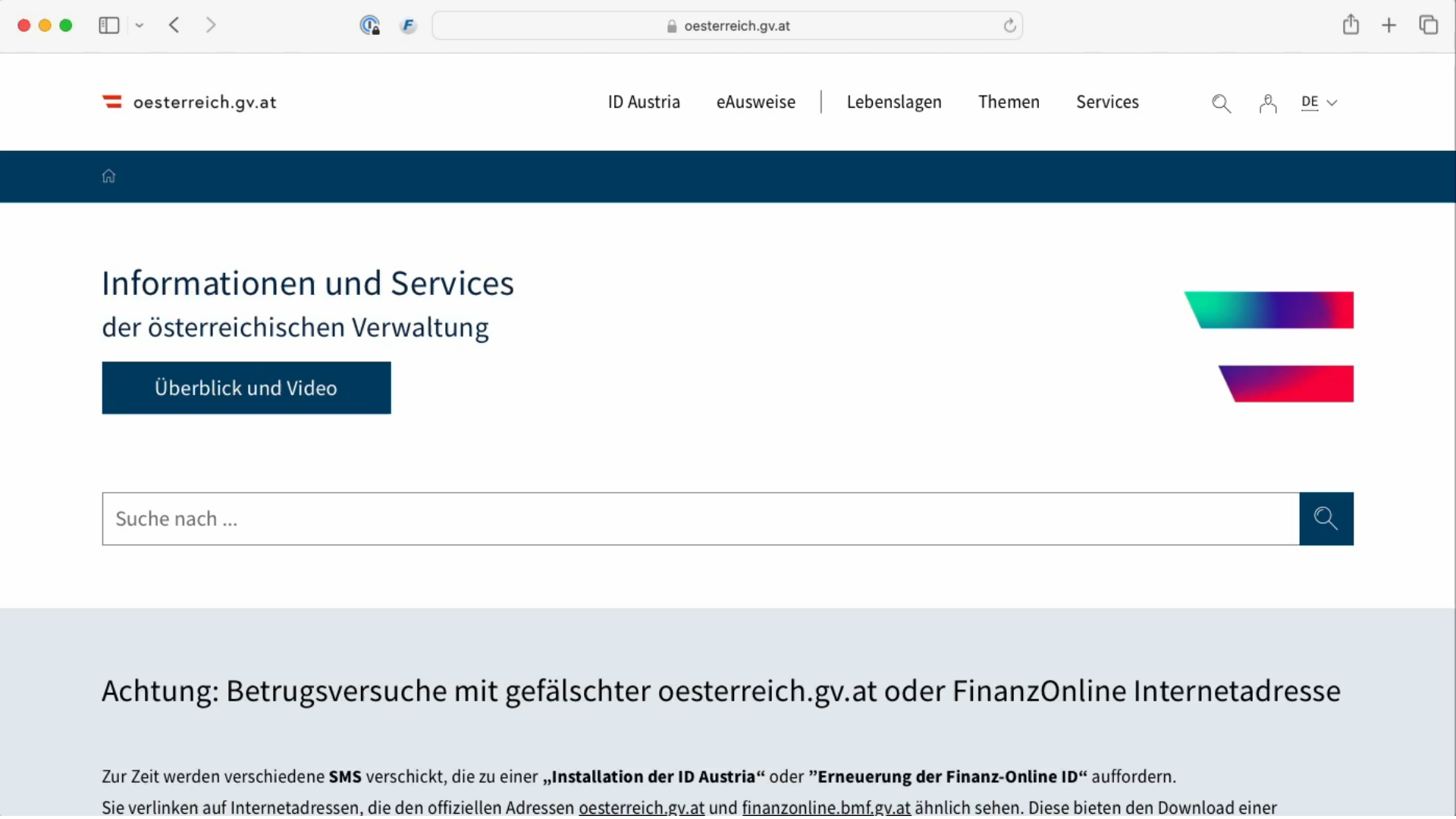
LEISTUNGEN | GESUNDHEITS-DIENSTLEISTER | DIENSTGEBER | KONTAKT

ÜBER UNS | LEISTUNGEN | FACHINFORMATIONEN | VORSORGE / PROGRAMME | INTERNATIONAL

GUT ZU WISSEN

LEISTUNGEN

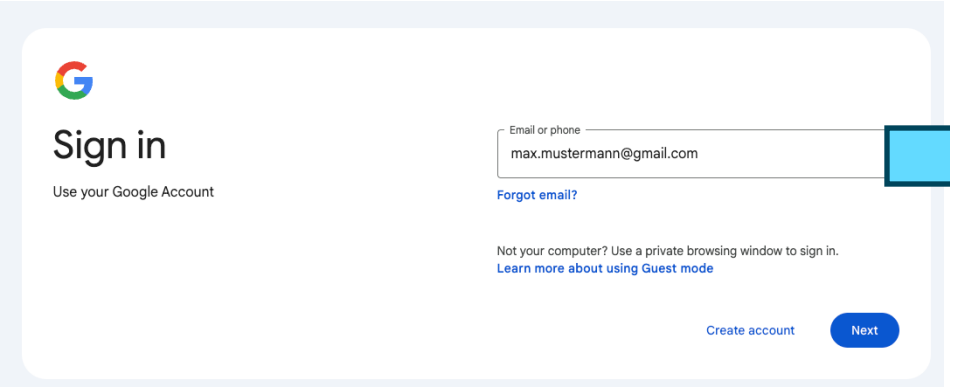
GESUNDHEITSDIENSTLEISTER

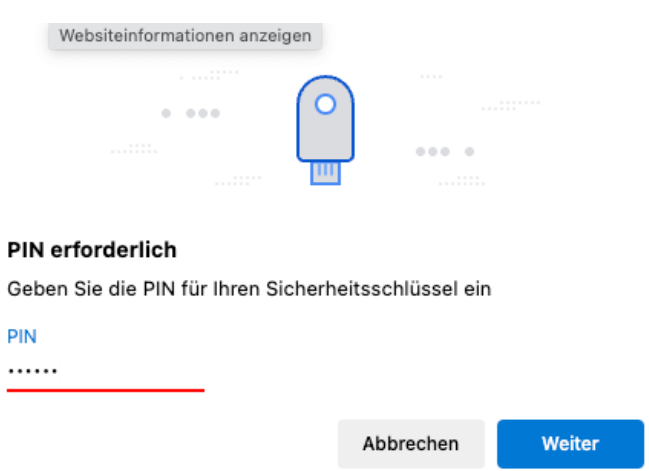

oesterreich.gv.at
oesterreich.gv.at
ID Austria
eAusweise
Lebenslagen
Themen
Services
DE
Informationen und Services
der österreichischen Verwaltung
Überblick und Video
Suche nach ...
Achtung: Betrugsversuche mit gefälschter oesterreich.gv.at oder FinanzOnline Internetadresse
Zur Zeit werden verschiedene **SMS** verschickt, die zu einer **„Installation der ID Austria“** oder **”Erneuerung der Finanz-Online ID“** auffordern.
Sie verlinken auf Internetadressen, die den offiziellen Adressen oesterreich.gv.at und finanzonline.bmf.gv.at ähnlich sehen. Diese bieten den Download einer


20:05
sozialversicherung.at
Meine SV
GUT ZU WISSEN
LEISTUNGEN

FIDO (Fast Identity Online)

- Entwickelt für Multifaktor-Authentifizierung (MFA)
- WebAuthn API & Client-to-Authenticator Protocol (CTAP)
- „Non-Discoverable credential“



