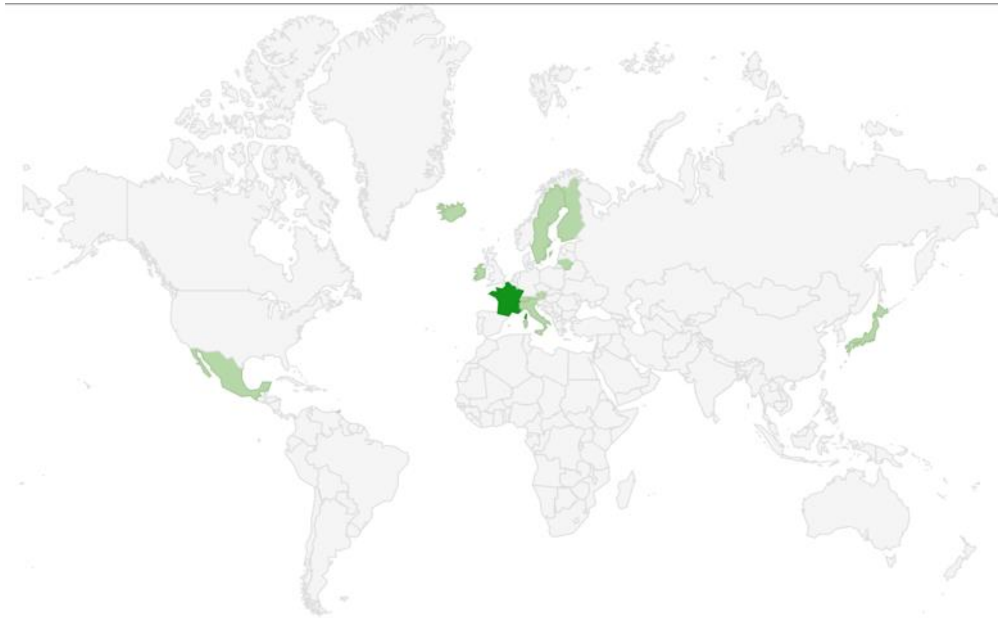
VERIDIUM

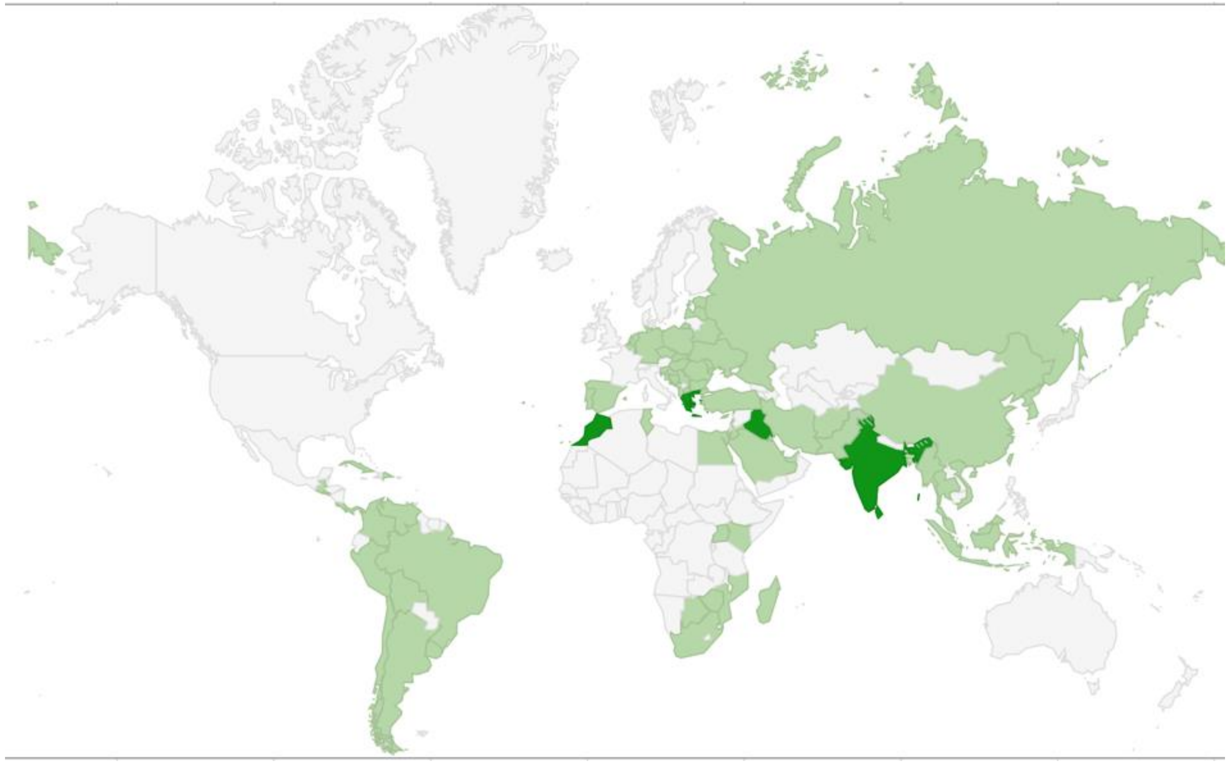
HANDS ON SECURITY

Biometric Authentication via IEEE 2410 and Decentralized Identifiers (DIDs)

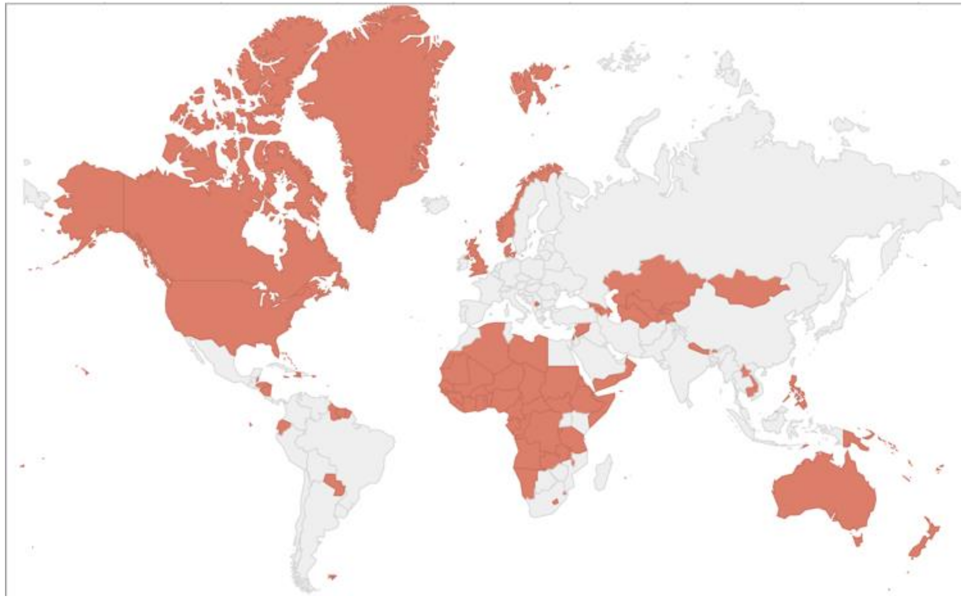
National ID cards: **no growth**



15 Non-compulsory National ID card (FR w/biometrics)



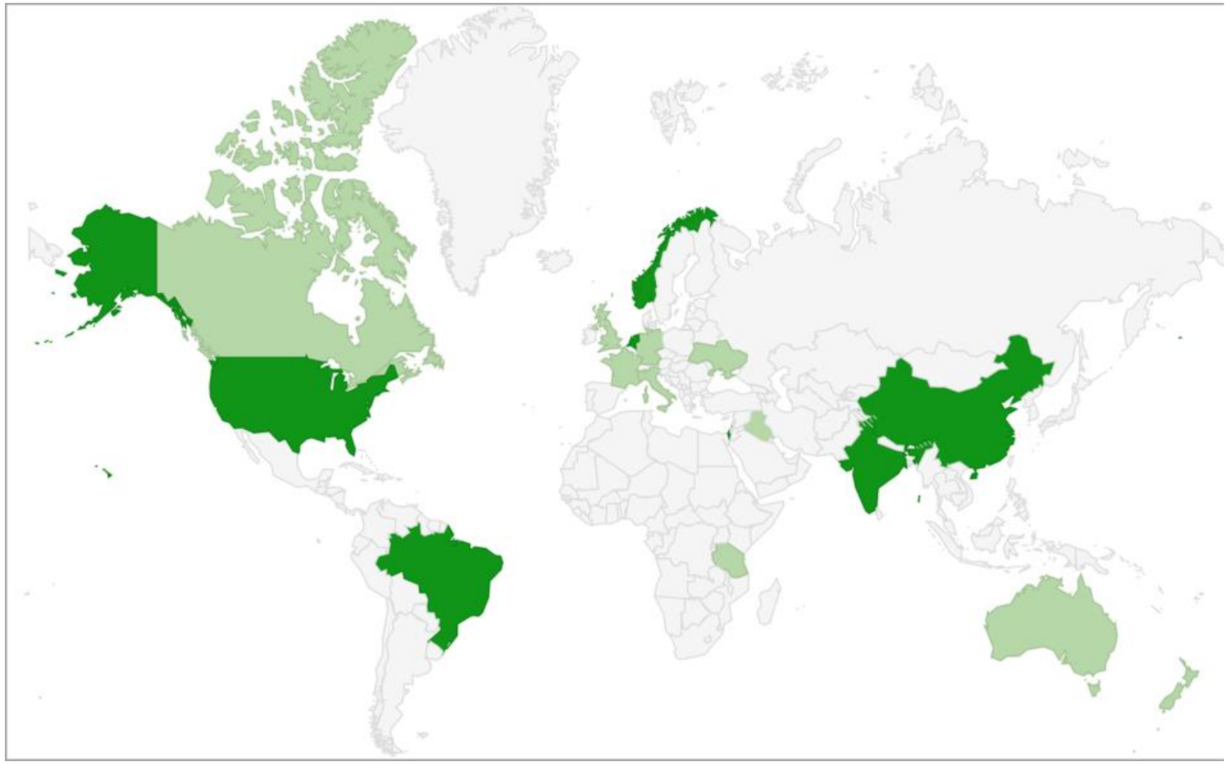
85 Compulsory National ID card
(4+ w/biometrics)



