JOHANNES KEPLER UNIVERSITY LINZ

Keynote

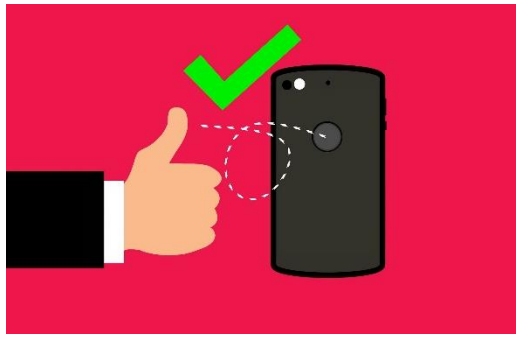
Digital Authentication in the Real World without Sacrificing Privacy

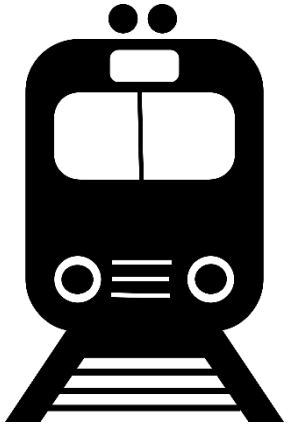
Computing Conference 2020, 2020-07-16 16:30 (BST/UTC+1), London/virtual

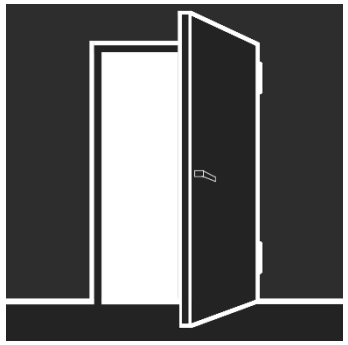
Univ.-Prof. Dr. René Mayrhofer (JKU Linz)
(Full disclosure: also affiliated with Android security, but not speaking for Google today)

JOHANNES KEPLER UNIVERSITY LINZ
Altenberger Straße 69
4040 Linz, Austria
jku.at

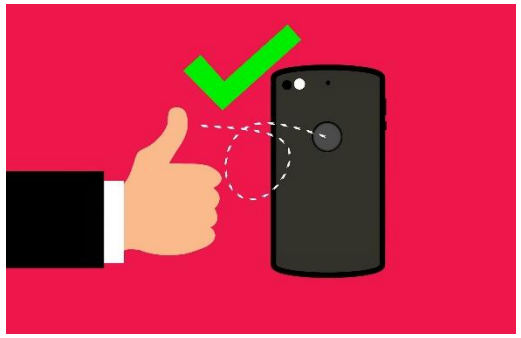
Digital Authentication – Identity and Attributes

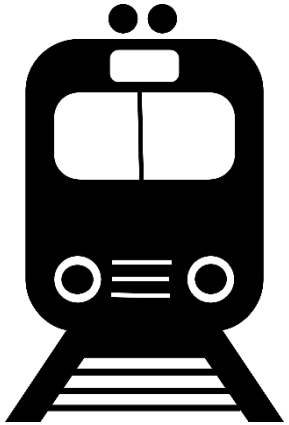




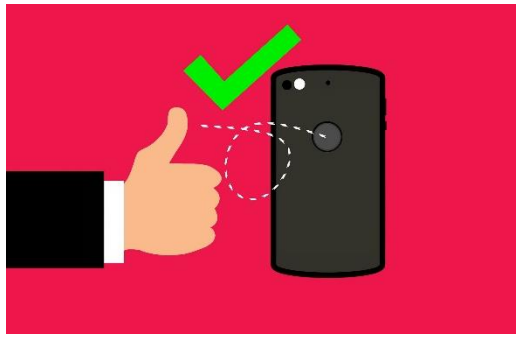


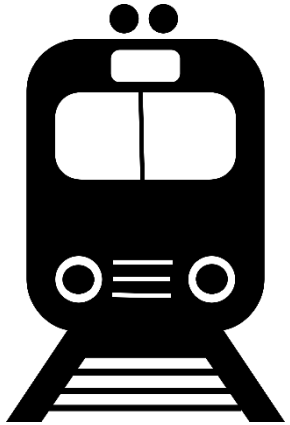
Digital Authentication – Identity and Attributes

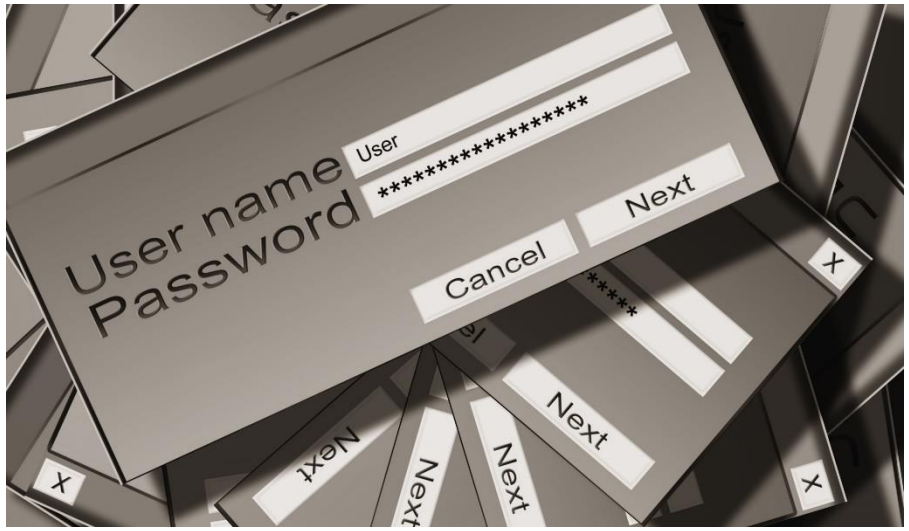




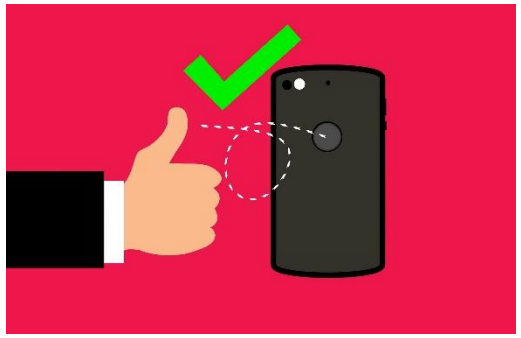
Digital Authentication – “State of the Art”