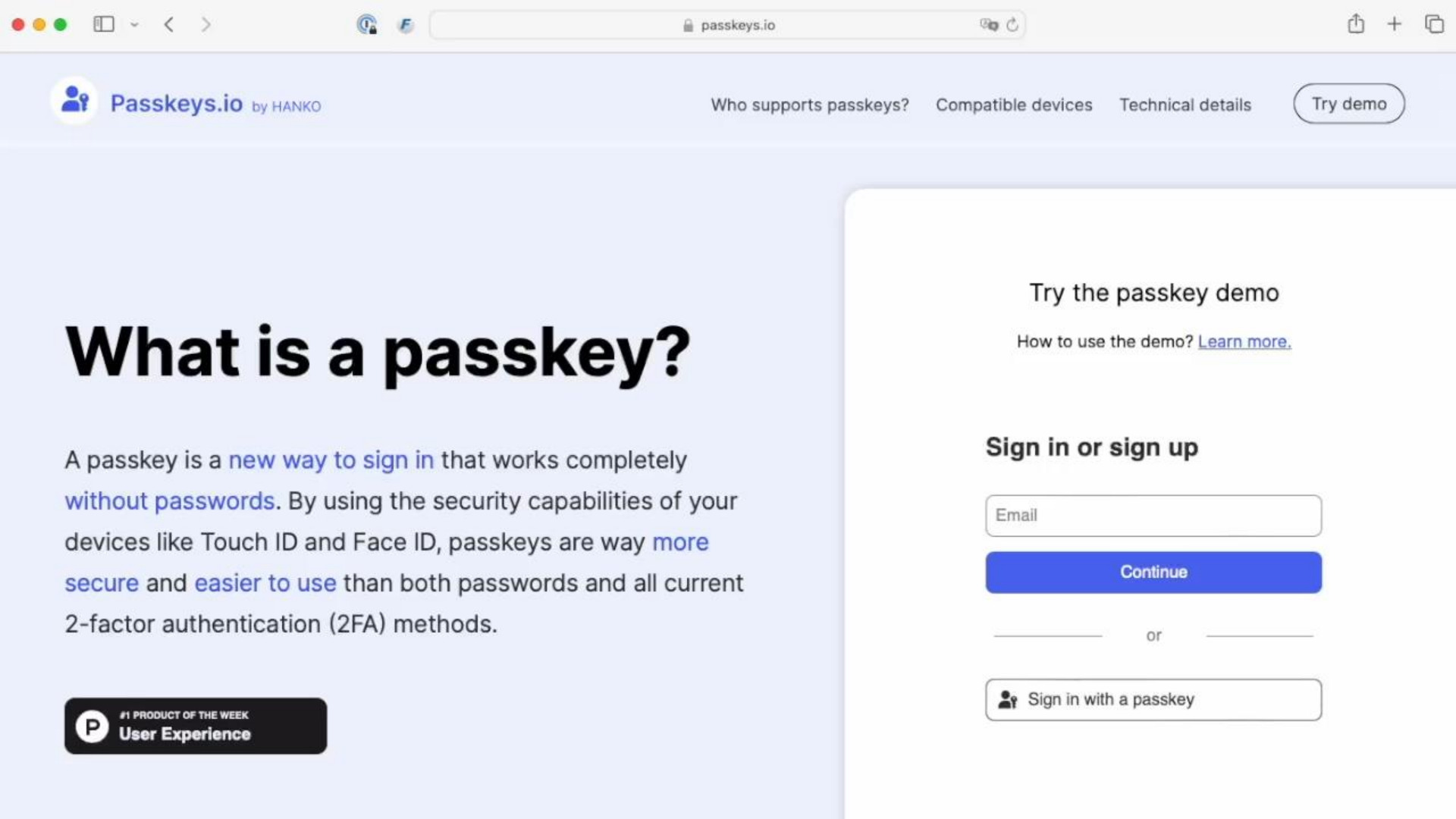


Was ist passkeys?

- Weiterentwicklung von WebAuthn (FIDO)
- „Synced“ Credentials

Was ist passkeys?