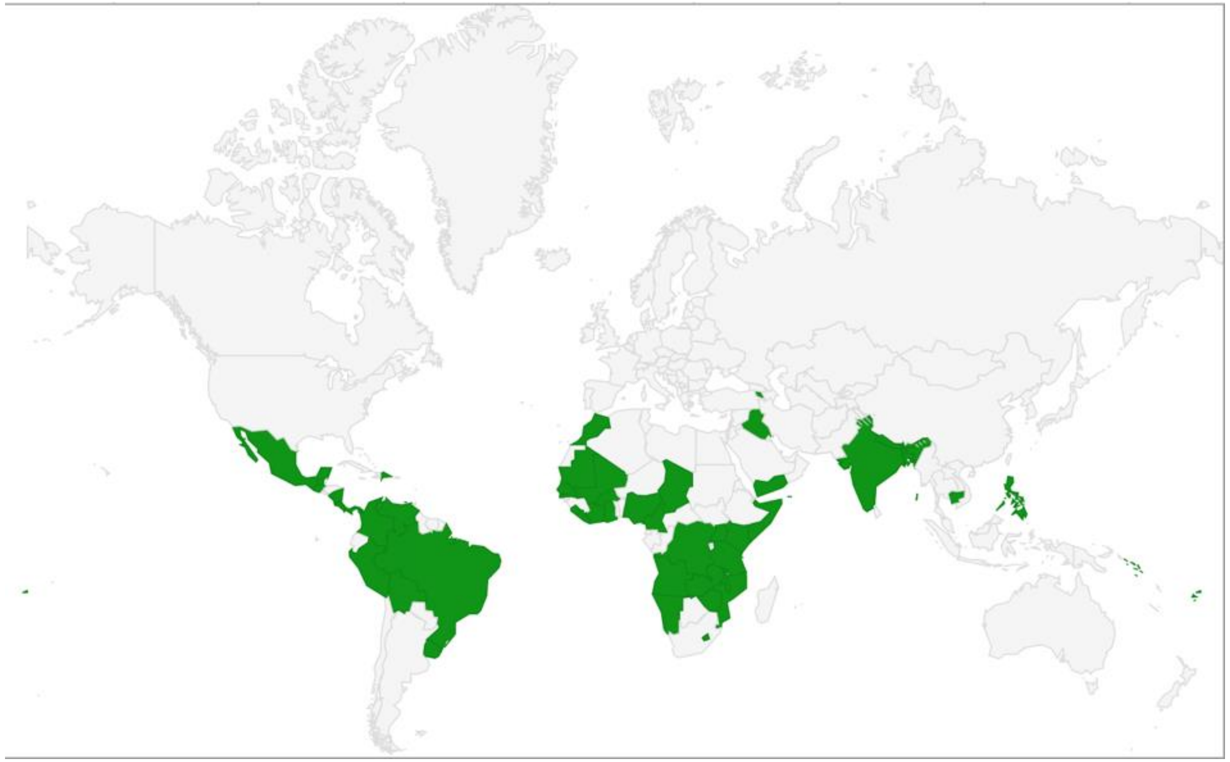
93 w/no national ID card

EVOLUTION

National biometric databases: **growth**

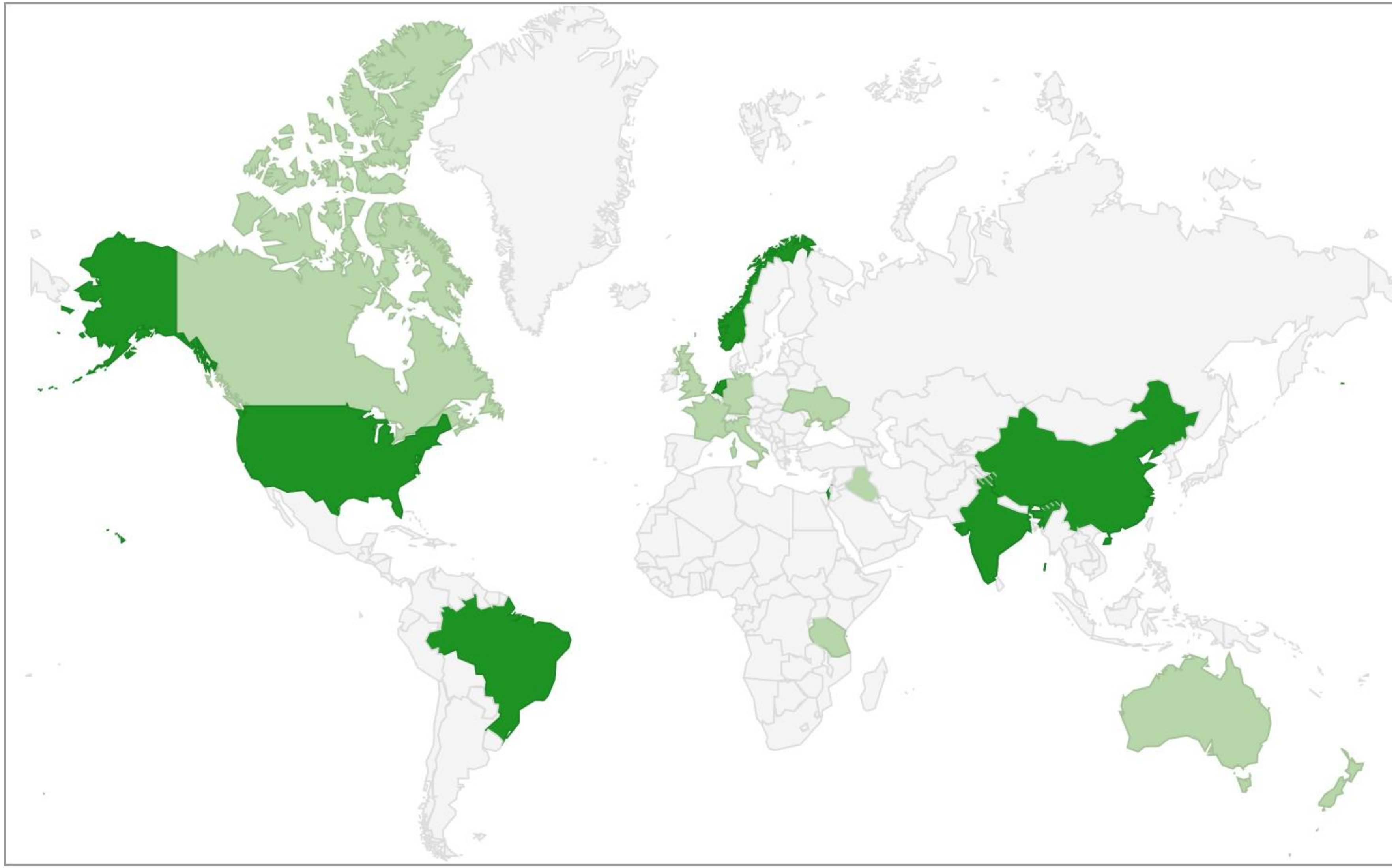


National Biometric Databases
(# of fingerprints)

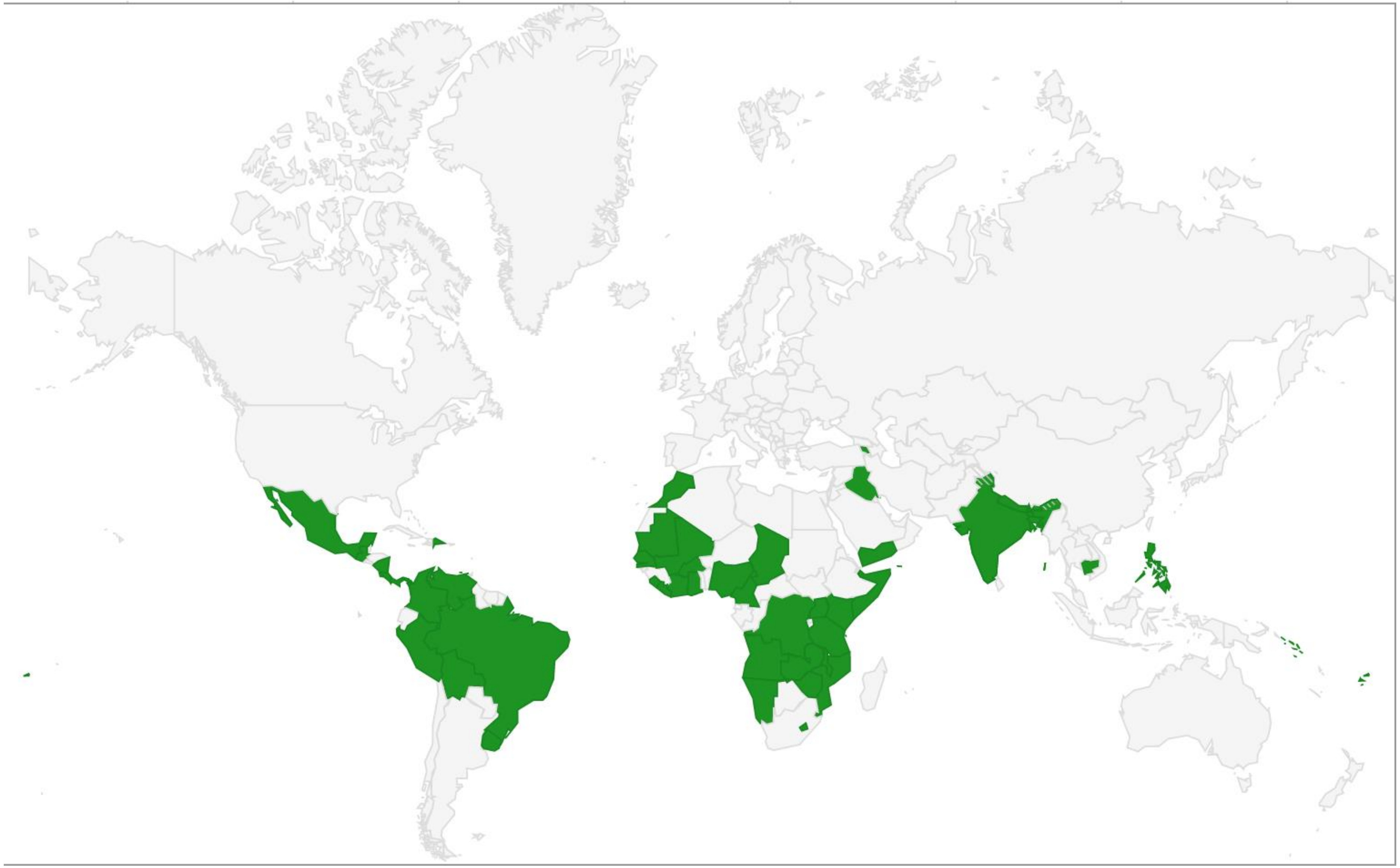


National Biometric Databases for Voting

Country	Fingerprints
Australia	2
Brazil	10
Canada	2
China	10
France	2
Gambia	2
Germany	2
India	10
Iraq	2
Israel	10
Italy	2
Netherlands	10
New Zealand	2
Norway	10
Tanzania	2
Ukraine	2
United Kingdom	2
United States	10



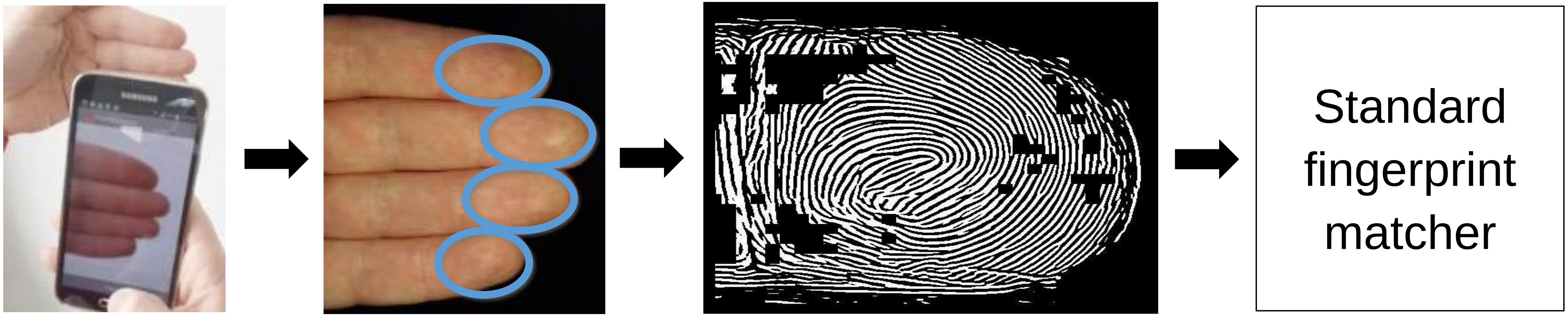
18 National Biometric Databases
(# of fingerprints)



50 National Biometric Databases for Voting

- Armenia
- Angola
- Bangladesh
- Bhutan
- Bolivia
- Brazil
- Burkina Faso
- Cambodia
- Cameroon
- Chad
- Colombia
- Comoros
- Congo (Democratic Republic of)
- Costa Rica
- Ivory Coast
- Dominican Republic,
- Fiji
- Gambia
- Ghana
- Guatemala
- India
- Iraq
- Kenya
- Lesotho
- Liberia
- Malawi
- Mali
- Mauritania
- Mexico
- Morocco
- Mozambique
- Namibia
- Nepal
- Nicaragua
- Nigeria
- Panama
- Peru
- Philippines
- Senegal
- Sierra Leone
- Solomon Islands
- Somaliland
- Swaziland
- Tanzania
- Uganda
- Uruguay
- Venezuela
- Yemen
- Zambia
- Zimbabwe

KYC & AML ENROLLMENT VERIFICATION



Standard fingerprint matcher

Current:

- Required to open account
- Physically show up at a branch
- Prints must be compared to backend federal systems (Mexico & Brazil)

Proposed:

- Allow opening of bank accounts *remotely*
    - *NIST 800-63A allows IL3 remotely with witness*
- Meet KYC & AML compliance
- Account in pending state until verified