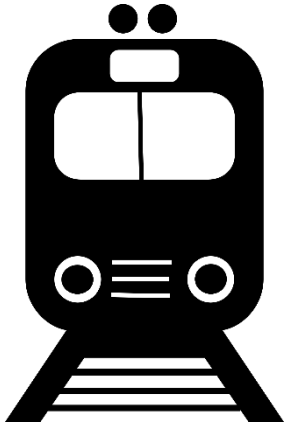




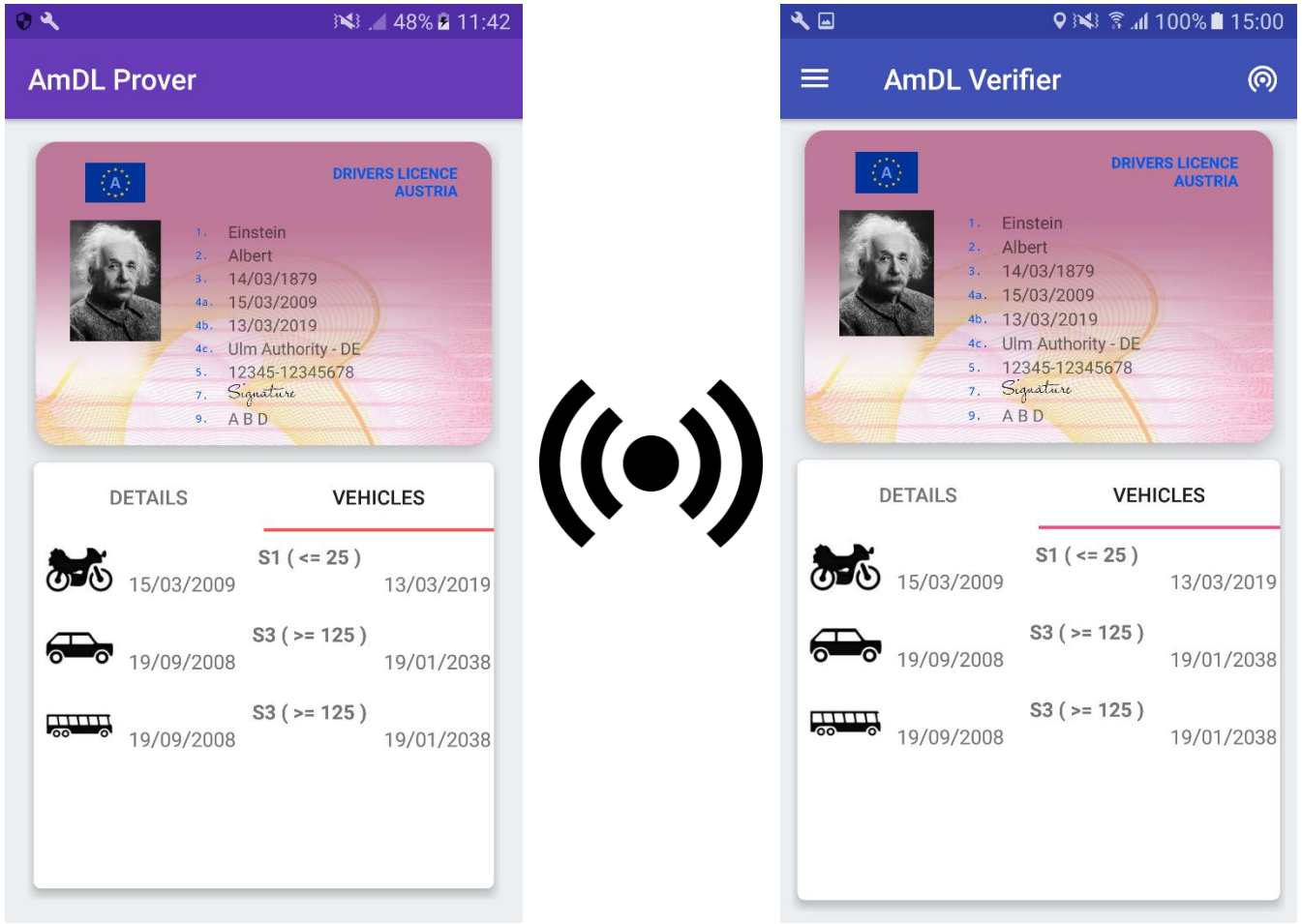


Digital Authentication – Identity on Smartphones





Scenario 1: Traffic Check

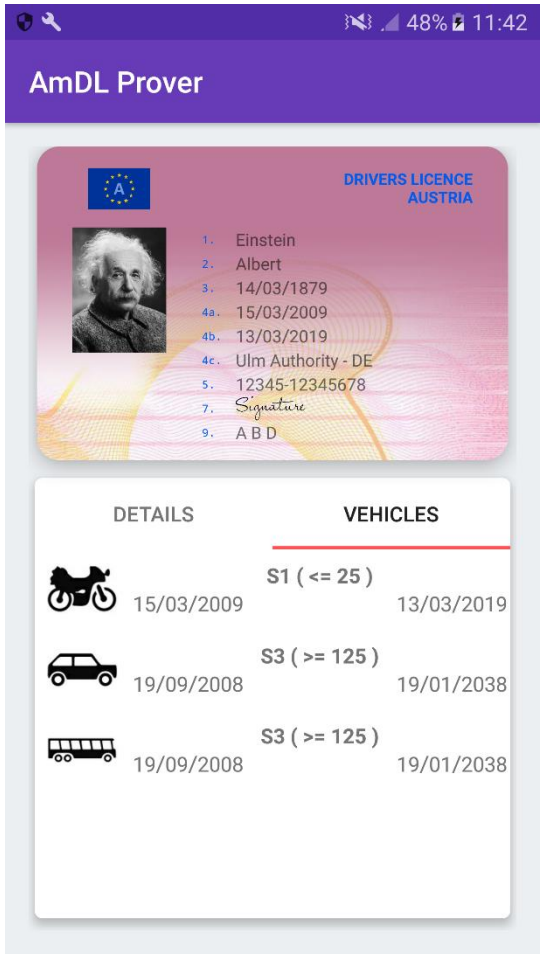


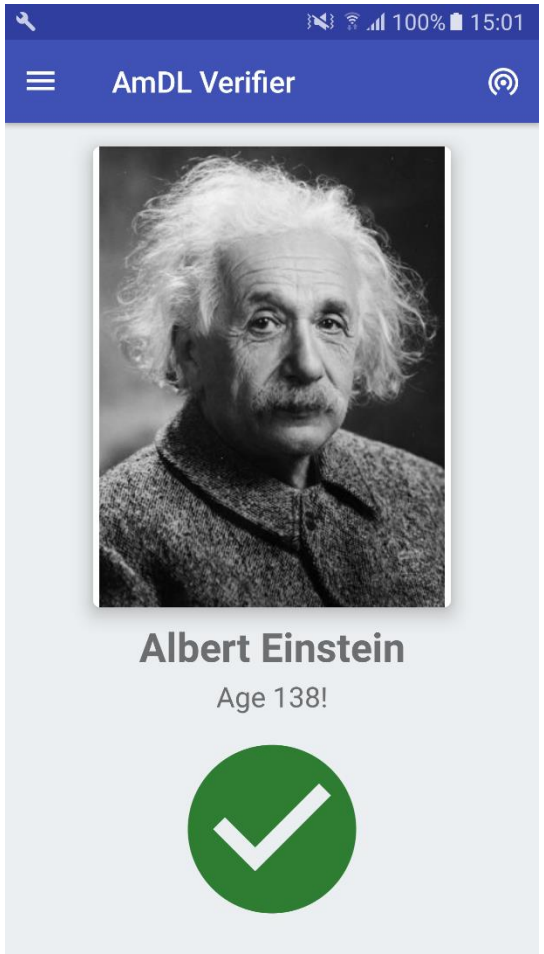
All attributes are transferred

- Name
- Date of birth
- Face picture in full resolution
- (optional) Place of residence
- (optional) Biometric features
- Vehicle classes, potential restrictions, …

Also needs to work offline!