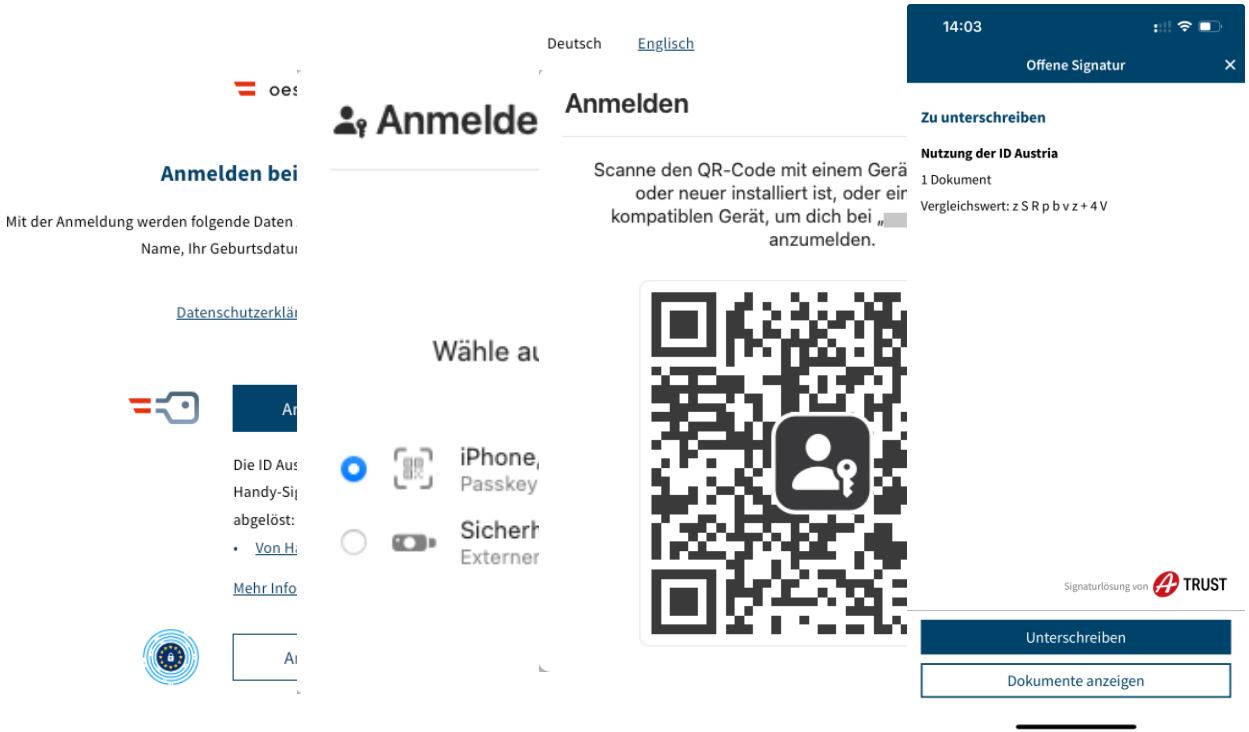
- „Discoverable credential“
  - Unterstützung von Mobilegeräten als Authenticator
  - Kein User-Handle durch User
  - Einschränkung auf z.B. Domäne (oesterreich.gv.at)
  - Benutzer wählt Authenticator
  - Passkey liefert User-Handle


passkeys.io
Passkeys.io by HANKO
Who supports passkeys?
Compatible devices
Technical details
Try demo
What is a passkey?
A passkey is a new way to sign in that works completely without passwords. By using the security capabilities of your devices like Touch ID and Face ID, passkeys are way more secure and easier to use than both passwords and all current 2-factor authentication (2FA) methods.
#1 PRODUCT OF THE WEEK
User Experience
Try the passkey demo
How to use the demo? Learn more.
Sign in or sign up
Email
Continue
or
Sign in with a passkey