BUNQ VIDEO ONBOARDING

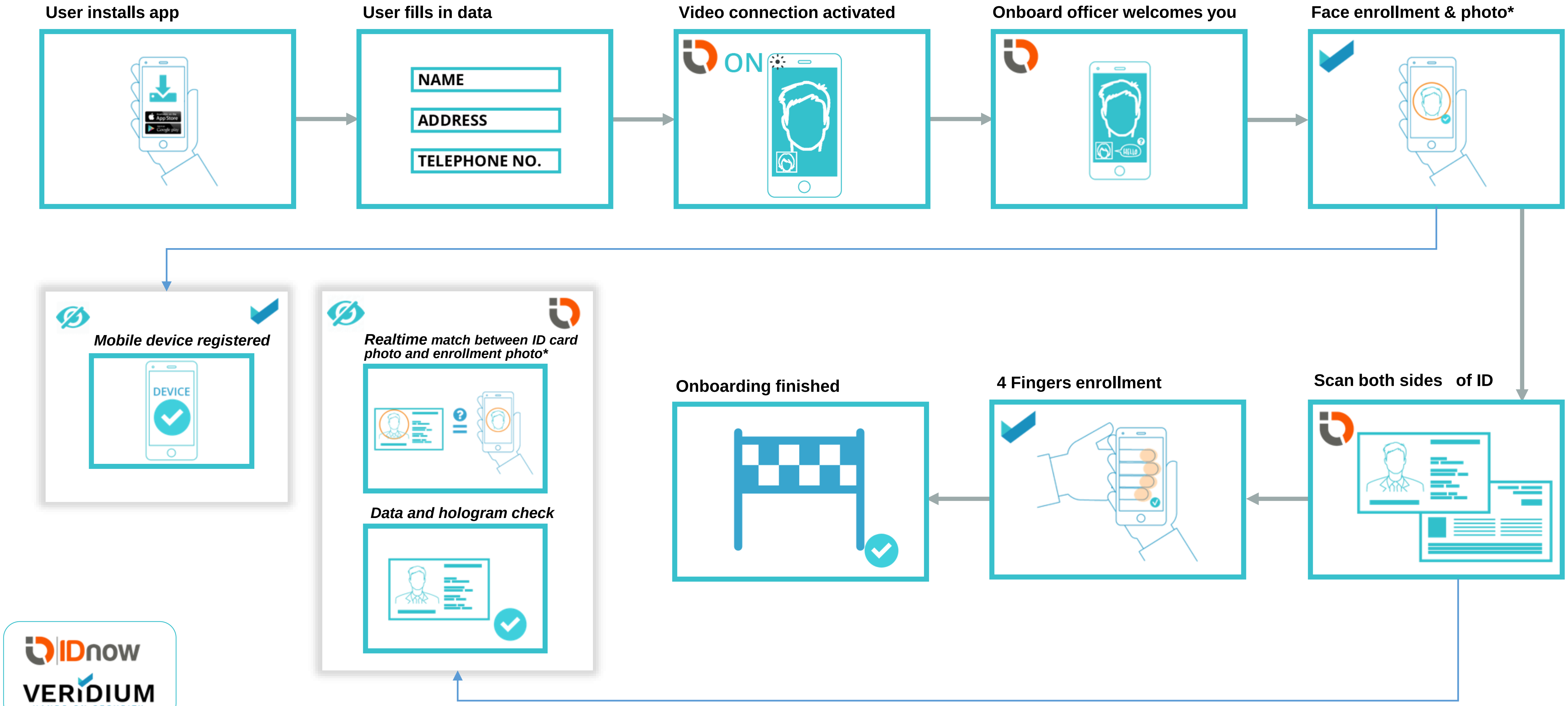
Current:

- Video used to verify identity
- National ID card held up

Proposed:

- Use facial recognition in video
- Interviewer prompts or uses recording post-interview
- Verification process within minutes against national records

INITIAL ONBOARDING & ENROLLMENT



User installs app

User fills in data

Video connection activated

Onboard officer welcomes you

Face enrollment & photo*

Mobile device registered

Scan both sides of ID

4 Fingers enrollment

Onboarding finished

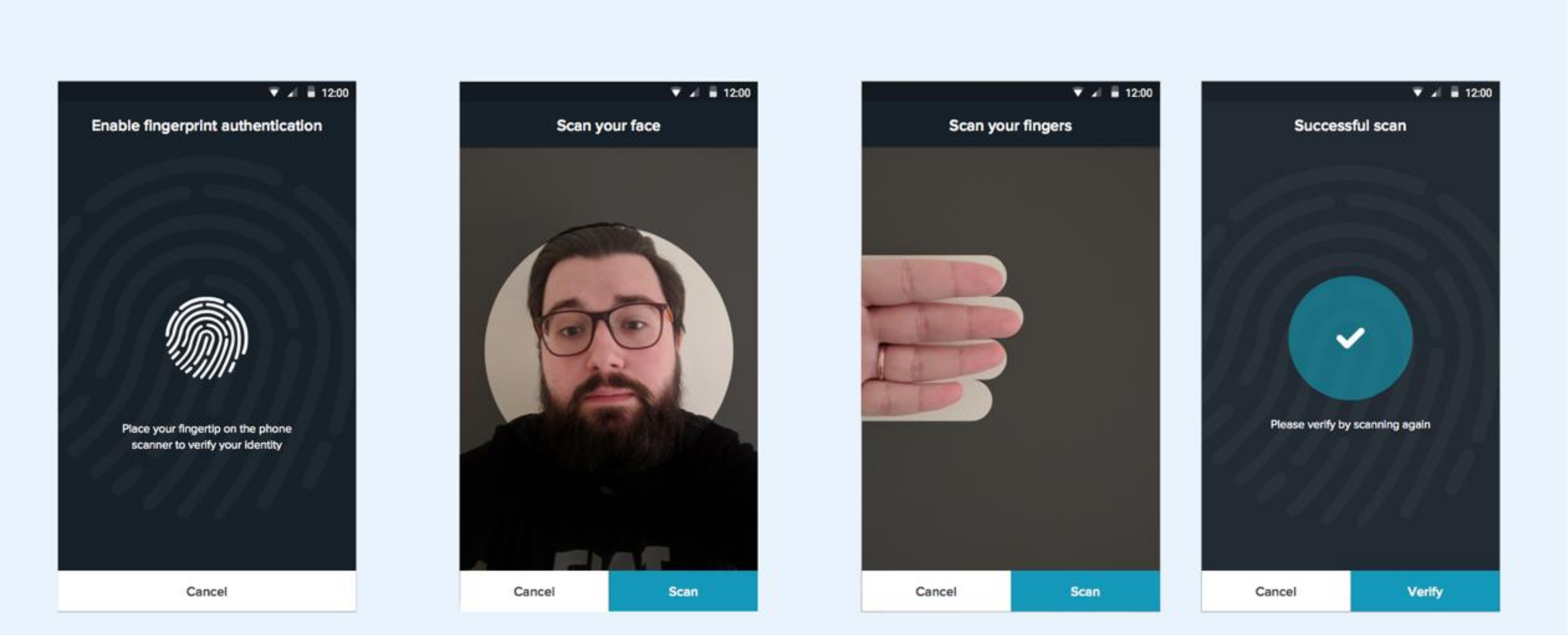
Realtime match between ID card photo and enrollment photo*

Data and hologram check

IDnow

VERIDIUM
HANDS ON SECURITY

AUTHENTICATION



Enable fingerprint authentication

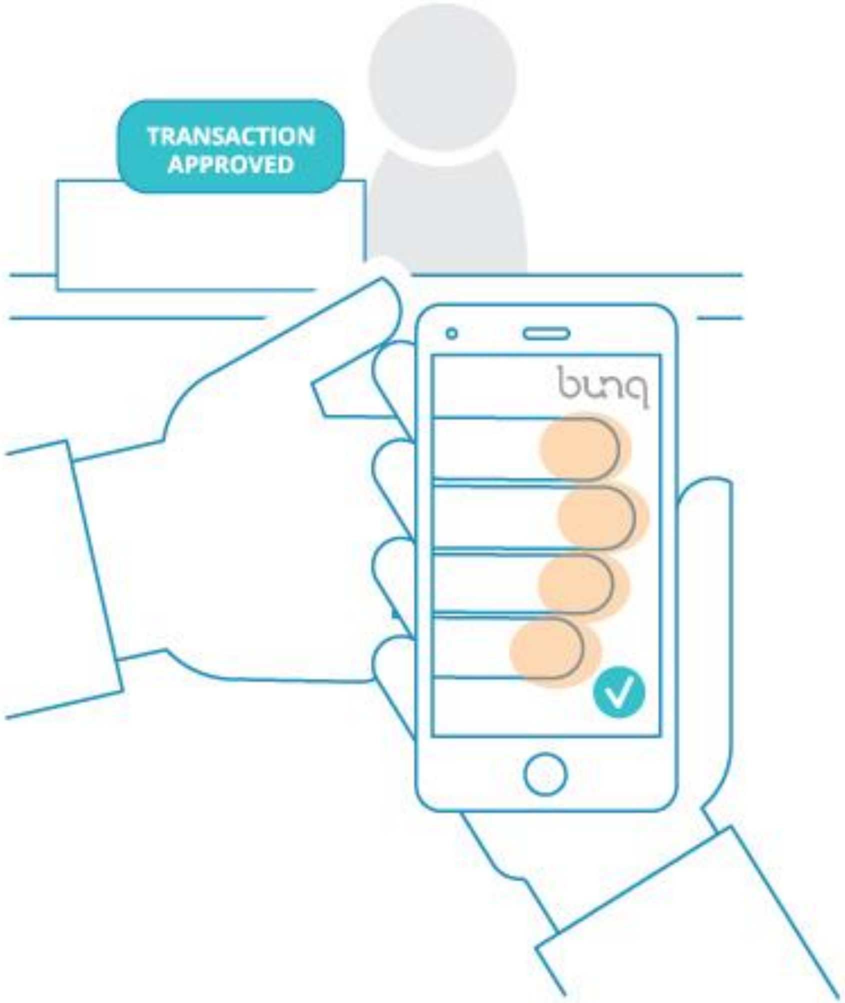
Place your fingertip on the phone scanner to verify your identity

Scan your face

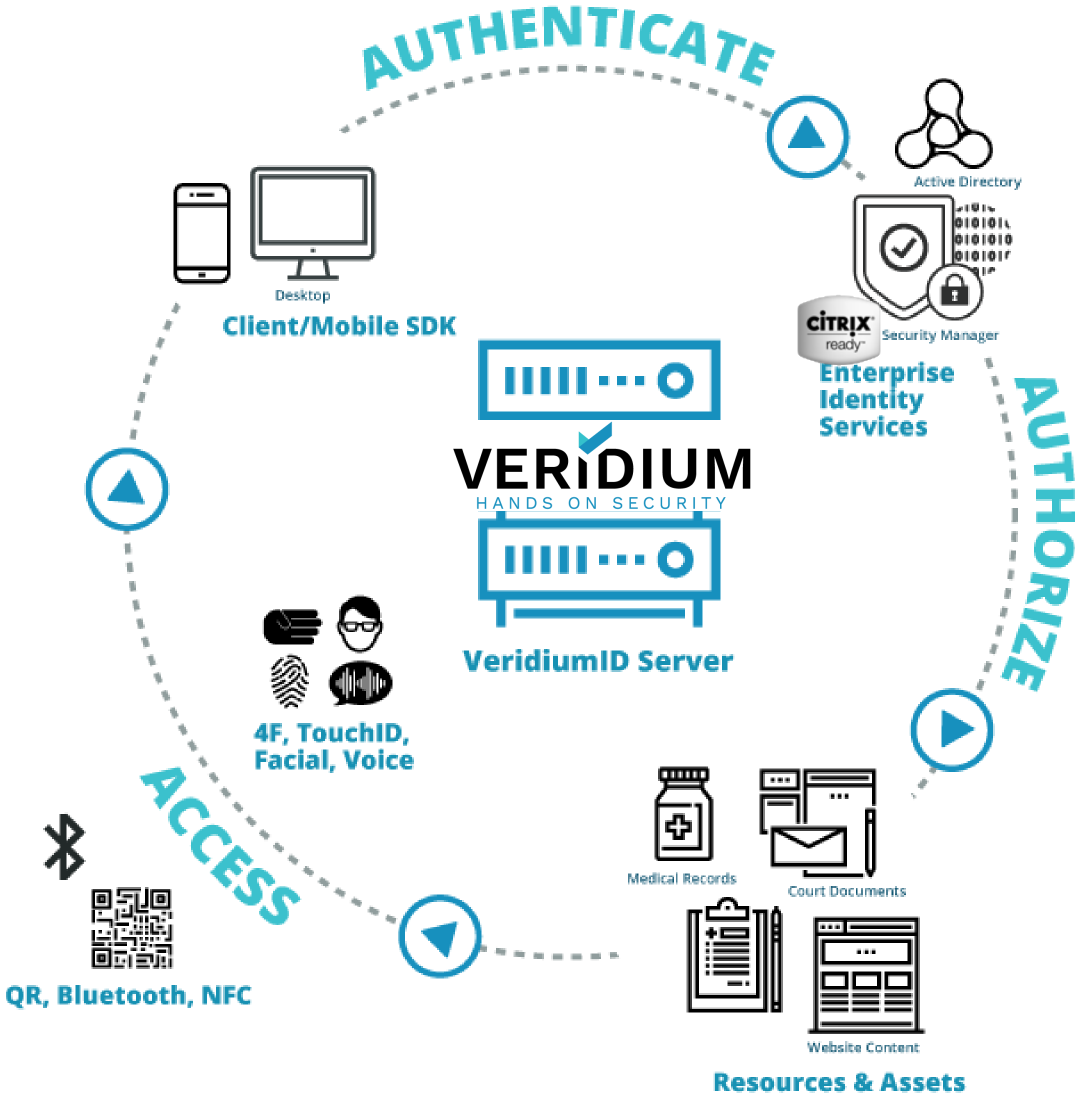
Scan your fingers

Successful scan

Please verify by scanning again



IEEE 2410-2017
Biometric Open Protocol Standard (BOPS)