Scenario 2: Proof of Age





Only relevant attributes

- Face picture
- Age

Scenario 3: Public Transport

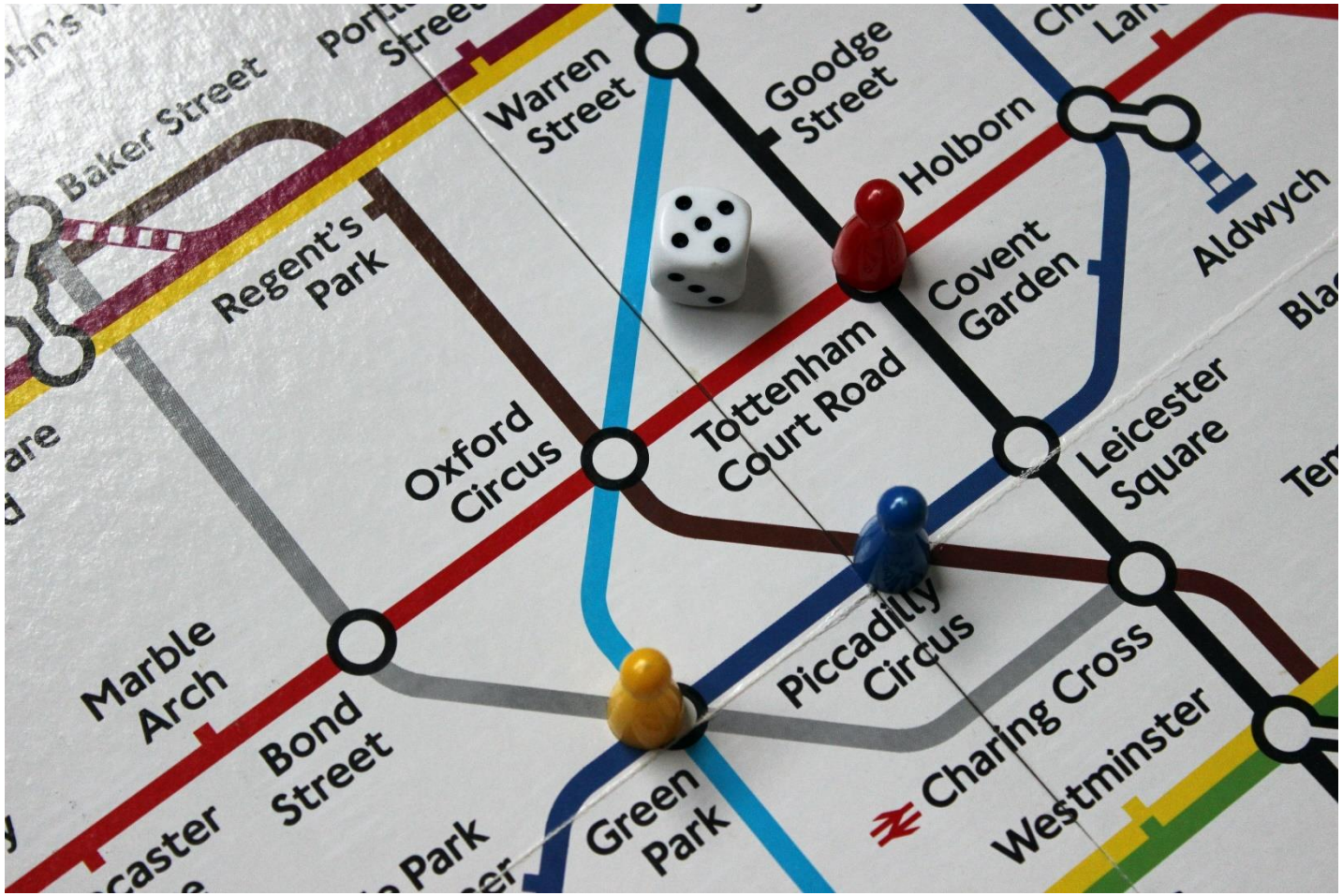


Image credit: https://pixabay.com/photos/underground-tube-map-stations-2725336/

Location traces constitute highly sensitive data

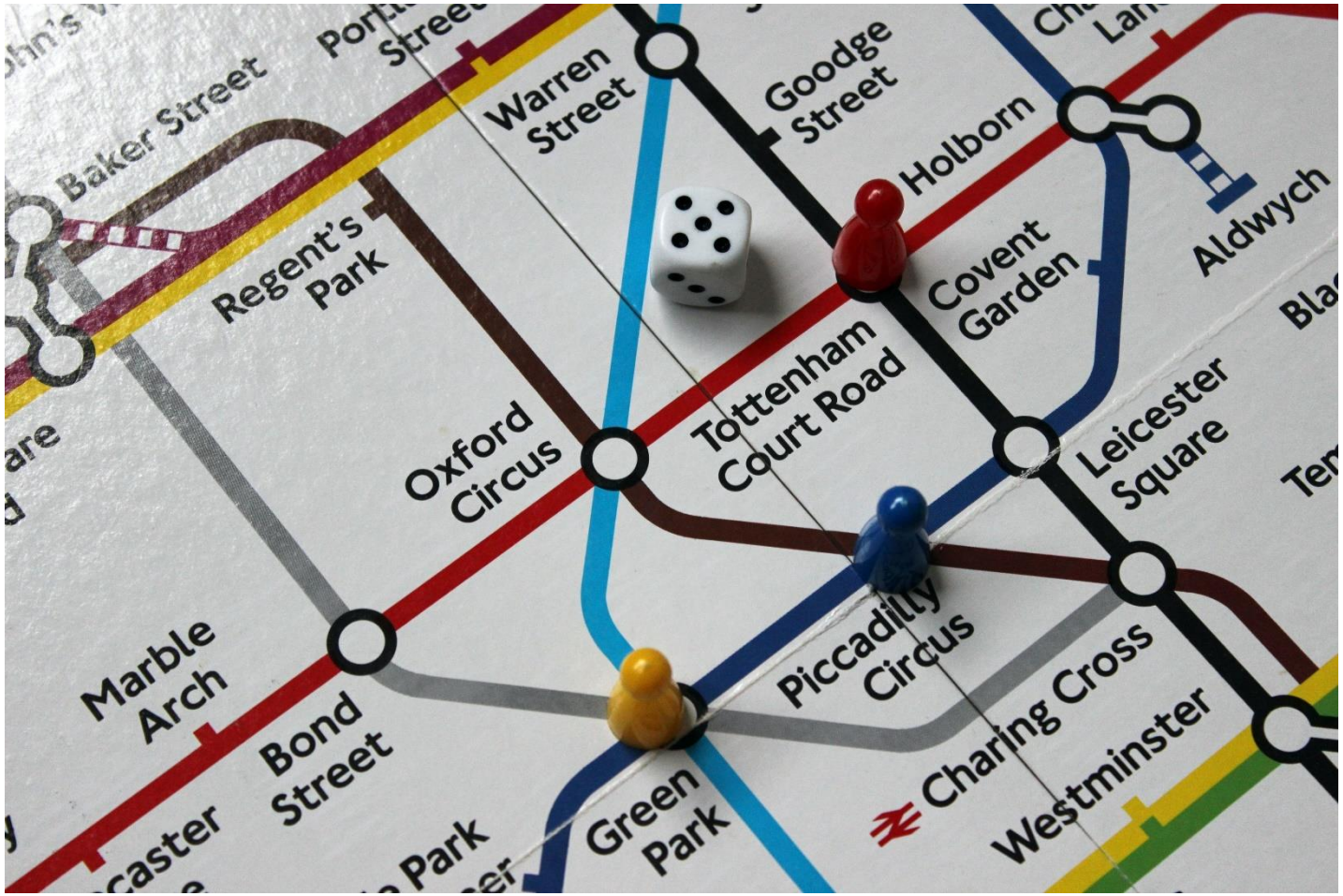
- Place of residence / work
- Religious beliefs
- Illnesses
- Hobbies, particular preferences

Only relevant attributes

- Place of entry / exit **or**
- Possession of time based ticket

But no unique identifier!

Scenario 4: Contact Tracing



Location traces constitute highly sensitive data

- Place of residence / work
- Religious beliefs
- Illnesses
- Hobbies, particular preferences

Only relevant attributes

- Contact with (pseudonym) person X for Y minutes on day Z

But no unique identifier!