ID Austria Integration

- Sicherheitstechnisch gleichwertiger Vorgang
  - Kein Passwort notwendig
- Aktuell nur App2App
- Mittels Passkeys auch in Browser möglich
  - Zwei Ansätze
    - HW-basierte Key-Attestation
    - ID Austria Passkey Provider
  - Ein Schnittstelle für App und FIDO Token
  - Demonstrator für Android 14+

ID Austria Integration



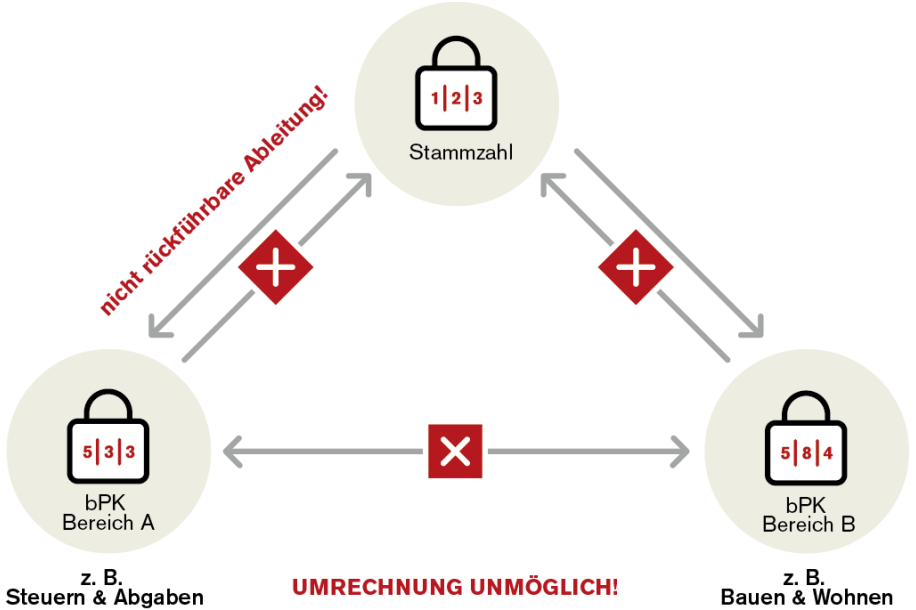
Privacy

Stammzahlen-basierte Pseudonyme

Aktuelle Systematik bPK

- Einweg-Hashfunktion
  - SHA-1 (Stammzahl + Bereich)
- Nicht rückführbar
- Von IDA/SZR erzeugt

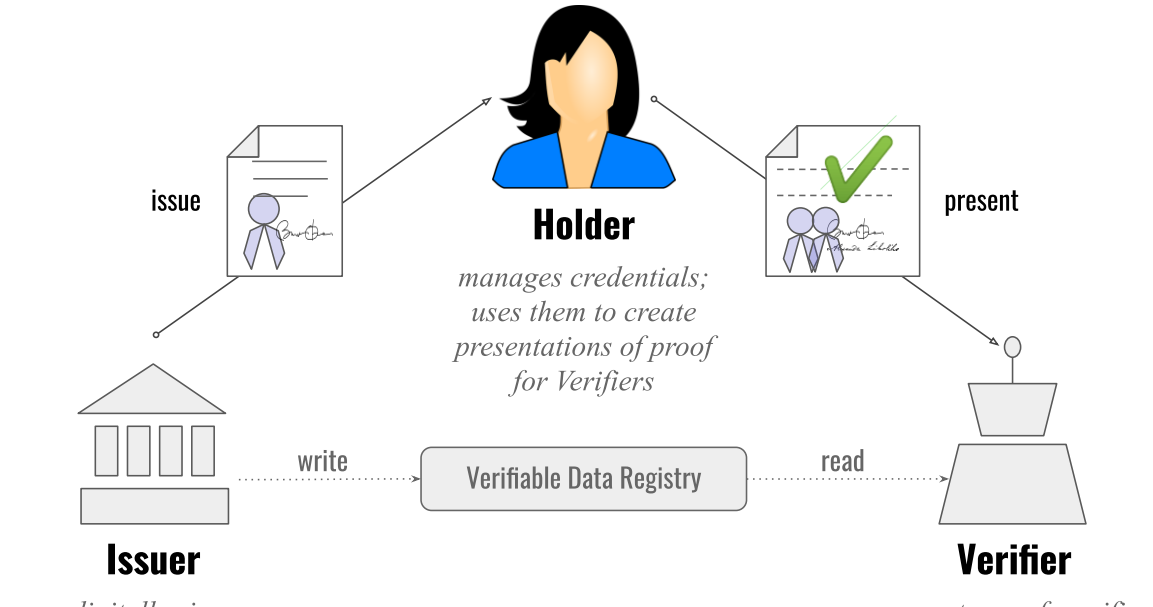
- IDA/SZR kennt Bereich bzw. Service Provider (!)



