Vertrauen, Sicherheit, Privacy in der Digital Society

Dr. Andre Kudra

esatus

Agenda

- Vertrauen ist menschlich
- Digitale Identität ist dezentral
- Warum wir in Credentials vertrauen

Vertrauen ist menschlich

esatus

Menschen in Interaktion
Vertrauen als Kern der Gesellschaft

Die Heimcomputer-Revolution
Digitales erobert Lebenswirklichkeit

Digitalkultur

Die als UNESCO immaterielles Kulturerbe anerkannte *Demoszene*.

“This is not Morgan Freeman”
Steigende Bedrohungen durch Deepfake AI

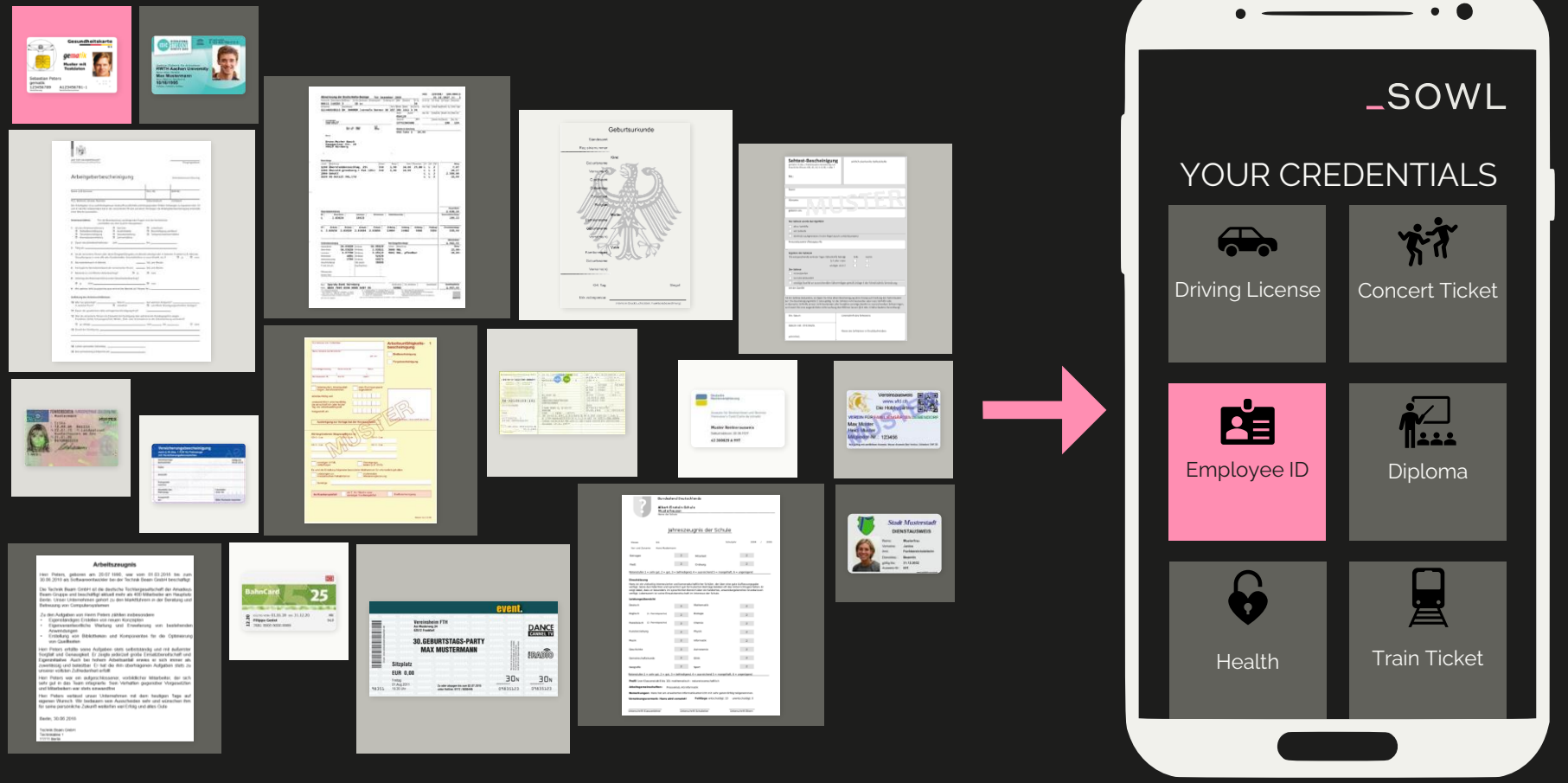
Sehr überzeugende Deepfake Videos erschüttern unser Vertrauen in die digitale Welt.