Requirements for Digital ID

Functional

- Real-world identification
- One-to-many
- Revocation

Mobility

- Offline
- Power-off
- Scalability

Security

- Key confidentiality
- Unforgeability
- Communication protection
- (future) State-of-the-art cryptography

Privacy

- Anonymity
- (forward/backward) Unlinkability
- User control
- Privacy-preserving attribute queries

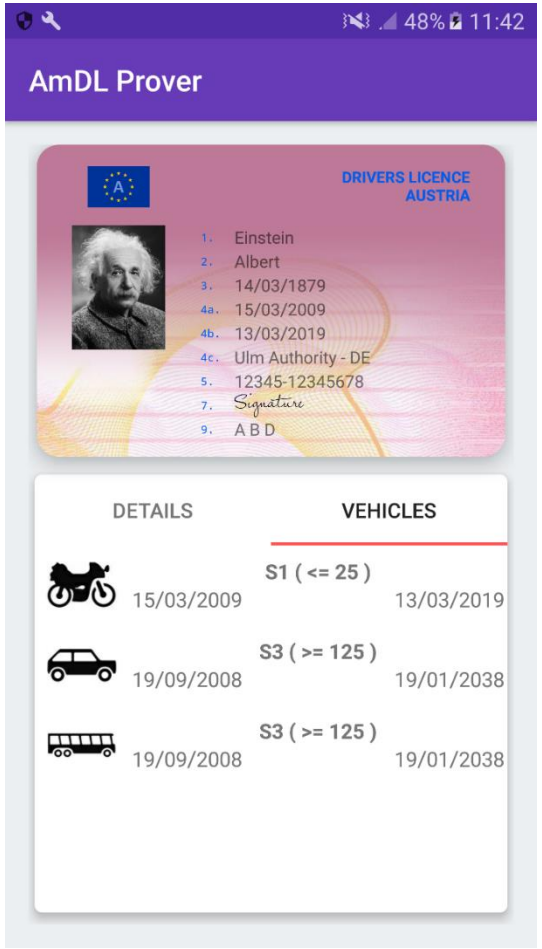
Michael Hölzl, Michael Roland, and René Mayrhofer. “Real-World Identification: Towards a Privacy-Aware Mobile eID for Physical and Offline Verification”. In *Proceedings of the 14th International Conference on Advances in Mobile Computing and Multi Media* (MoMM '16), ACM Press, November 2016

Security and Privacy for draft mDL standard (ISO 18013-5)

- **Security** properties:
  - **Anti-forgery**: Identity Credential data is signed by the Issuing Authority
  - **Anti-cloning**: Secure Hardware produces MAC during provisioning using a key derived from a private key specific to the credential and an ephemeral public key from the reader. Public key corresponding to credential private key is signed by the Issuing Authority
  - **Anti-eavesdropping**: Communications between Reader/Verifier and Secure Hardware are encrypted and authenticated
- **Privacy** properties:
  - **Data minimization**: Reader/Verifier only receives data consented to by the holder. Backend infrastructure does not receive information about use
  - **Unlinkability**: Application may provision single-use keys
  - **Auditability**: Every transaction and its data is logged and available only to the Holder (not the application performing the transaction)

Question:
Strictly require secure (certified) hardware?

The Android implementation



Android Standard

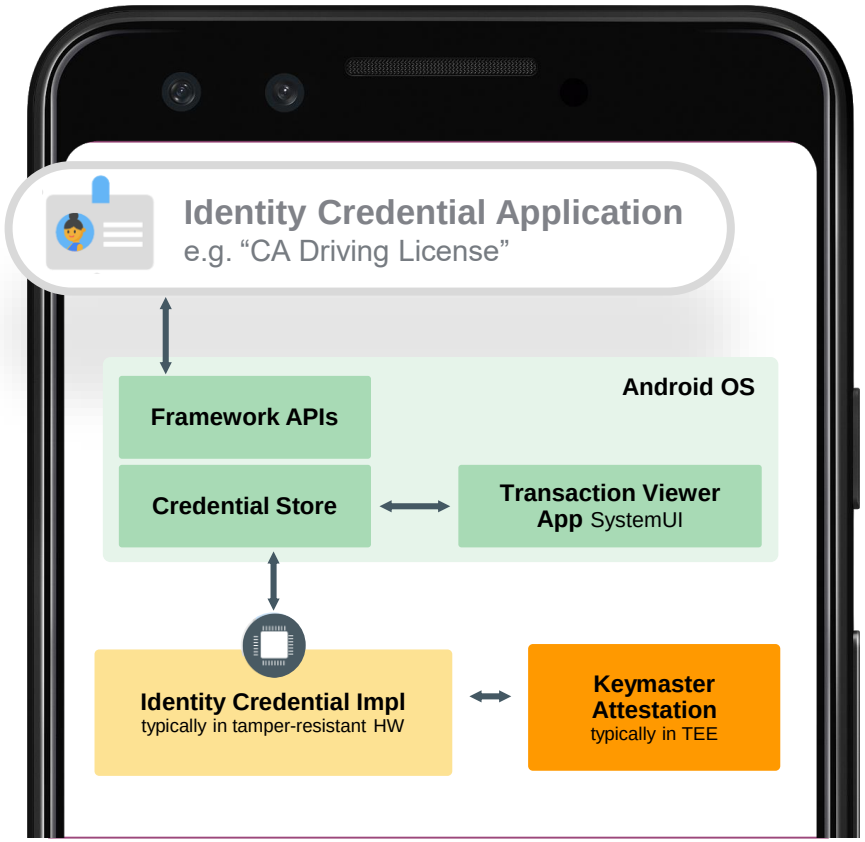
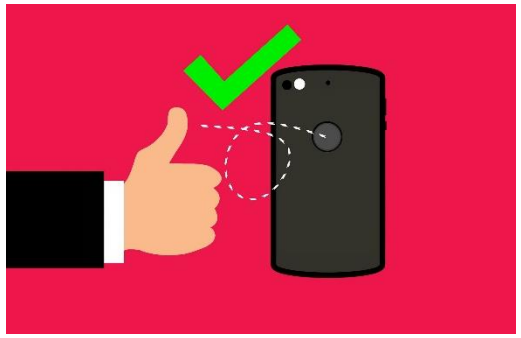
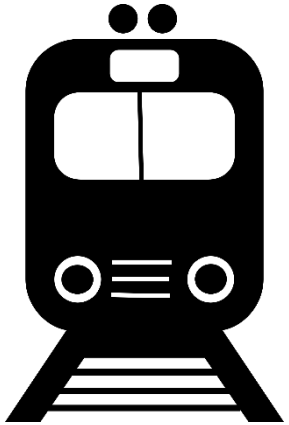


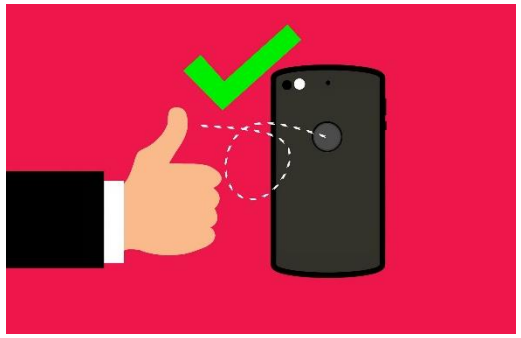
Image credit: Google

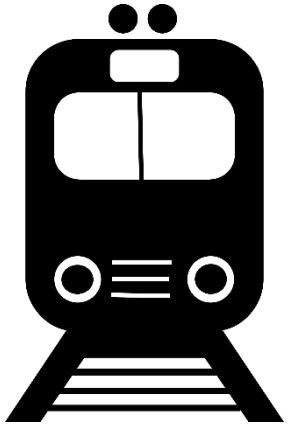
Digital Authentication – Identity on Smartphones