eIDAS 2.0

- eIDAS 2 Verordnung (1183/2024) mit 20. Mai in Kraft
- EU Wallet mit Ende 2026 erwartet
- Neue Konzepte
  - Dezentrale Attributauslieferung
  - Pseudonyme

EU Wallet – Dezentrales Konzept



Source: wikimedia.org

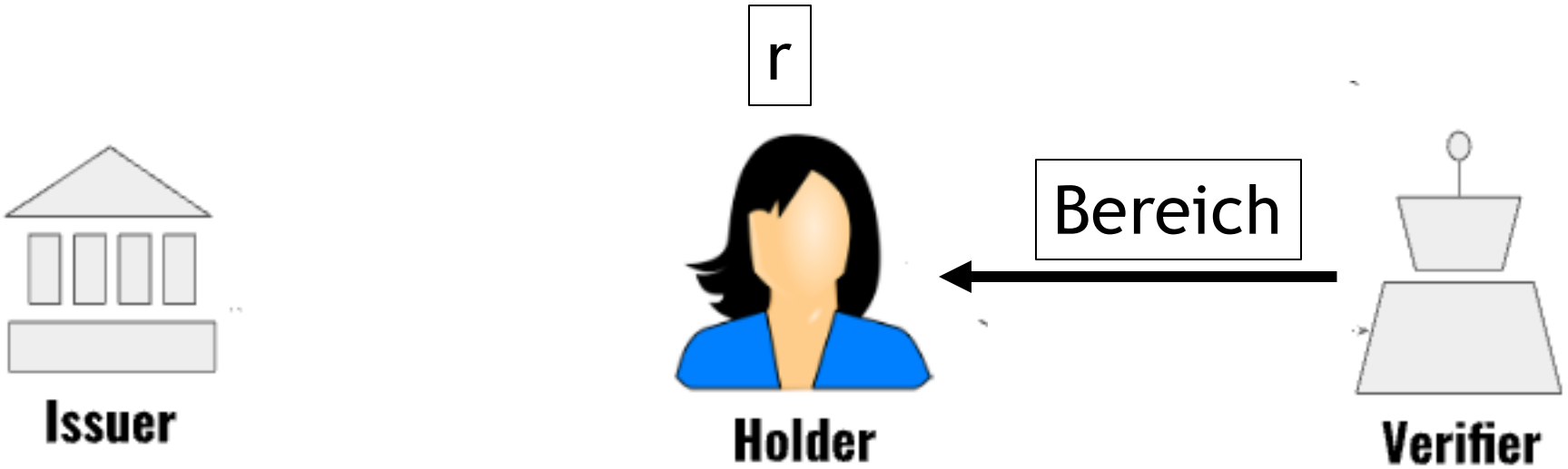
Pseudonyme in EU Wallet

- Pairwise Pseudonymous Identifier (PPID)
  - Eindeutiges Pseudonym pro User und Service Provider
  - Nicht korrelierbar zwischen SP (ähnlich bPK)
  - Erzeugung
    - Zufällig (CSPRNG)
      - Nachteil: verloren, falls kein Backup und Wallet verloren geht
    - Von eindeutiger ID abgeleitet (bspw. Stammzahl)