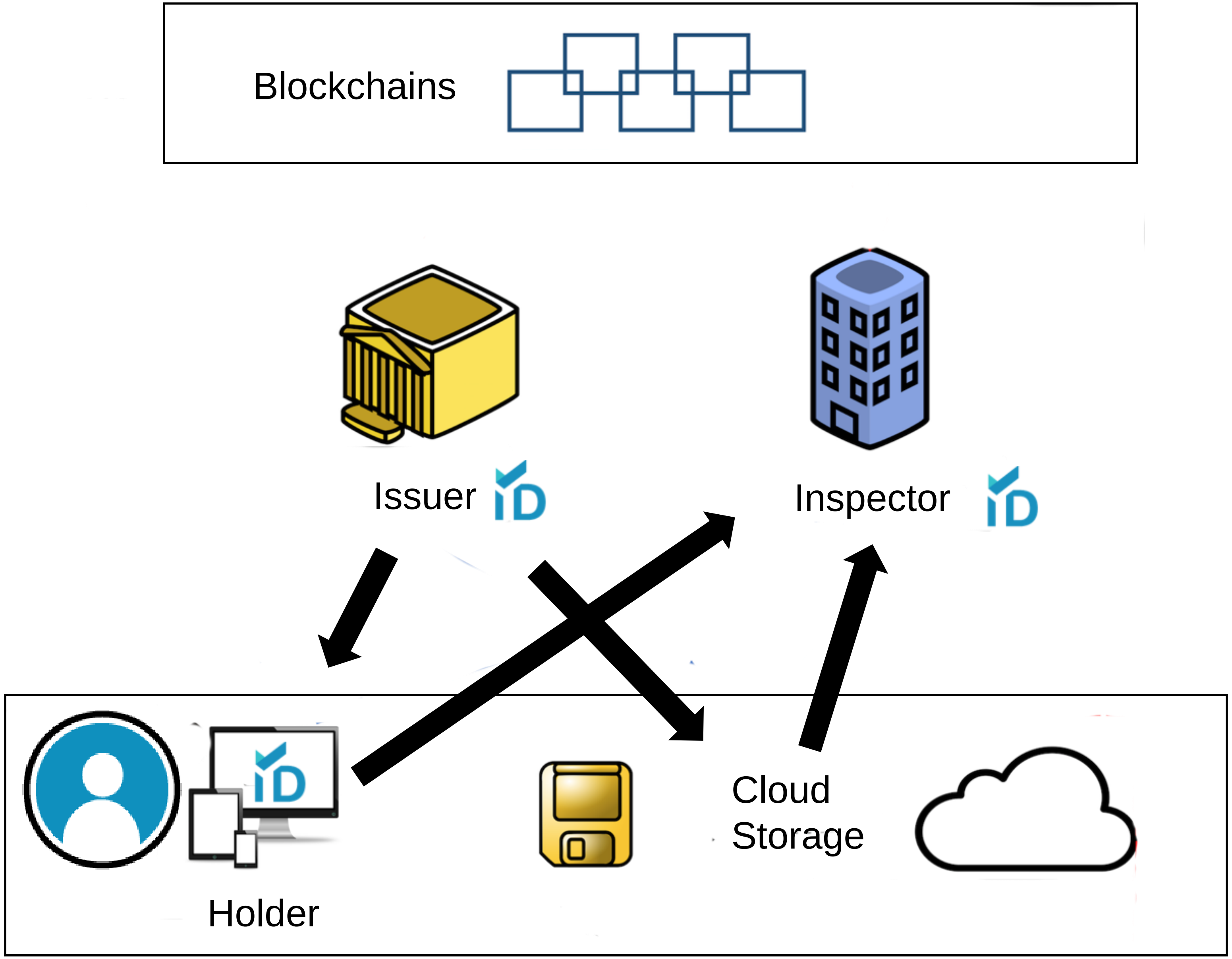
IEEE 2410-2017
Biometric Open Protocol Standard (BOPS)

IEEE 2410-2017 configuration options

Storage	Matching	
	Mobile	Server
Mobile	✓ (FIDO UAF compliant)	✓
Server	✓	✓
Shares (both mobile and server)	✓	✓

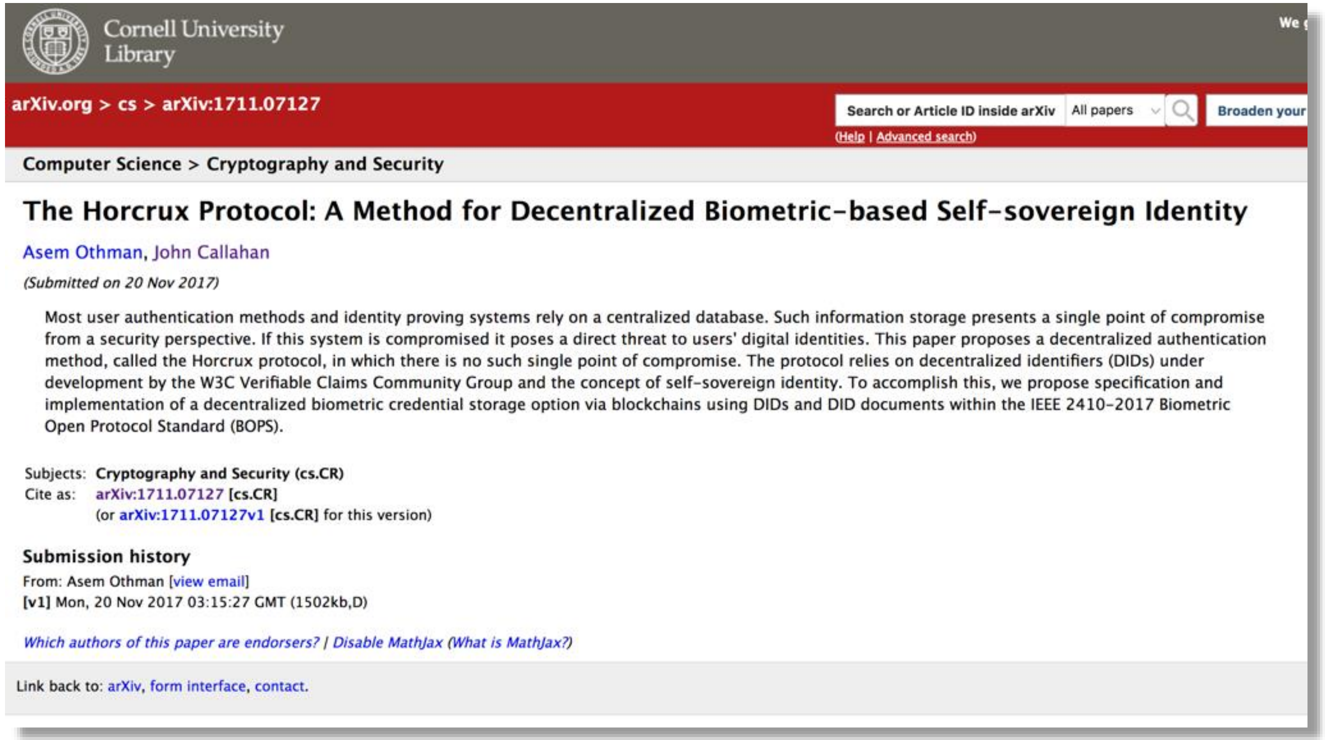
REVOLUTION

SELF-SOVEREIGN IDENTITY



HORCRUX PROTOCOL

- Current:
  - Biometrics held on device and/or server (FIDO UAF & BOPS)
- Future:
  - Biometric Self-Sovereign Identity (B-SSI)
  - References to identity shares via blockchain
  - Actual shares are stored **off-chain**: IPFS, OpenPDS, etc.
  - BOPS servers fetch shares to combine from valid sources (aka Horcruxes)


Cornell University Library
We
arXiv.org > cs > arXiv:1711.07127
Search or Article ID inside arXiv
All papers
Broaden your
(Help | Advanced search)
Computer Science > Cryptography and Security

The Horcrux Protocol: A Method for Decentralized Biometric-based Self-sovereign Identity

Asem Othman, John Callahan

(Submitted on 20 Nov 2017)

Most user authentication methods and identity proving systems rely on a centralized database. Such information storage presents a single point of compromise from a security perspective. If this system is compromised it poses a direct threat to users' digital identities. This paper proposes a decentralized authentication method, called the Horcrux protocol, in which there is no such single point of compromise. The protocol relies on decentralized identifiers (DIDs) under development by the W3C Verifiable Claims Community Group and the concept of self-sovereign identity. To accomplish this, we propose specification and implementation of a decentralized biometric credential storage option via blockchains using DIDs and DID documents within the IEEE 2410-2017 Biometric Open Protocol Standard (BOPS).

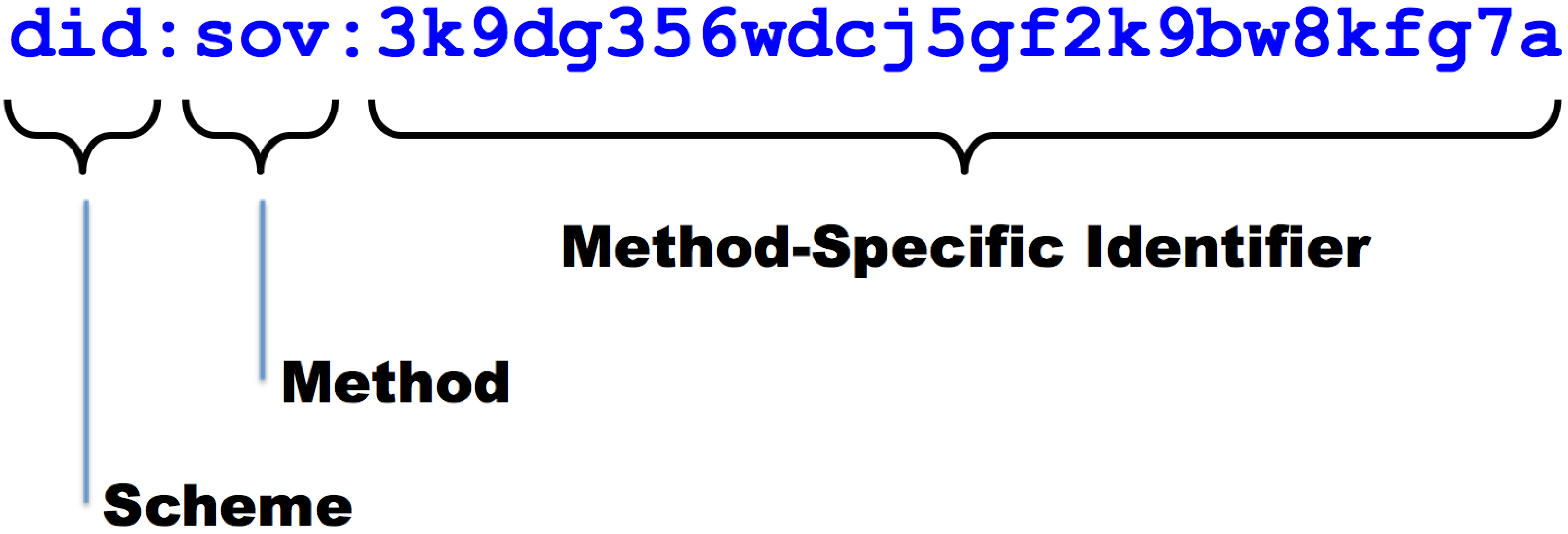
Subjects: **Cryptography and Security (cs.CR)**
Cite as: arXiv:1711.07127 **[cs.CR]**
(or **arXiv:1711.07127v1** **[cs.CR]** for this version)

Submission history
From: Asem Othman [view email]
[v1] Mon, 20 Nov 2017 03:15:27 GMT (1502kb,D)

Which authors of this paper are endorsers? | Disable MathJax (What is MathJax?)