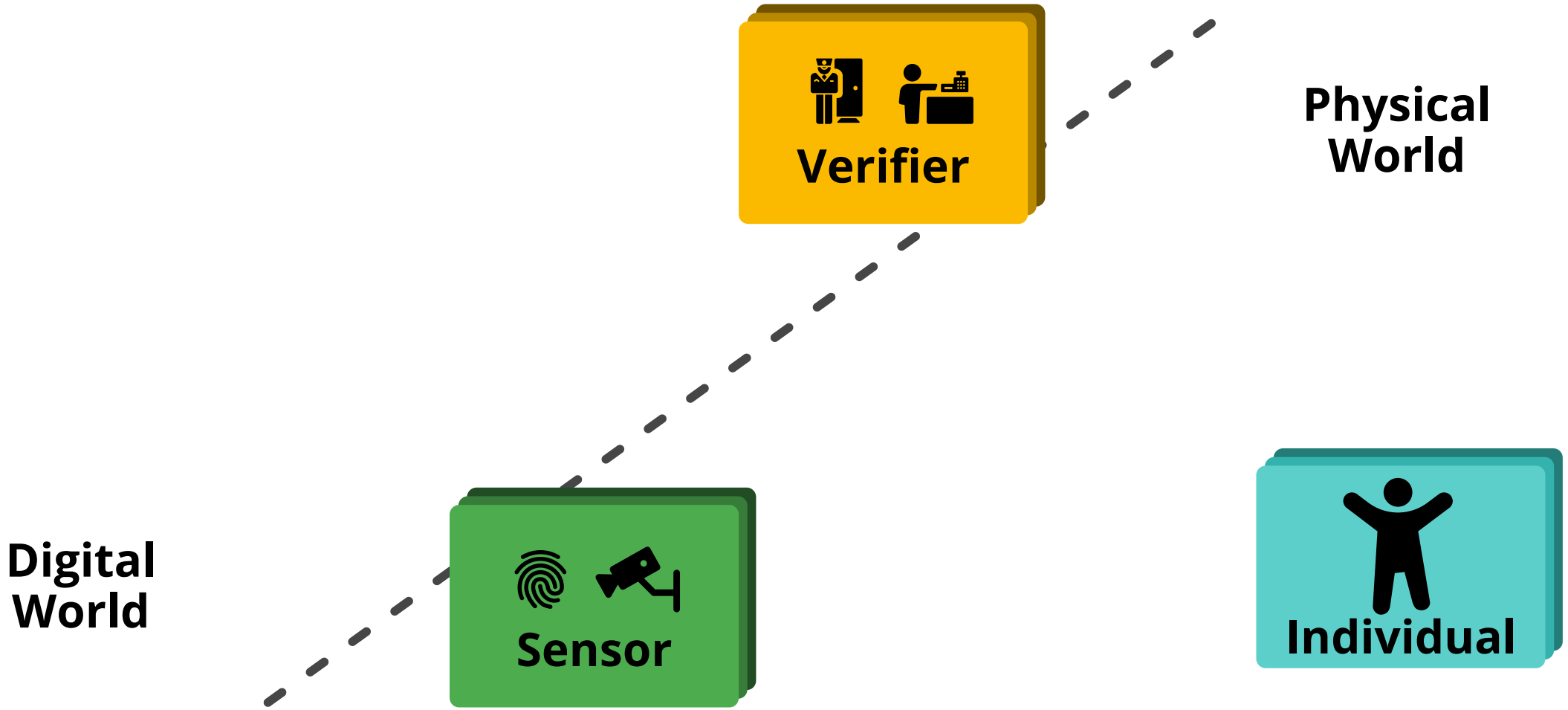


Digital Authentication – Vision

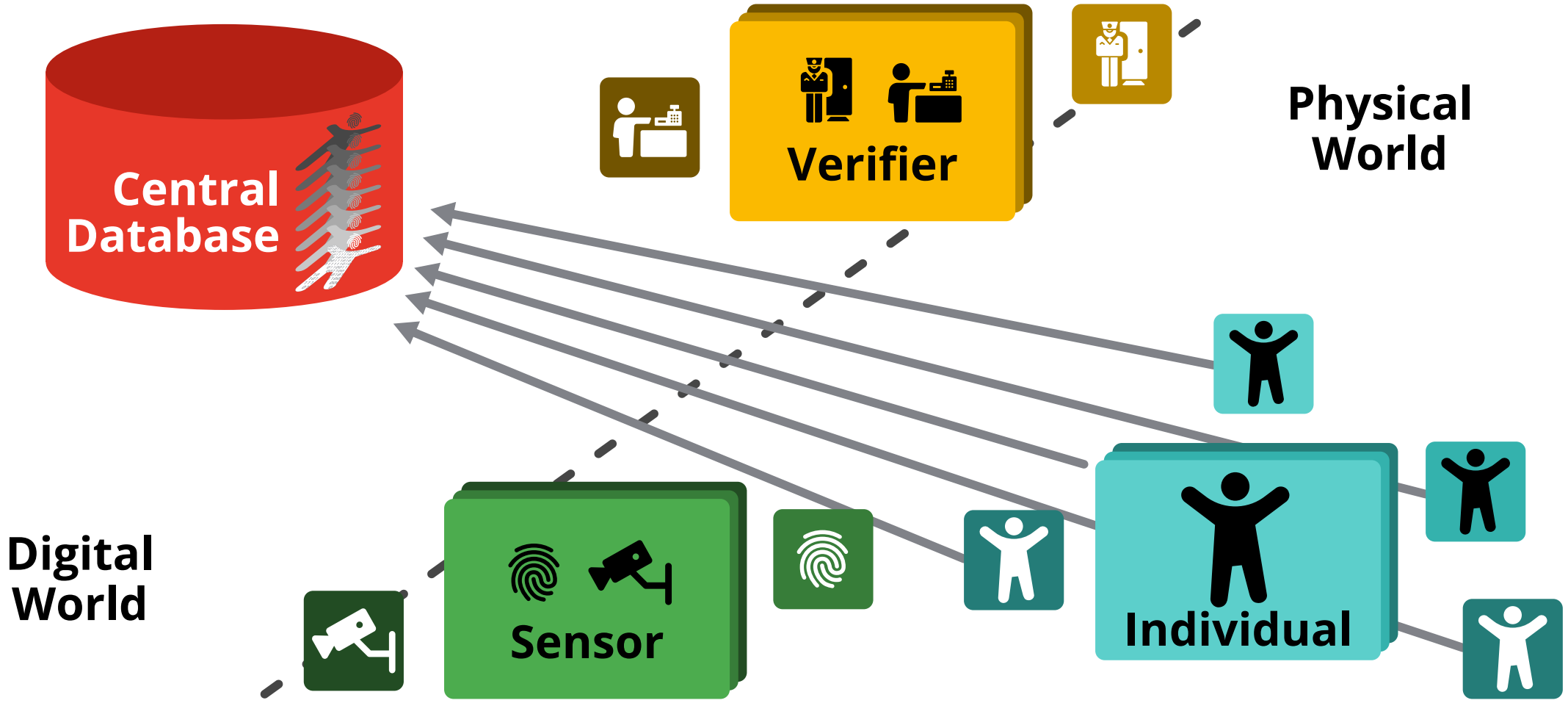


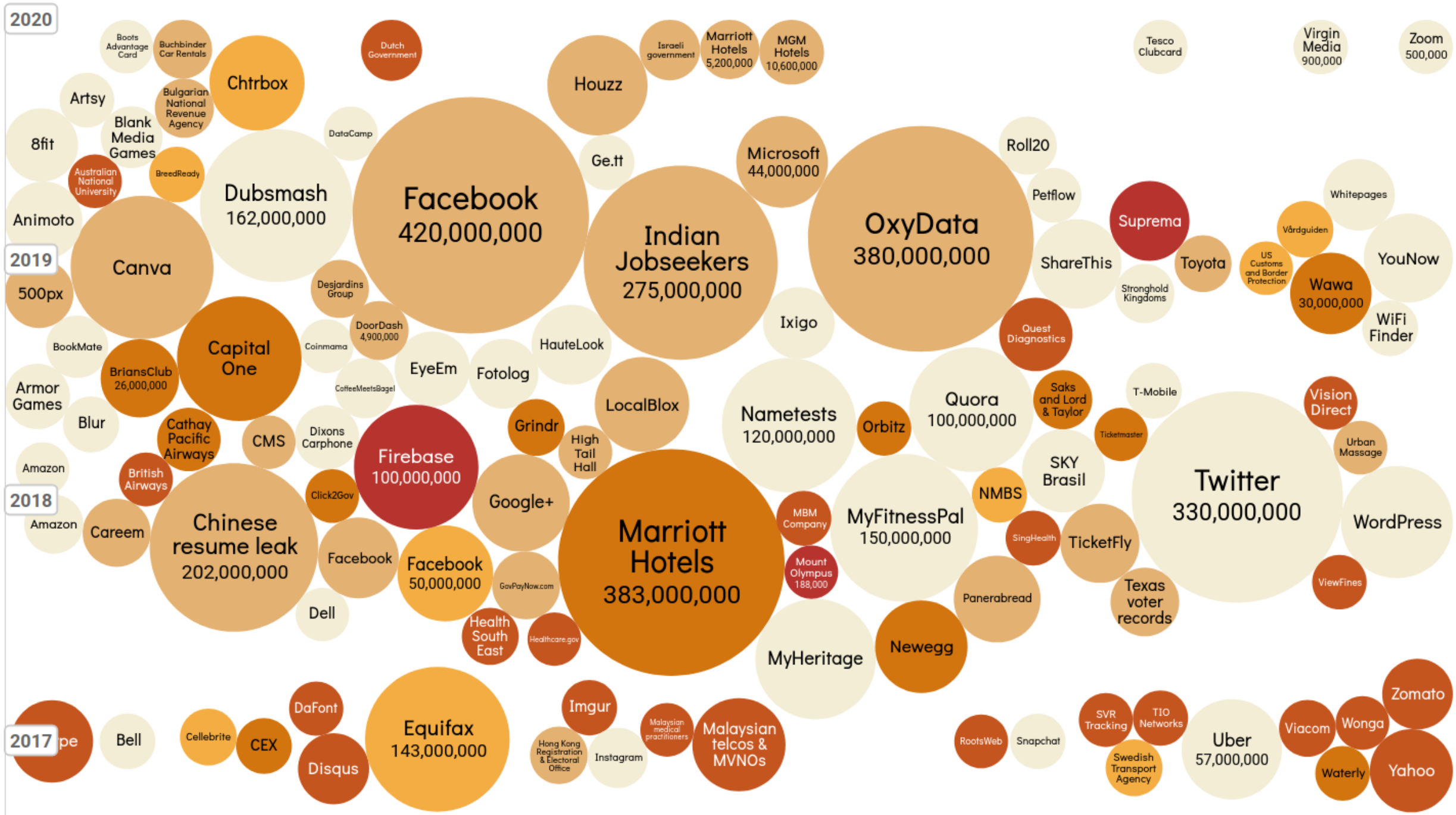


Digital Authentication – Vision

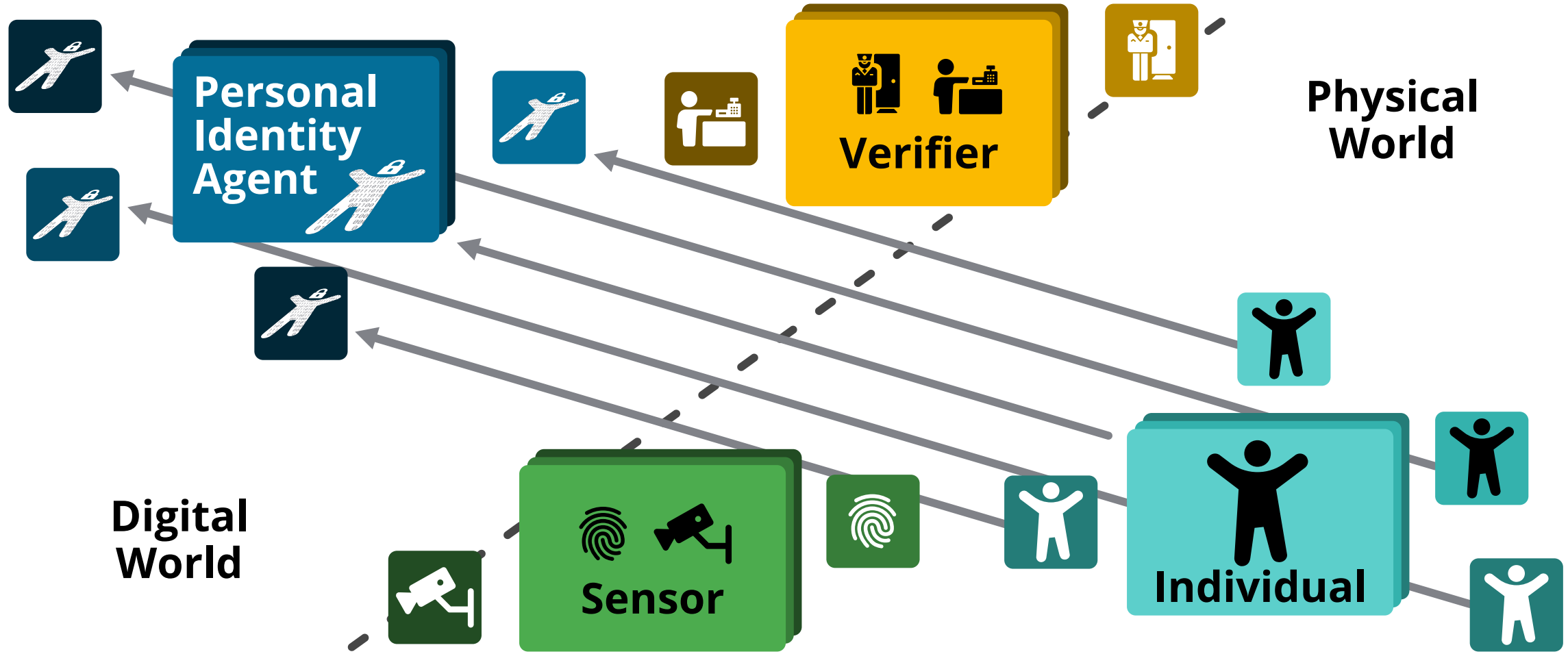


Digital Authentication – Centralized Approach

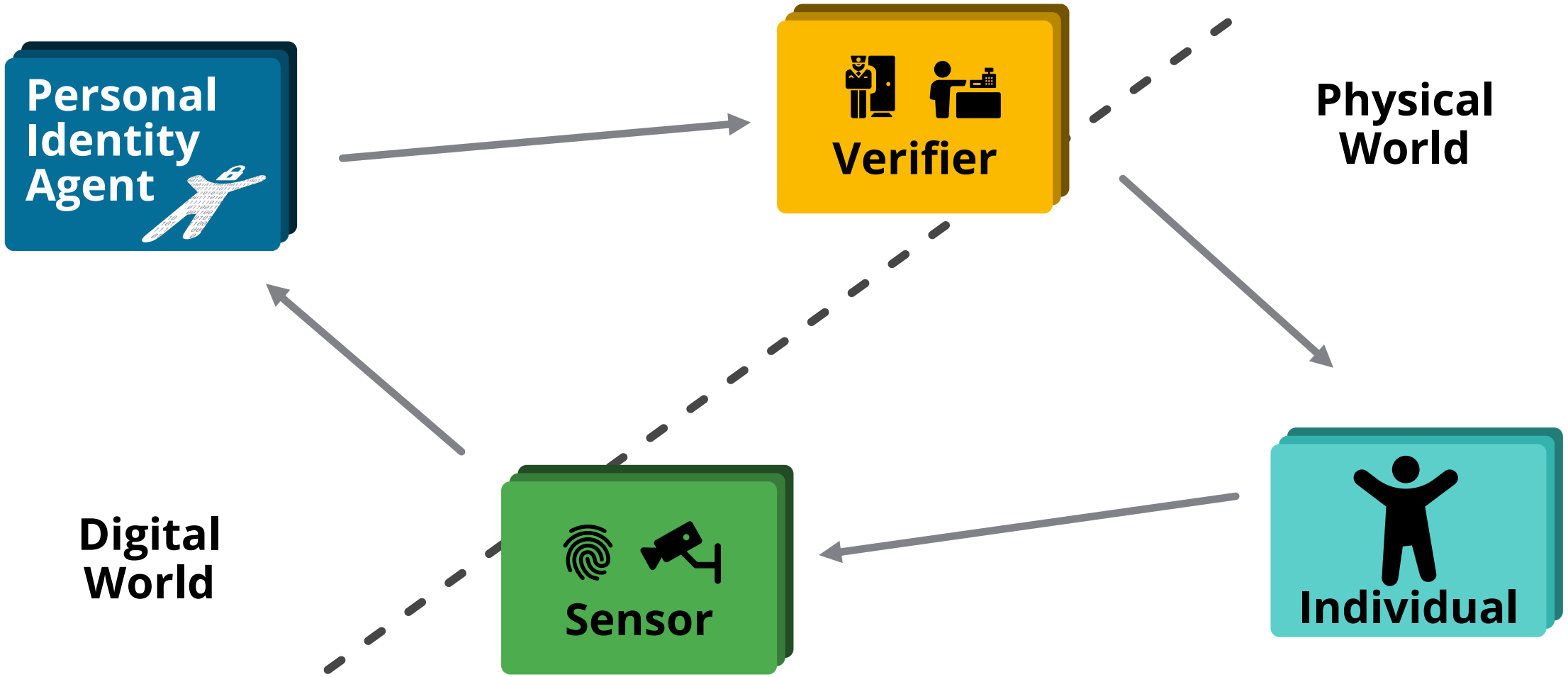



2020
2019
2018
2017
Boots Advantage Card
Buchbinder Car Rentals
Chtrbox
Dutch Government
Houzz
Israeli government
Marriott Hotels 5,200,000
MGM Hotels 10,600,000
Tesco Clubcard
Virgin Media 900,000
Zoom 500,000
Artsy
Bulgarian National Revenue Agency
Blank Media Games
8fit
DataCamp
Australian National University
BreedReady
Dubsmash 162,000,000
Facebook 420,000,000