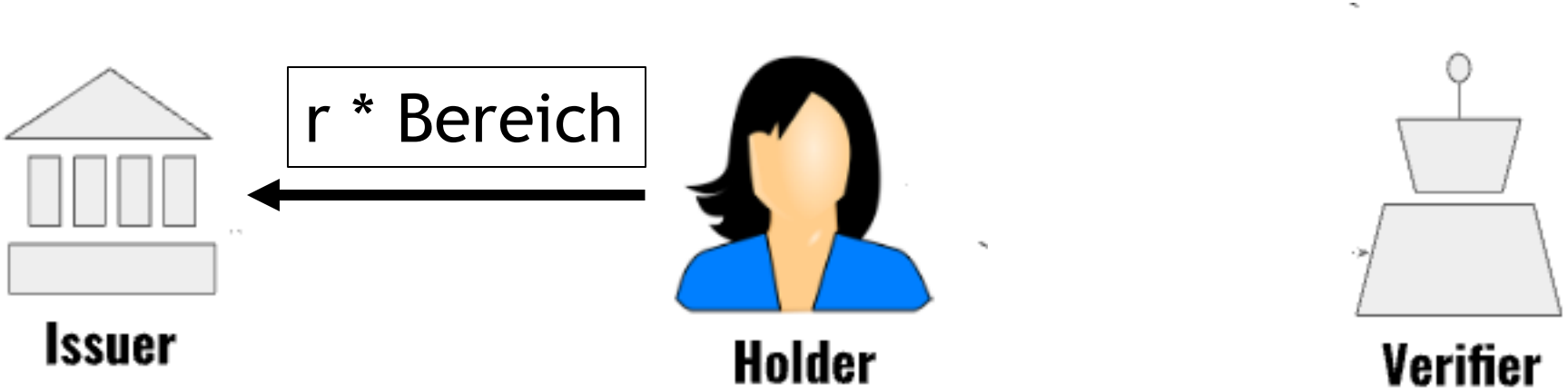
ID-basiert - Sicherheitsanforderungen

- Aussteller/Issuer (IDA/SZR) sollte nicht wissen, wer SP ist
- SP muss validieren können, dass Pseudonym von IDA/SZR ausgestellt wurde und somit auf Stammzahl basiert
- SP darf Stammzahl selbst nicht kennenlernen
- Ansätze
  - Offline (Lokale Schnorr Signatur)
  - Online (OPRF – Oblivious Pseudorandom Functions)
    - BISON Protokoll (EGIZ)