https://www.youtube.com/watch?v=oxXpB9pSETo

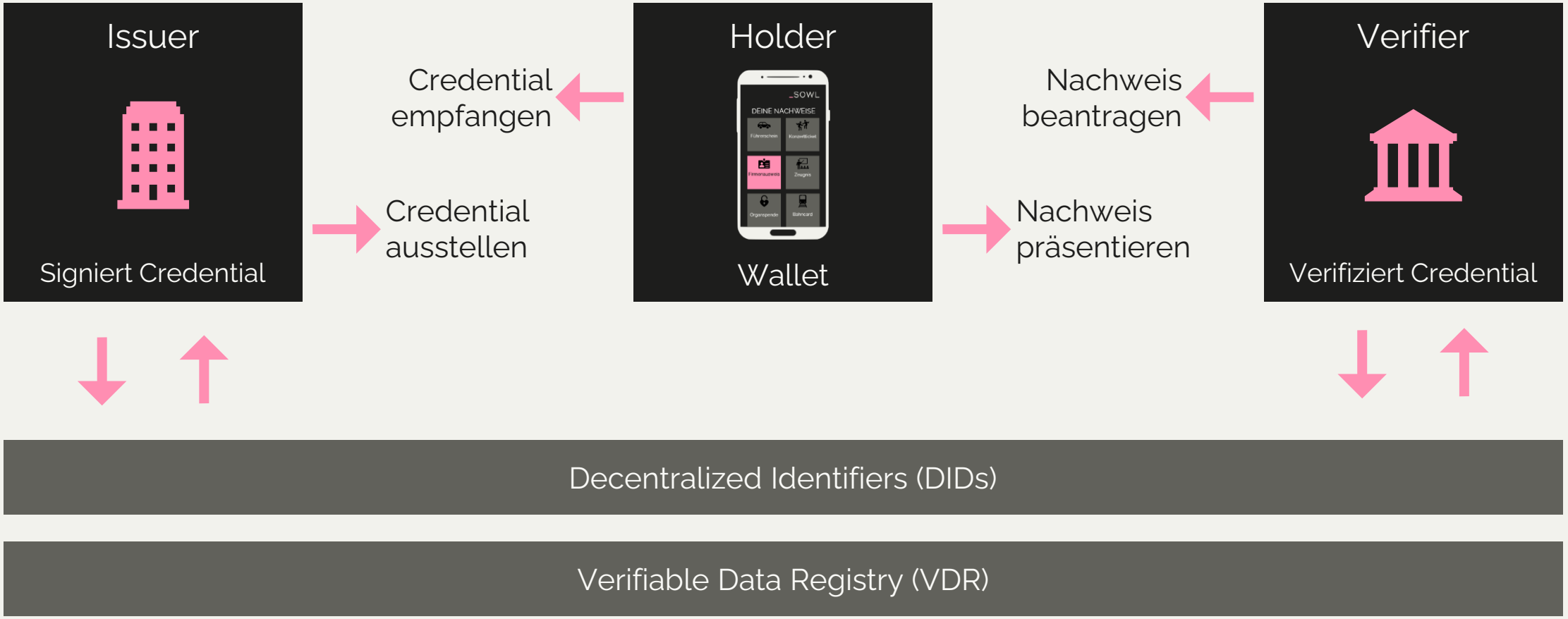
Digitale Identität ist dezentral

esatus

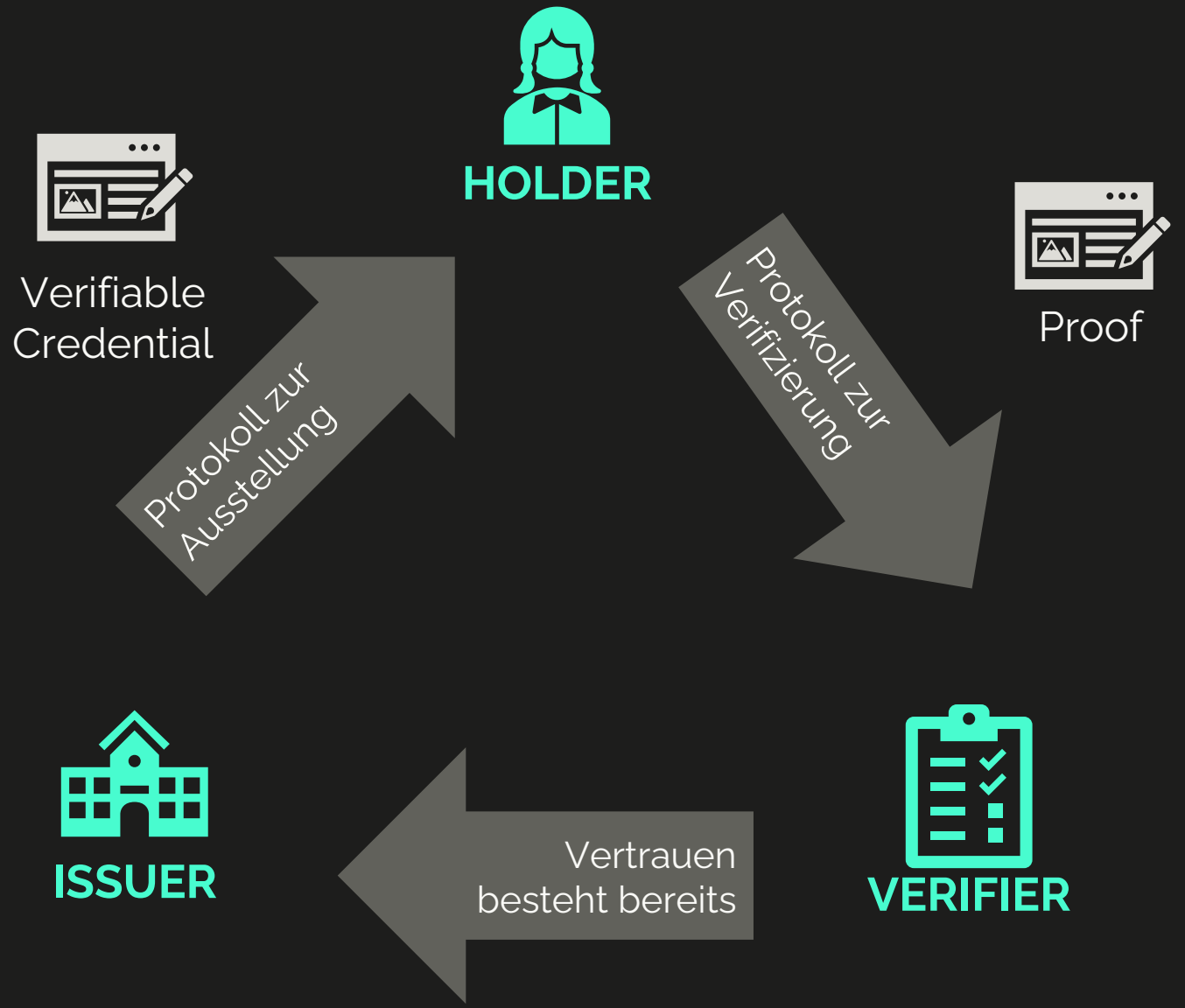
Decentralized Identity – Bequem, sicher, effizient



Das Paradigma Dezentraler Identität – Die Identität der Zukunft ist dezentral, ist sie auch unbesiegbar?



Das Vertrauens-dreieck
Warum genau ist das jetzt sicher?



Warum wir in Credentials vertrauen

esatus

Confidentiality
Vertraulichkeit
Es weiß nur der, der darf und soll

Wallet ist nur mir zugänglich – mein Smartphone, mein Gesicht, meine PIN, ich gebe selektiv frei

Daten sind *klassisch* gespeichert und geschützt – Zugriffskontrolle, Verschlüsselung

Fragt nur ab, was er braucht und haben darf, Daten *klassisch* gespeichert und geschützt

Integrity
Integrität
Unverändert seit Ausstellung

Wallet ist nur mir zugänglich, Credentials sind verschlüsselt, Backups machen

Daten werden bei Ausstellung als Hash erzeugt und mit digitaler Signatur versehen

Modifikationen sind erkennbar, ansonsten sind Daten *klassisch* geschützt

Availability
Verfügbarkeit
Immer da wenn man es braucht

Meine Wallet ist immer dabei, die Credentials sind tatsächlich bei mir, Backup machen

Internetverbindung (meist) nötig für Ausstellung, Daten-haltung erfordert Redundanz/Backup

Internetverbindung (meist) nötig für Abfrage, Daten-haltung erfordert Redundanz/Backup

Authenticity
Authentizität
Ursprung ist eindeutig

Signierte Attribute identifizieren mich in meinen Credentials, meine Wallet, *lügen* nicht möglich

Daten werden bei Ausstellung mit digitaler Signatur versehen, die zuordenbar ist

Herkunft und Datensubjekt sind eindeutig erkennbar, Übertragung ist nachweisbar

Non-Repudiation
Nachweisbarkeit
Involvierung nicht abstreitbar

Signierte Attribute identifizieren mich, Übertragung nachweisbar, *lügen* nicht möglich