Ge.tt
Microsoft 44,000,000
Indian Jobseekers 275,000,000
OxyData 380,000,000
Roll20
Petflow
Animoto
Canva
Desjardins Group
DoorDash 4,900,000
Coinmama
Ixigo
Suprema
ShareThis
Toyota
Stronghold Kingdoms
Whitepages
Vårdguiden
US Customs and Border Protection
Wawa 30,000,000
YouNow
WiFi Finder
500px
BookMate
Capital One
HauteLook
Quest Diagnostics
BriansClub 26,000,000
CoffeeMeetsBagel
EyeEm
Fotolog
LocalBlox
Armor Games
Blur
Cathay Pacific Airways
CMS
Dixons Carphone
Grindr
High Tail Hall
Nametests 120,000,000
Orbitz
Quora 100,000,000
Saks and Lord & Taylor
T-Mobile
Ticketmaster
Vision Direct
Urban Massage
Amazon
British Airways
Firebase 100,000,000
Click2Gov
Google+
SKY Brasil
NMBS
Twitter 330,000,000
WordPress
Amazon
Careem
Chinese resume leak 202,000,000
Facebook
Facebook 50,000,000
GovPayNow.com
Marriott Hotels 383,000,000
MBM Company
Mount Olympus 188,000
MyFitnessPal 150,000,000
SingHealth
TicketFly
Dell
Health South East
Healthcare.gov
Panerabread
Texas voter records
ViewFines
MyHeritage
Newegg
Bell
Cellebrite
CEX
DaFont
Disqus
Equifax 143,000,000
Imgur
Hong Kong Registration & Electoral Office
Instagram
Malaysian medical practitioners
Malaysian telcos & MVNOs
RootsWeb
Snapchat
SVR Tracking
TIO Networks
Swedish Transport Agency
Uber 57,000,000
Viacom
Wonga
Zomato
Waterly
Yahoo

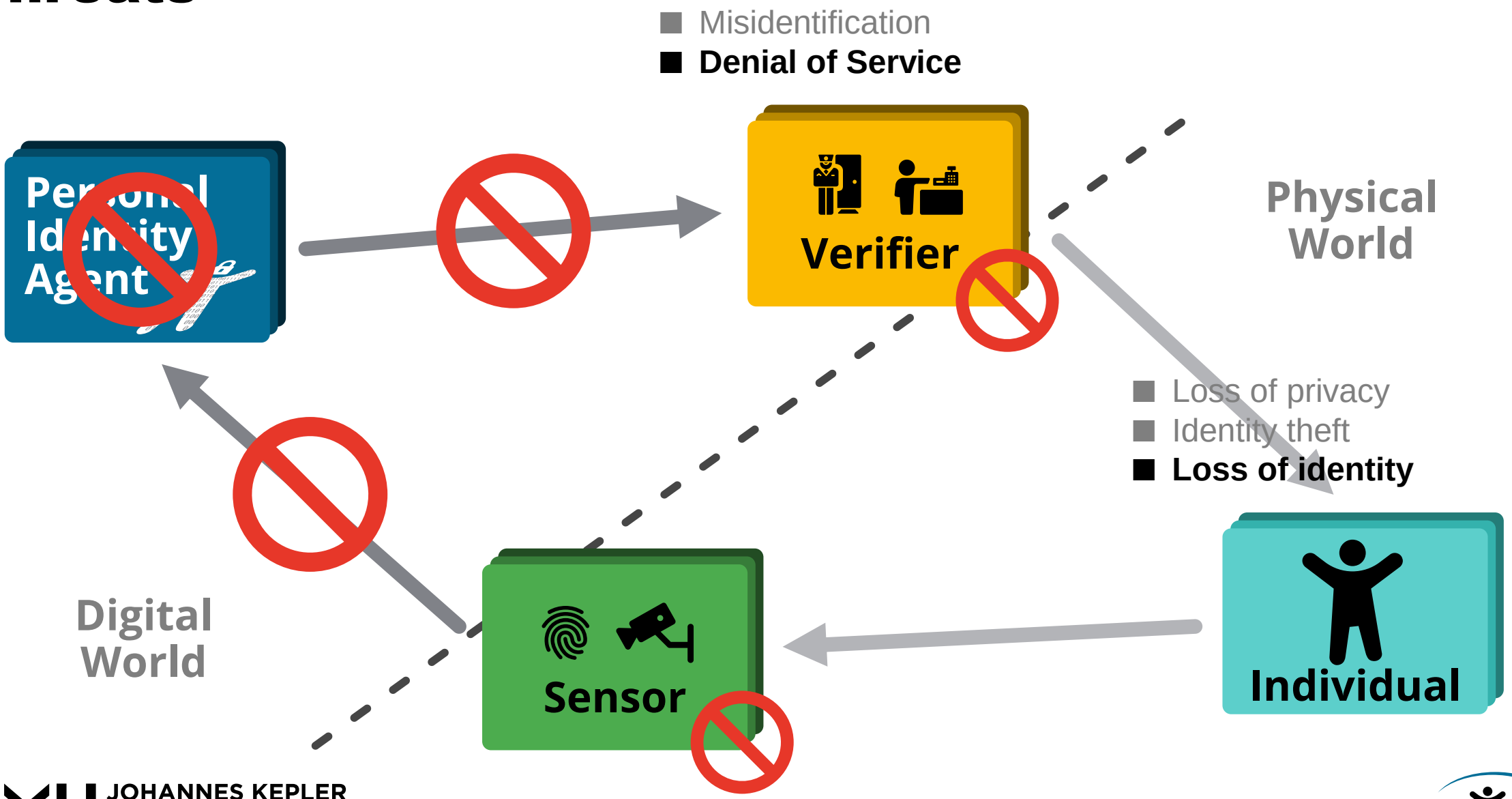
Digital Authentication – Decentralized Approach