Link back to: arXiv, form interface, contact.

Decentralized Identifiers (DIDs)



`did:sov:3k9dg356wdcj5gf2k9bw8kfg7a`

Method-Specific Identifier

Method

Scheme

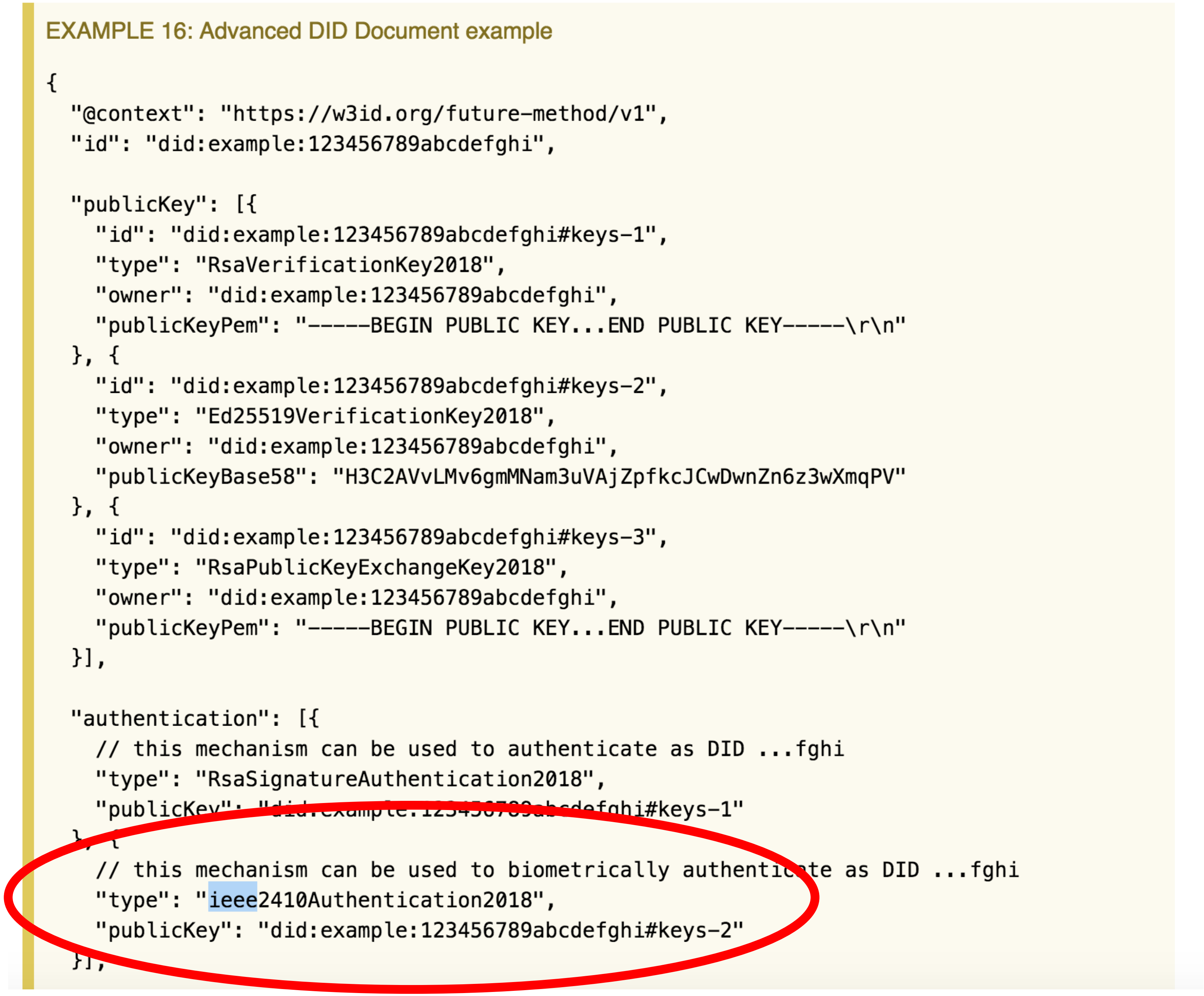
Decentralized Identifiers (DIDs)

did:***btcr***:34832AEED3729DE891-0A237BBE42323C

did:***sov***:C4718341-031917223490EF231299A2210

did:***ipid***:AA323CF23187324-123430DAB34891490

did:***v1***:FF900987483409890ECD323489823488C7



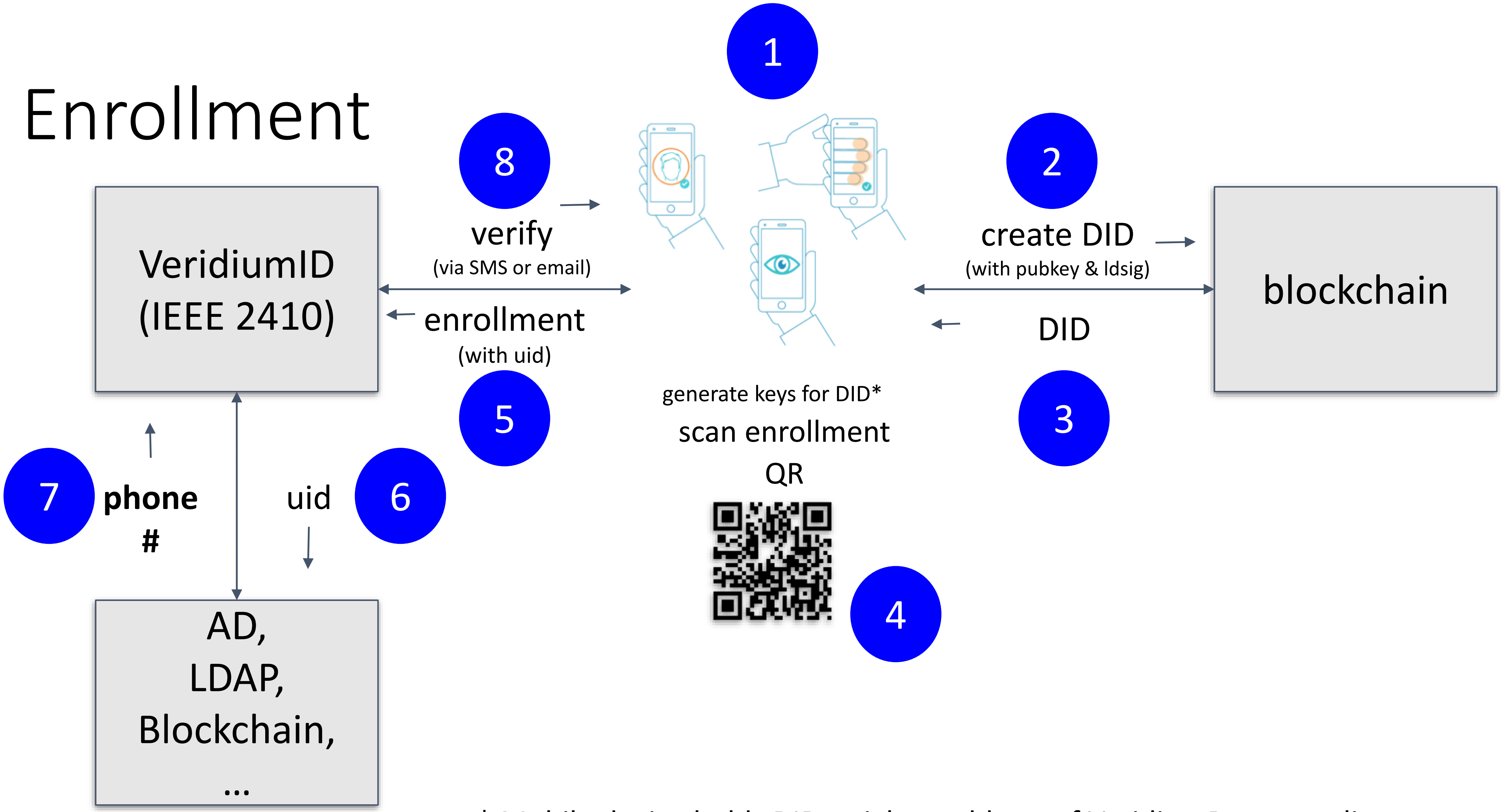
EXAMPLE 16: Advanced DID Document example

```
{
  "@context": "https://w3id.org/future-method/v1",
  "id": "did:example:123456789abcdefghi",

  "publicKey": [{
    "id": "did:example:123456789abcdefghi#keys-1",
    "type": "RsaVerificationKey2018",
    "owner": "did:example:123456789abcdefghi",
    "publicKeyPem": "-----BEGIN PUBLIC KEY...END PUBLIC KEY-----\r\n"
  }, {
    "id": "did:example:123456789abcdefghi#keys-2",
    "type": "Ed25519VerificationKey2018",
    "owner": "did:example:123456789abcdefghi",
    "publicKeyBase58": "H3C2AVvLMv6gmMNam3uVAjZpfkcJCwDwnZn6z3wXmqPV"
  }, {
    "id": "did:example:123456789abcdefghi#keys-3",
    "type": "RsaPublicKeyExchangeKey2018",
    "owner": "did:example:123456789abcdefghi",
    "publicKeyPem": "-----BEGIN PUBLIC KEY...END PUBLIC KEY-----\r\n"
  }],

  "authentication": [{
    // this mechanism can be used to authenticate as DID ...fghi
    "type": "RsaSignatureAuthentication2018",
    "publicKey": "did:example:123456789abcdefghi#keys-1"
  }, {
    // this mechanism can be used to biometrically authenticate as DID ...fghi
    "type": "ieee2410Authentication2018",
    "publicKey": "did:example:123456789abcdefghi#keys-2"
  }],
```

Enrollment



1

8

verify
(via SMS or email)

enrollment
(with uid)

5

2

create DID
(with pubkey & ldsig)