Daten werden bei Ausstellung mit digitaler Signatur versehen, die zuordenbar ist

Herkunft und Datensubjekt sind eindeutig erkennbar, Übertragung ist nachweisbar

Die Digital Society Conference

esatus

Digitale Identitäten
Schlüssel zu Sicherheit und Vertrauen

SCHÜLER

Adresse

Arbeitsergebnisse

Erkrankungen

Name

Verhalten

Muttersprache

Geburtsdatum

Fehlzeiten

Klasse

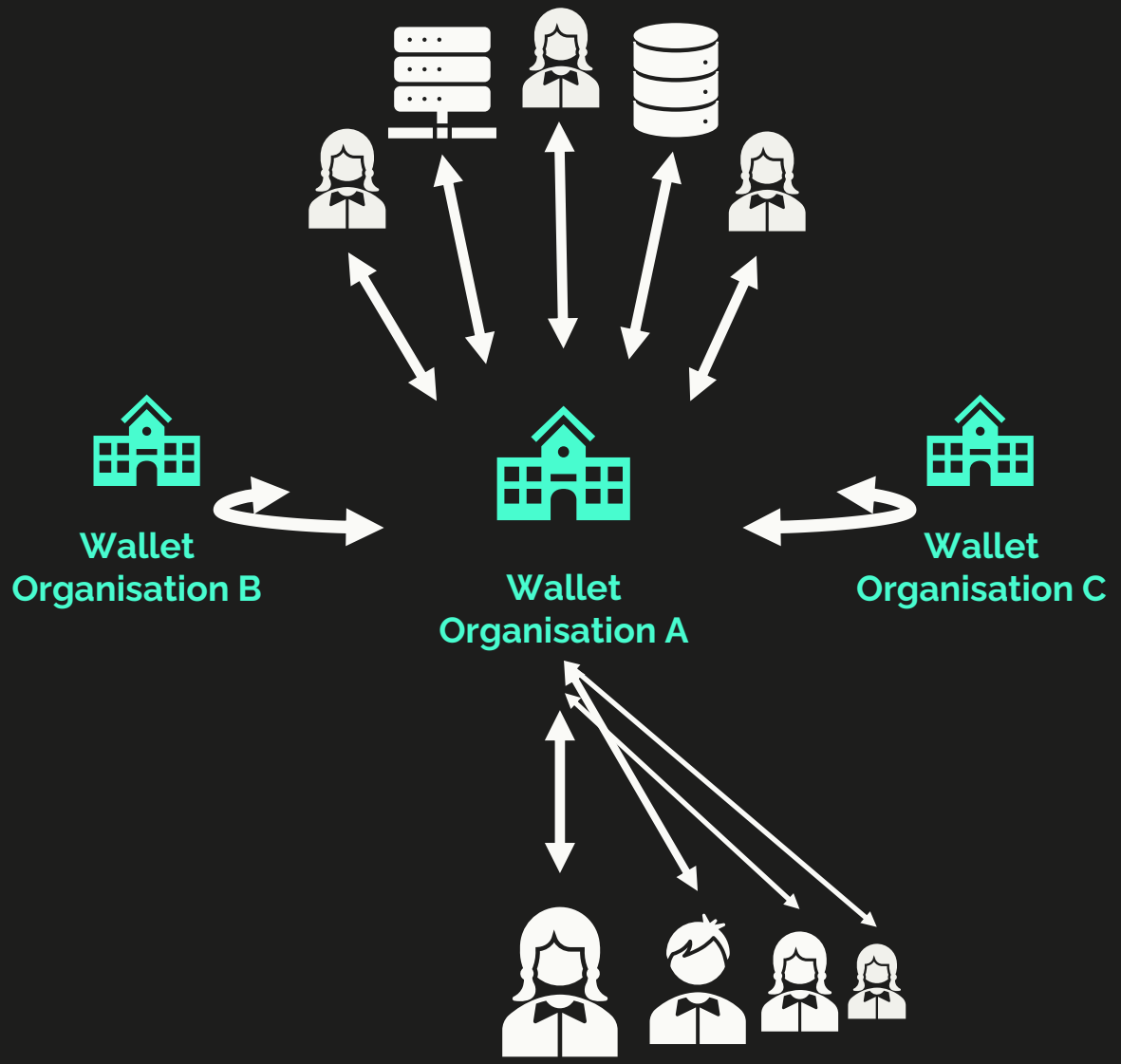
Noten

Hausaufgaben

LEHRER

ELTERN

Organisations-übergreifend Elektronisches Vertrauens-ökosystem



Regulierungslandschaft
Kein Standard, keine Durchbrüche

- W3C JSON-LD (US Department of Homeland Security)
- Hyperledger Indy & AnonCreds (BC Gov)
- KERI & ACDC (GLEIF vLEI, financial sector regulated)

PURE SSI

- OID4VC & SD-JWT (EU Architecture and Reference Framework/ARF)

COMPLEXITY-REDUCED SSI

- Mobile Driving Licence (mDL)

WANNABE SSI

- OpenID Connect
- PKI / X.509

NON SSI

esatus

Die Technologie ist nur ein Mittel, der Zweck ist entscheidend.

Lassen Sie uns gemeinsam Lösungen finden!