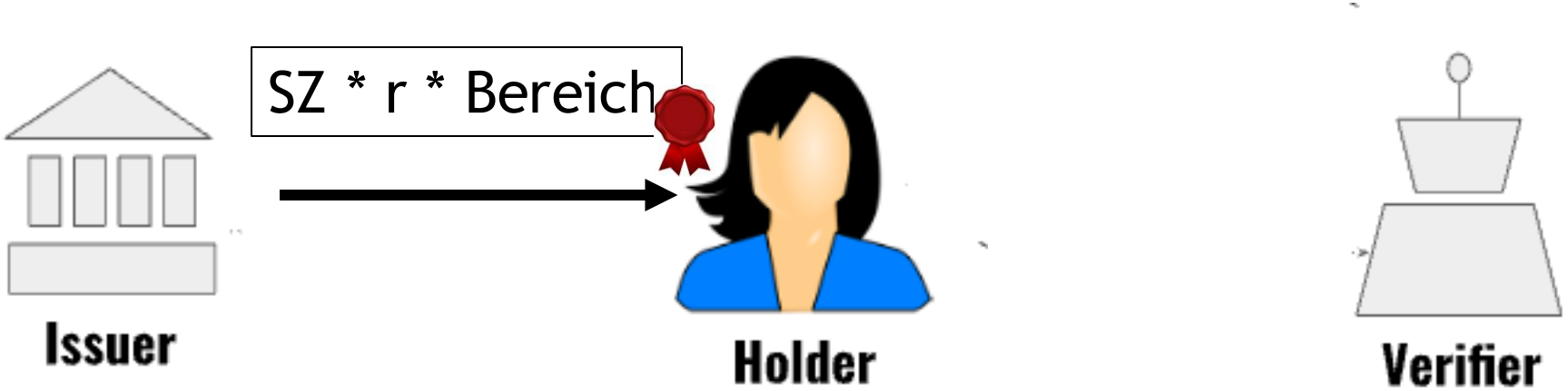
BISON Protokoll



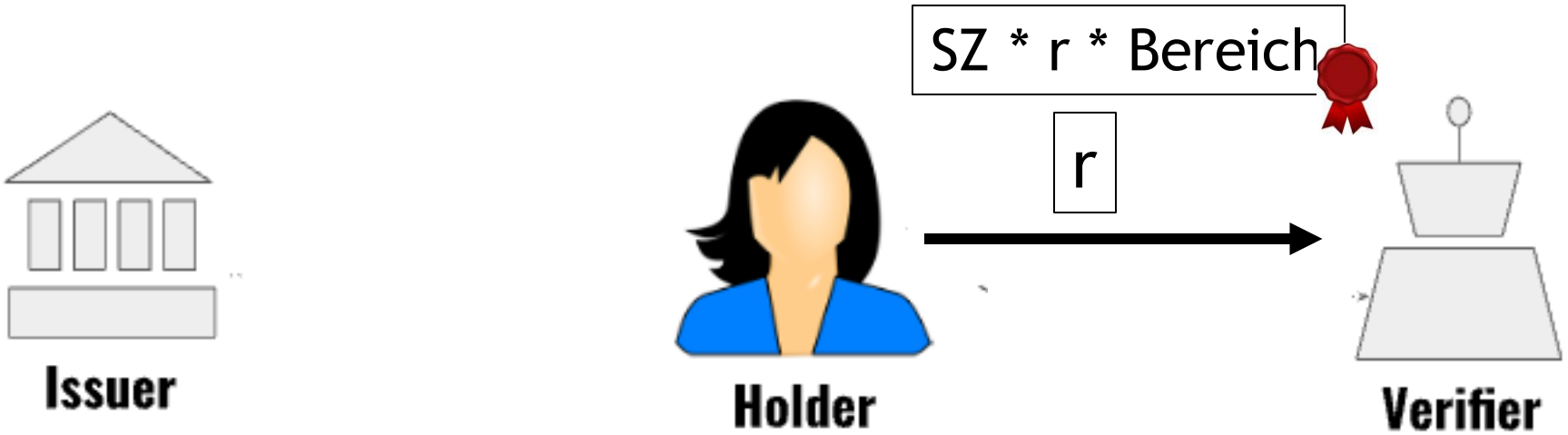
BISON Protokoll



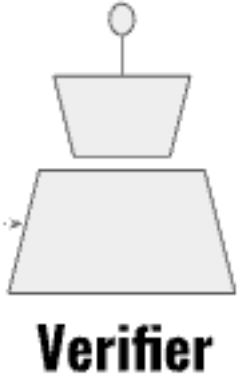
BISON Protokoll



BISON Protokoll



BISON Protokoll



$SZ * r * Bereich$ $*$ r^{-1} $=$ $SZ * Bereich$

Pseudonyme in EU Wallet

- Vorteile
  - Privatsphäreschützend: Aussteller kennt Service Provider nicht
- Nachteile
  - Erweiterung Spezifikationen (Presentation Protokolle)
  - Umsetzung kryptografischer Teile bei Service Provider

Fragen?

a-sit.at/

technology.a-sit.at