DID

3

VeridiumID
(IEEE 2410)

blockchain

generate keys for DID*

scan enrollment
QR

4

7

phone
#

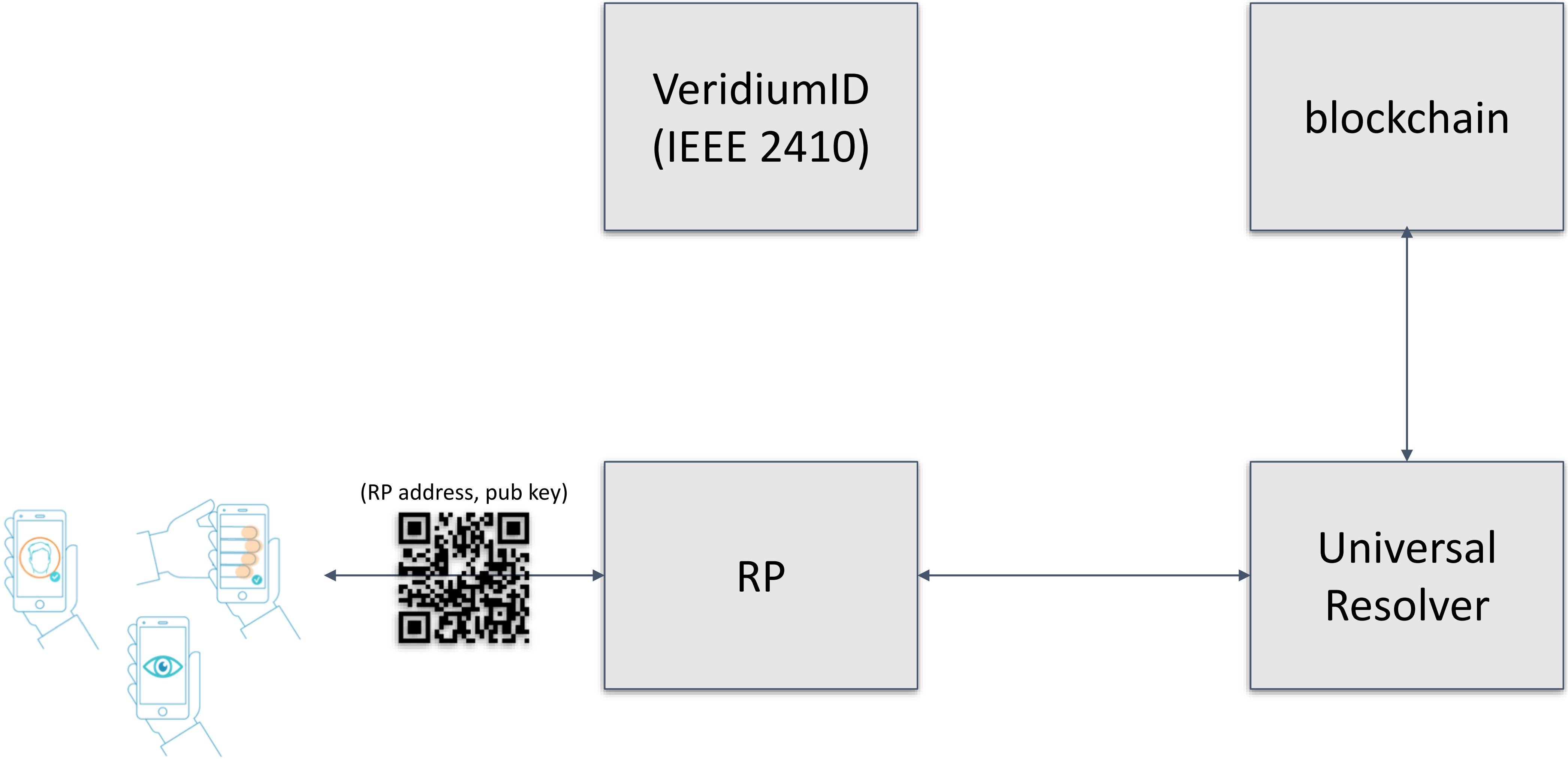
uid

6

AD,
LDAP,
Blockchain,
...

* Mobile device holds DID, privkey, address of VeridiumD server, client cert, and uid

Authentication



VeridiumID (IEEE 2410)

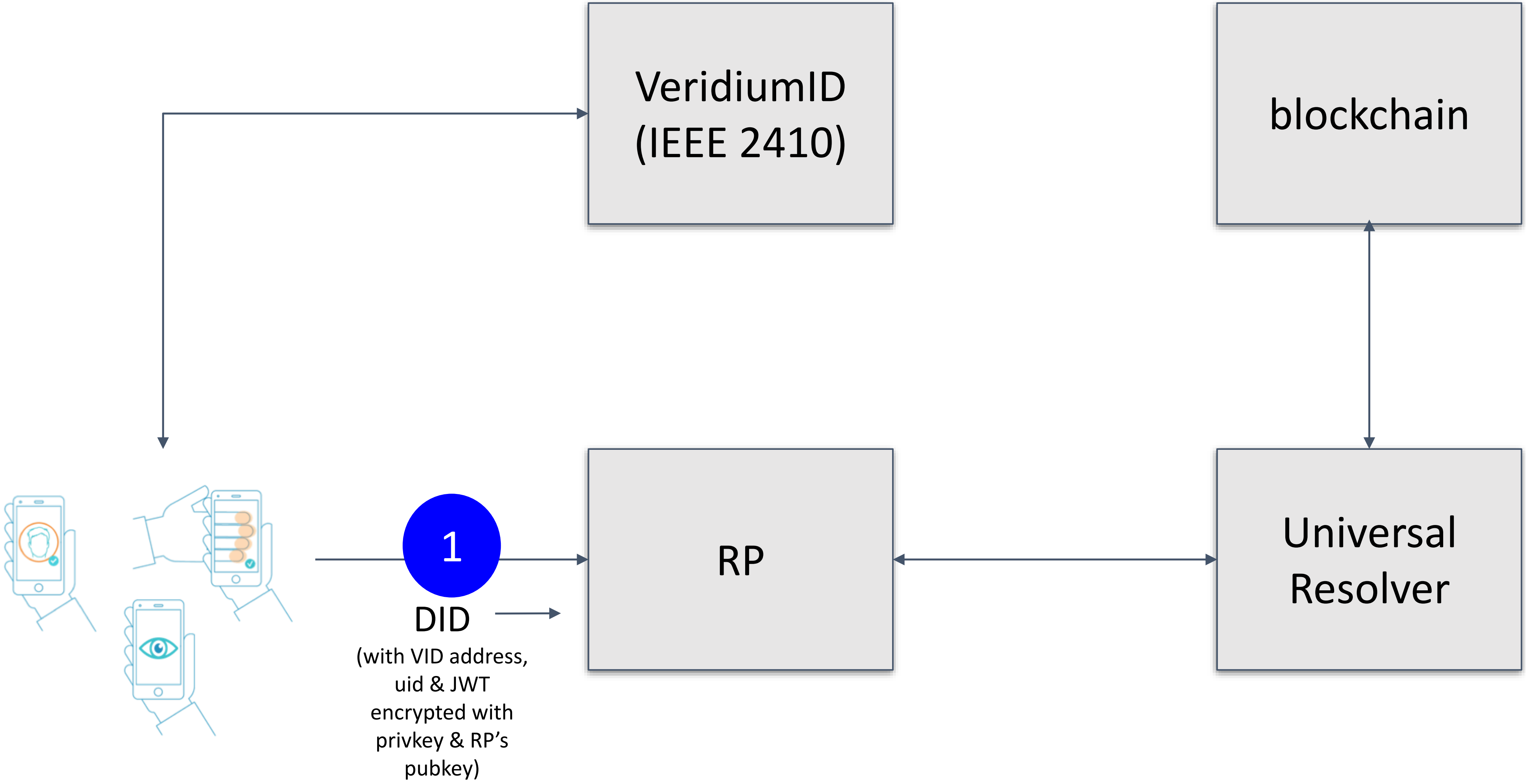
blockchain

(RP address, pub key)

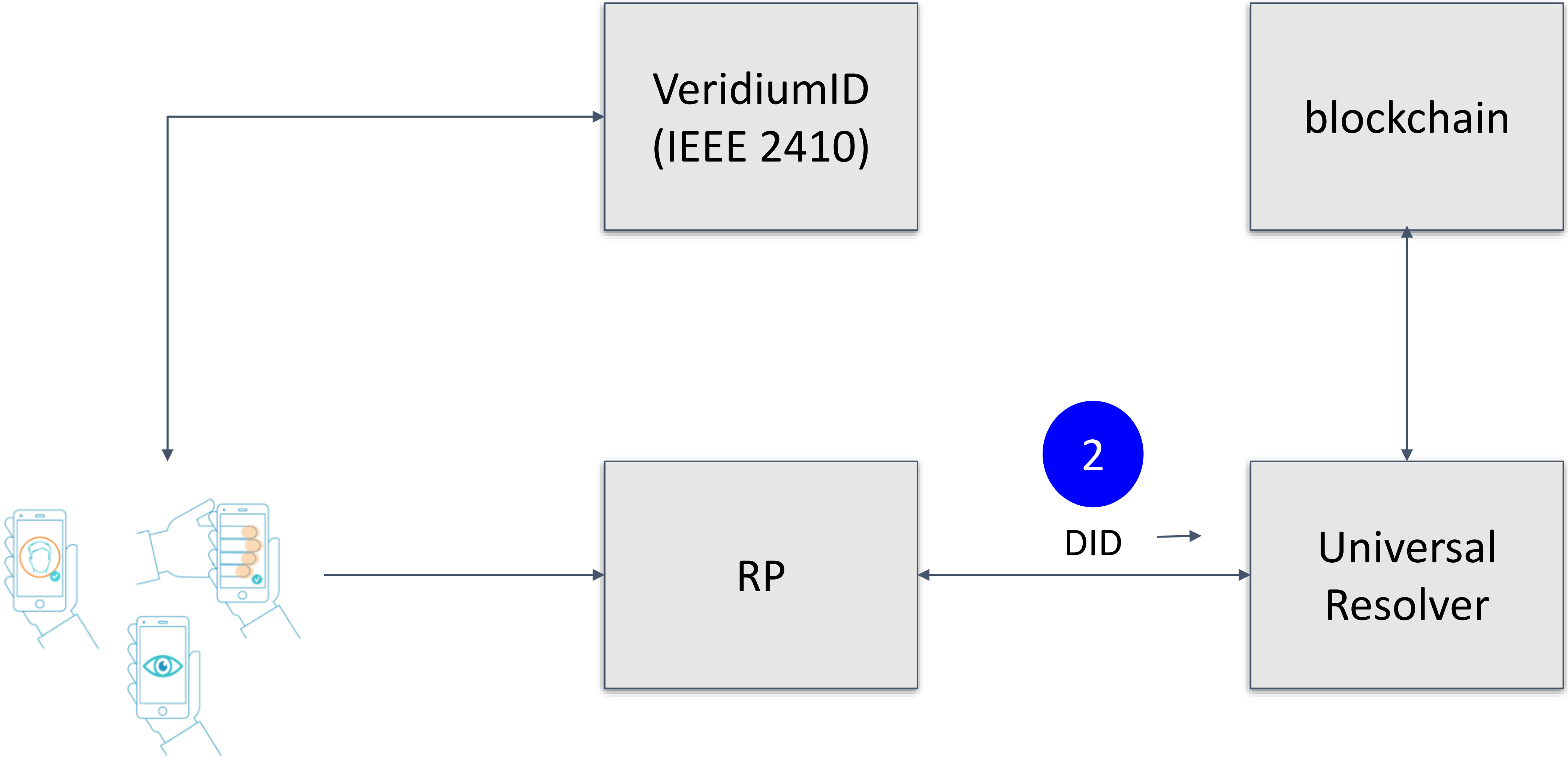
RP

Universal Resolver

Authentication



Authentication



VeridiumID (IEEE 2410)

blockchain

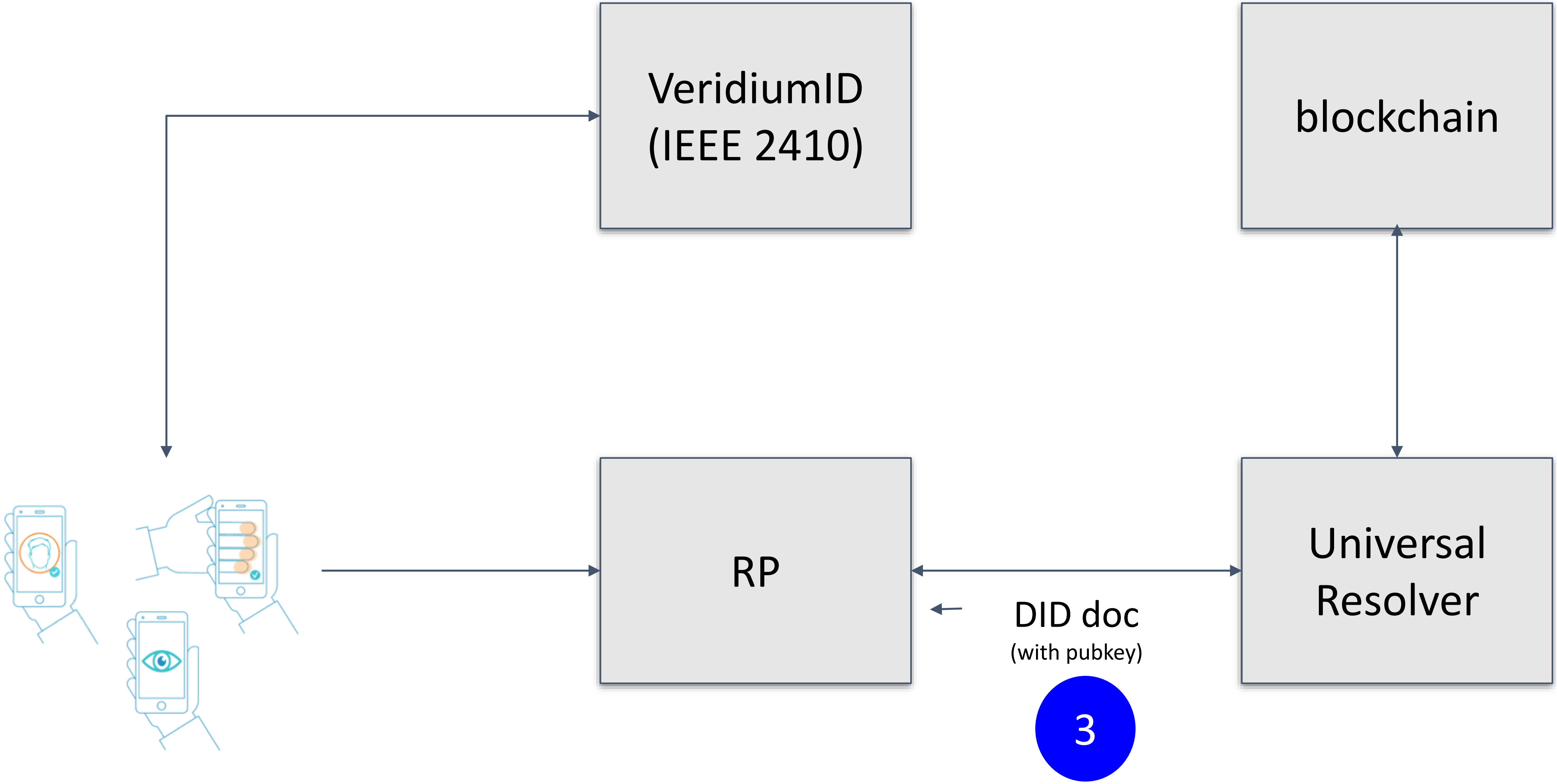
2

DID

RP

Universal Resolver

Authentication



VeridiumID (IEEE 2410)