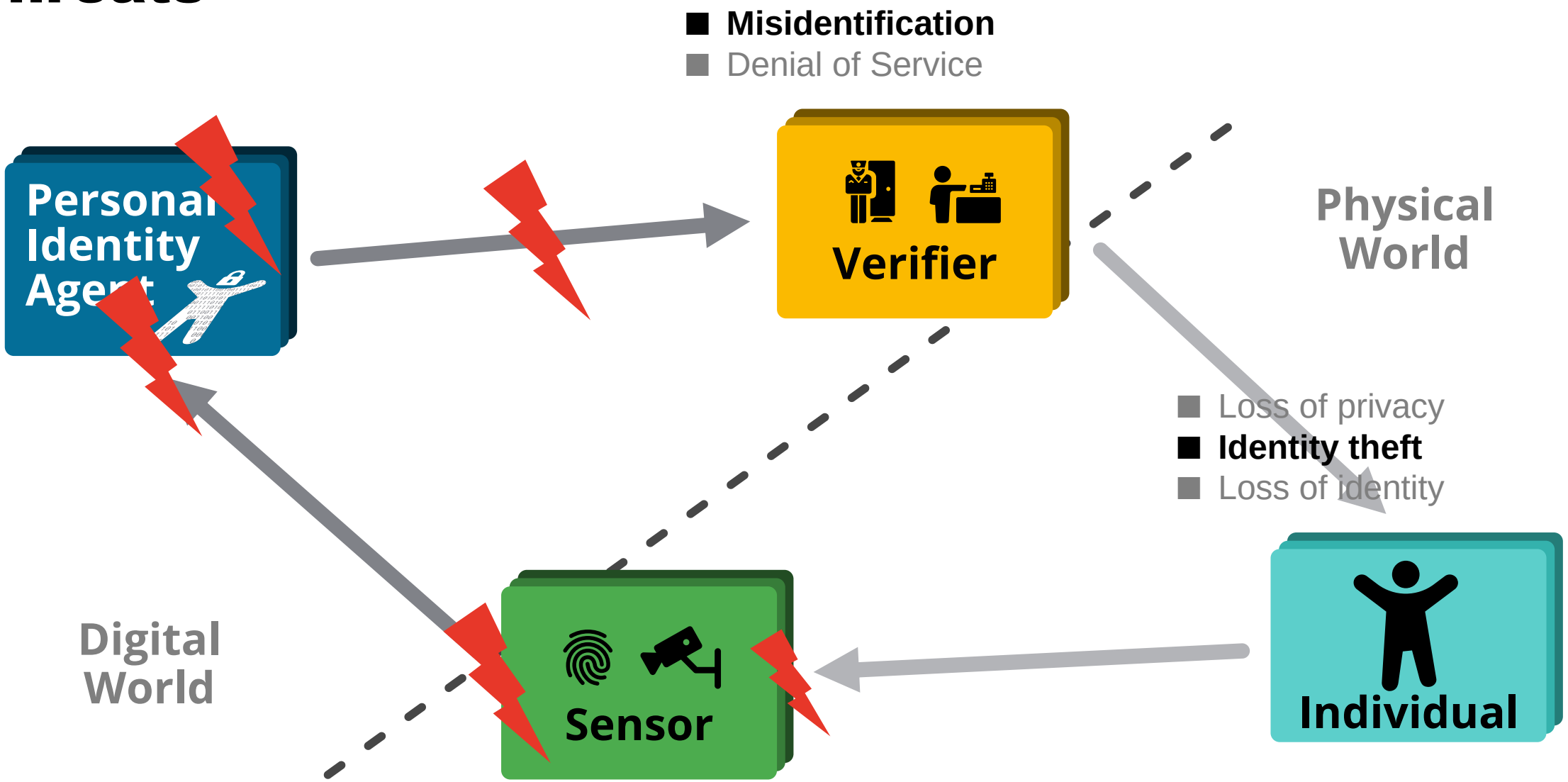
Digital Authentication – Decentralized Approach



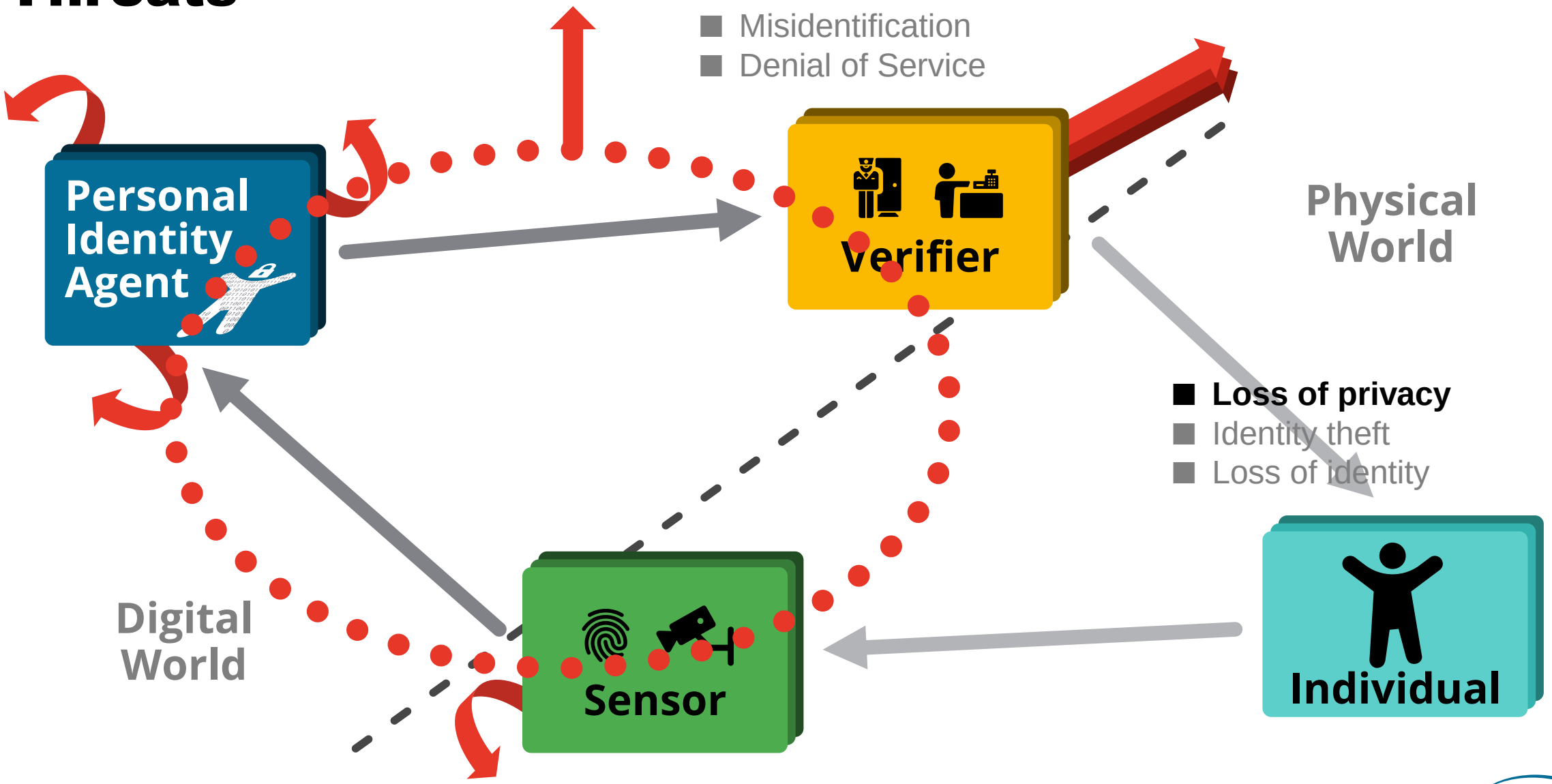
Threats


Misidentification
Denial of Service
Personal Identity Agent
Verifier
Physical World
Loss of privacy
Identity theft
Loss of identity
Digital World
Sensor
Individual

Threats


Misidentification
Denial of Service
Personal Identity Agent
Verifier
Physical World
Loss of privacy
Identity theft
Loss of identity
Digital World
Sensor
Individual

Threats


Misidentification
Denial of Service
Personal Identity Agent
Verifier
Physical World
Loss of privacy
Identity theft
Loss of identity
Digital World
Sensor
Individual

Digital Authentication in the Physical World

Image credit: https://pixabay.com/photos/private-privacy-green-secret-1647769/

JOHANNES KEPLER
UNIVERSITY LINZ

Questions?

Web: https://jku.at/ins
Email: rm@ins.jku.at
Twitter: @rene_mobile
Wire: @rm

DIGiDOW

JOHANNES KEPLER
UNIVERSITY LINZ
Altenberger Straße 69
4040 Linz, Austria
jku.at