blockchain

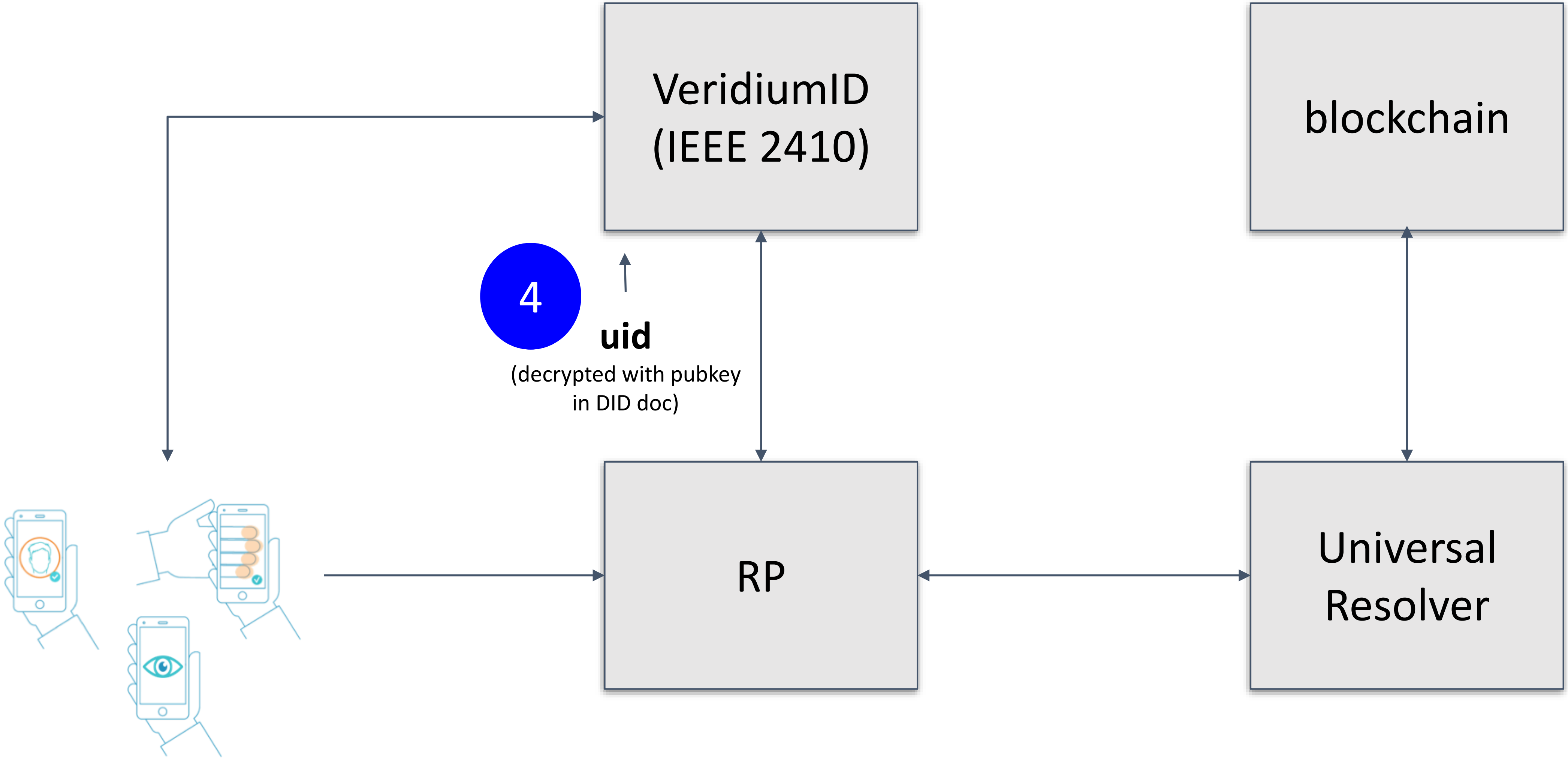
RP

Universal Resolver

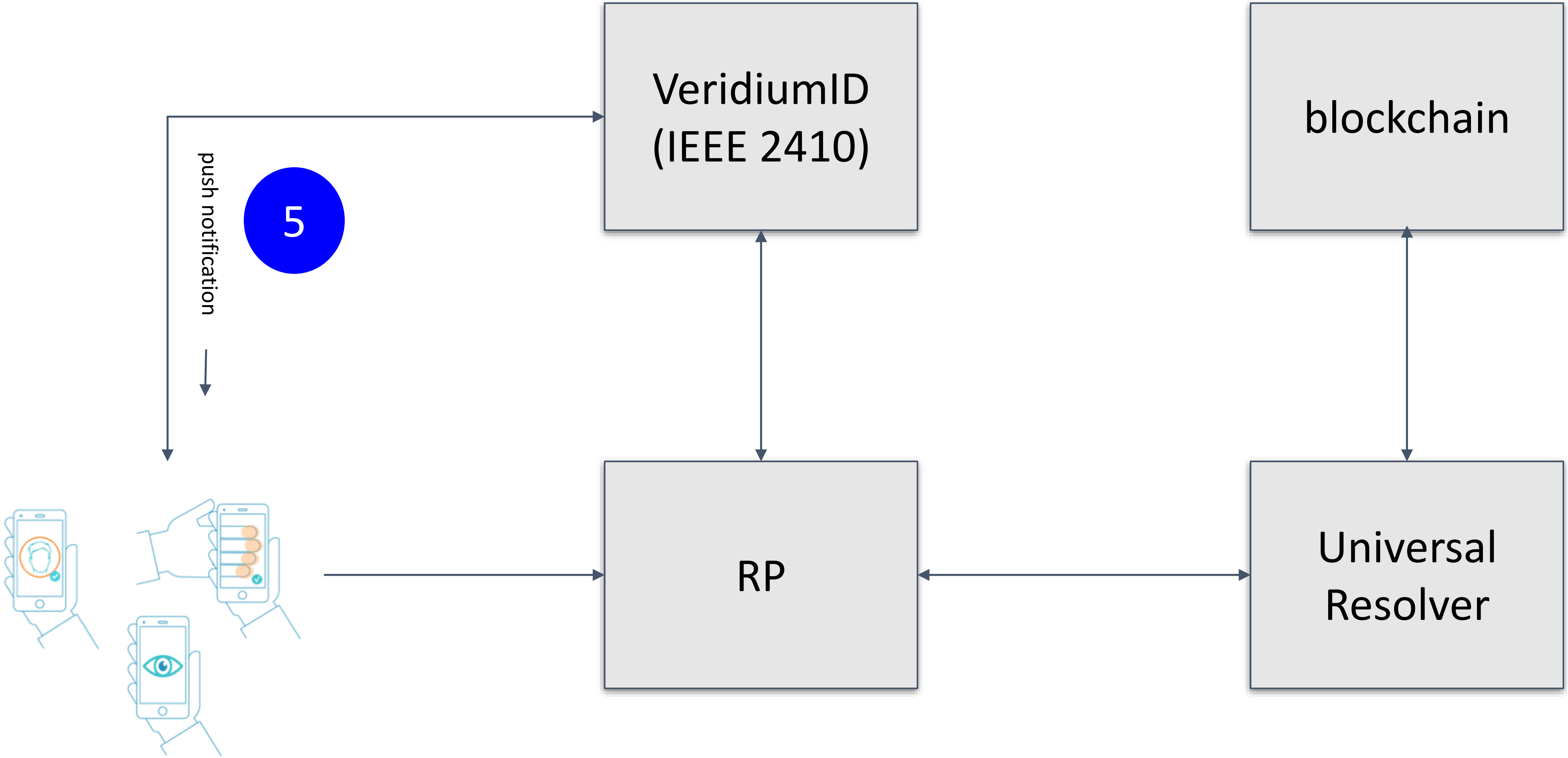
DID doc (with pubkey)

3

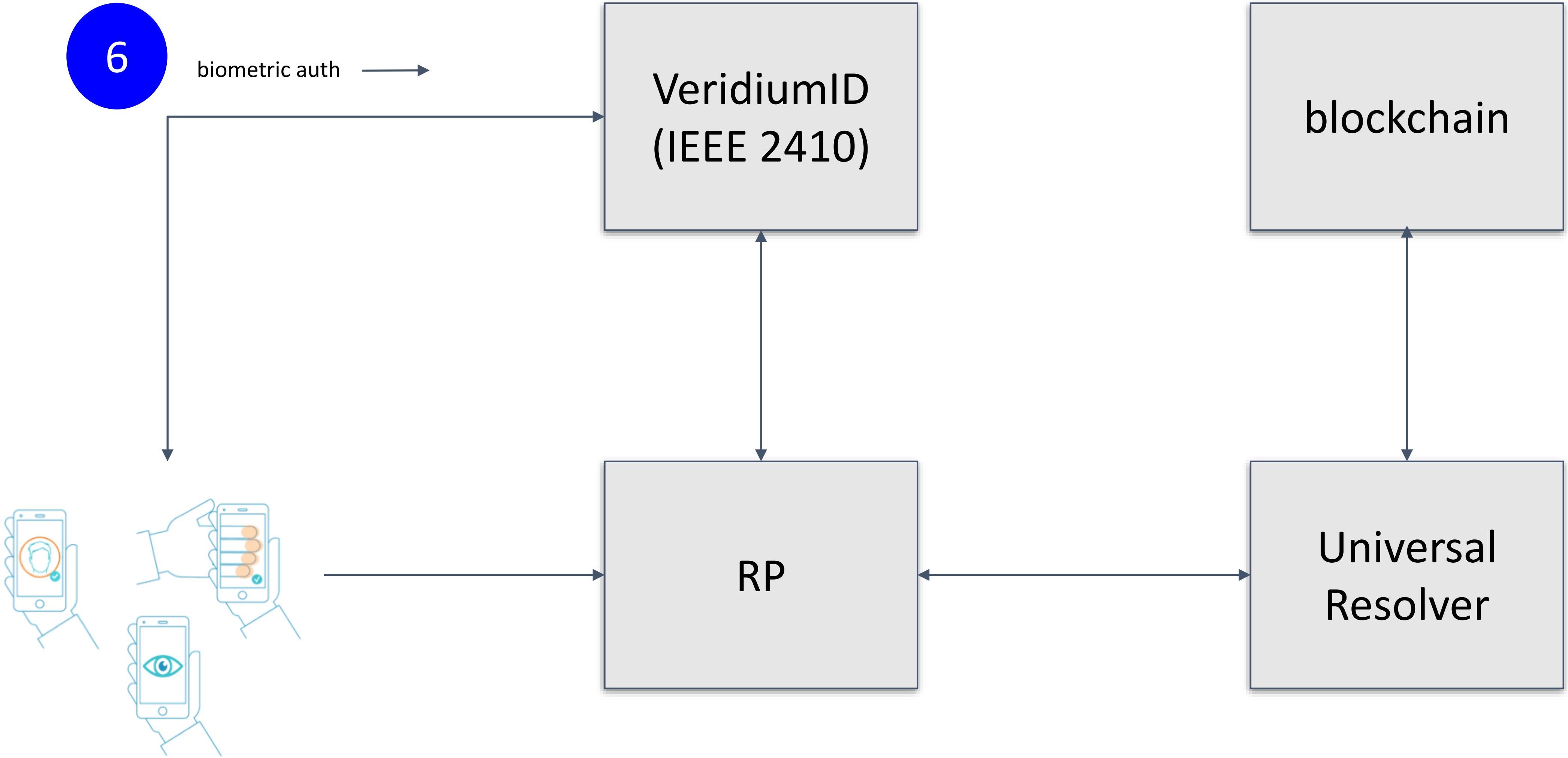
Authentication



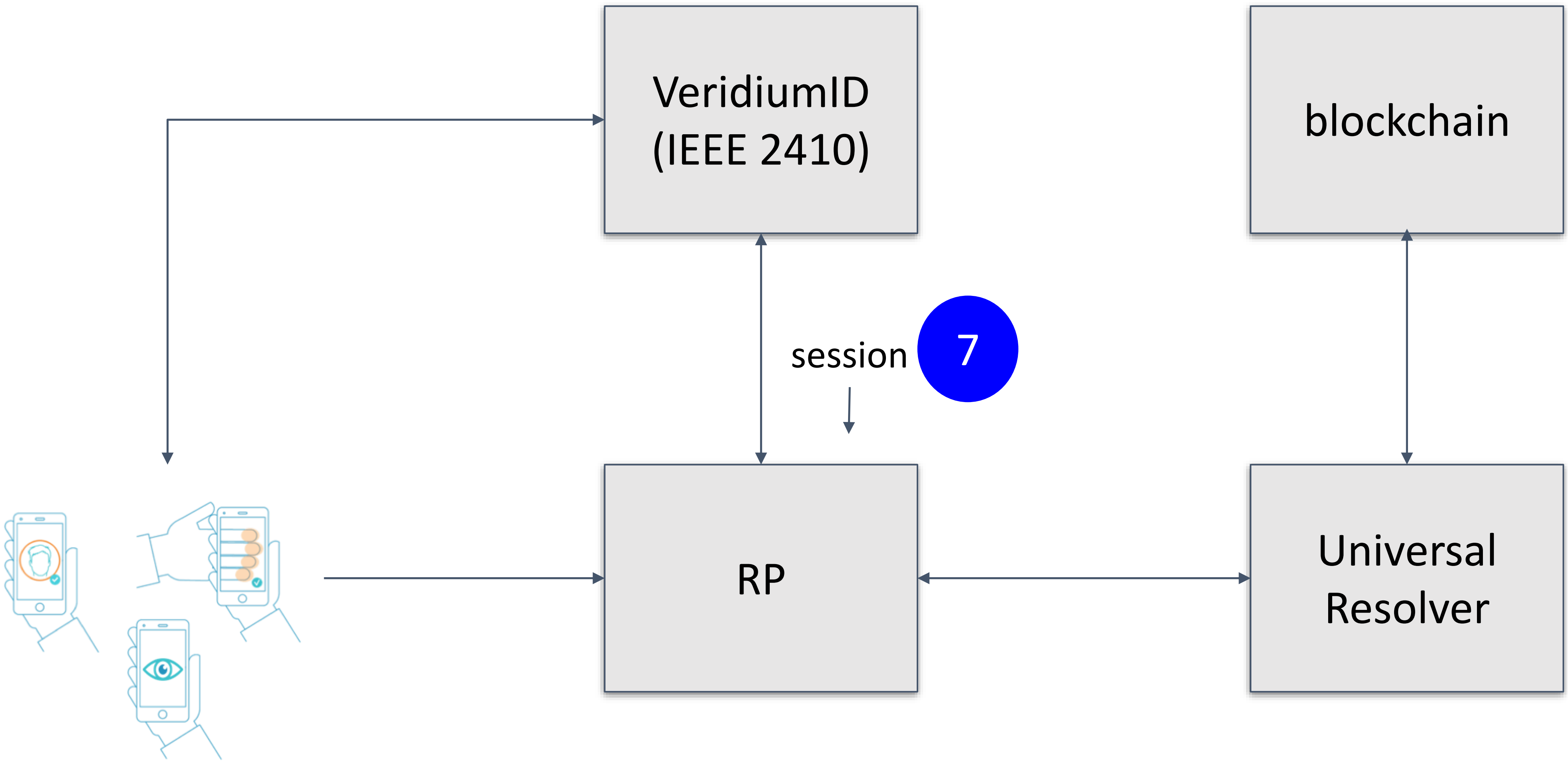
Authentication



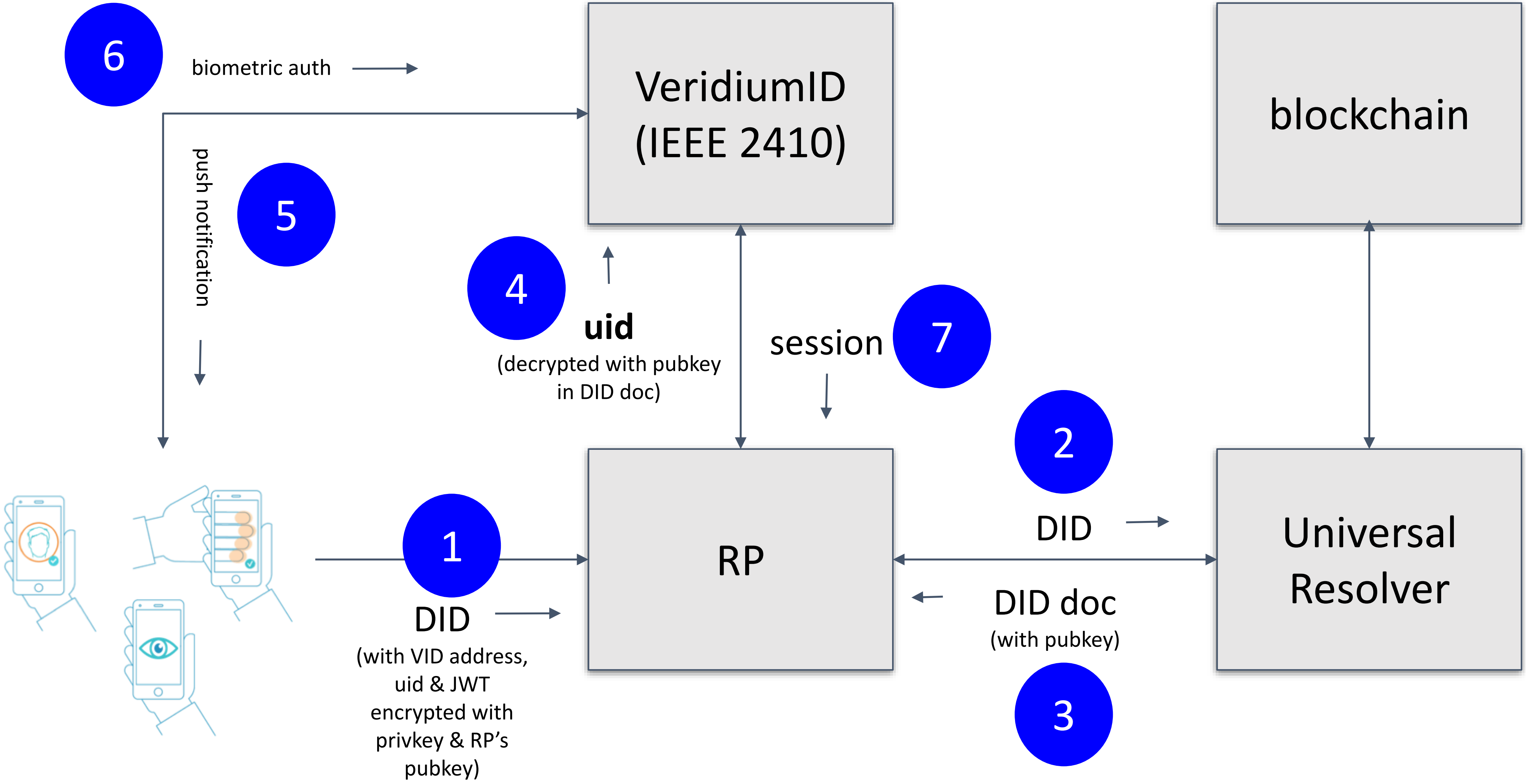
Authentication

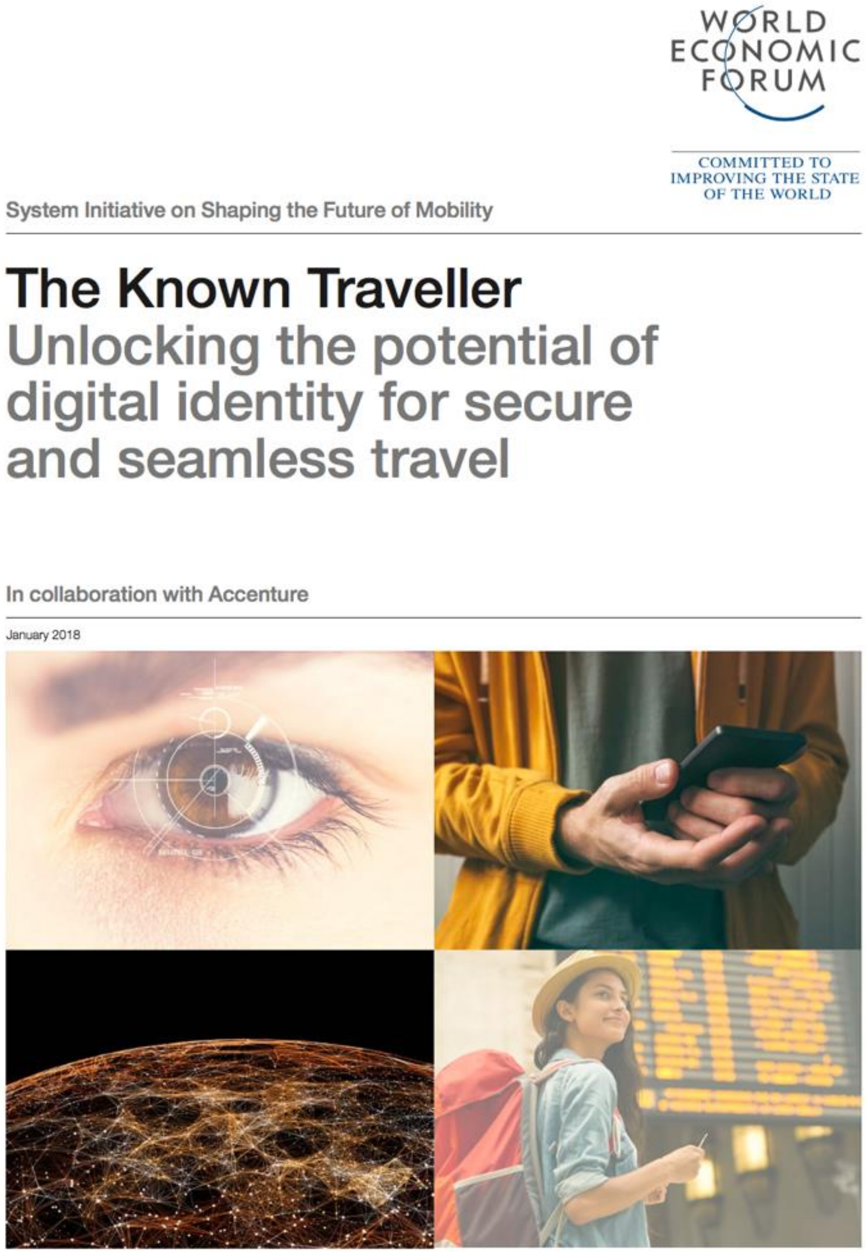


Authentication



Authentication


6
biometric auth →
push notification
5
VeridiumID (IEEE 2410)
blockchain
4
uid
(decrypted with pubkey in DID doc)
session
7
2
DID →
1
RP
Universal Resolver
DID →
(with VID address, uid & JWT encrypted with privkey & RP's pubkey)
← DID doc
(with pubkey)
3



WORLD ECONOMIC FORUM

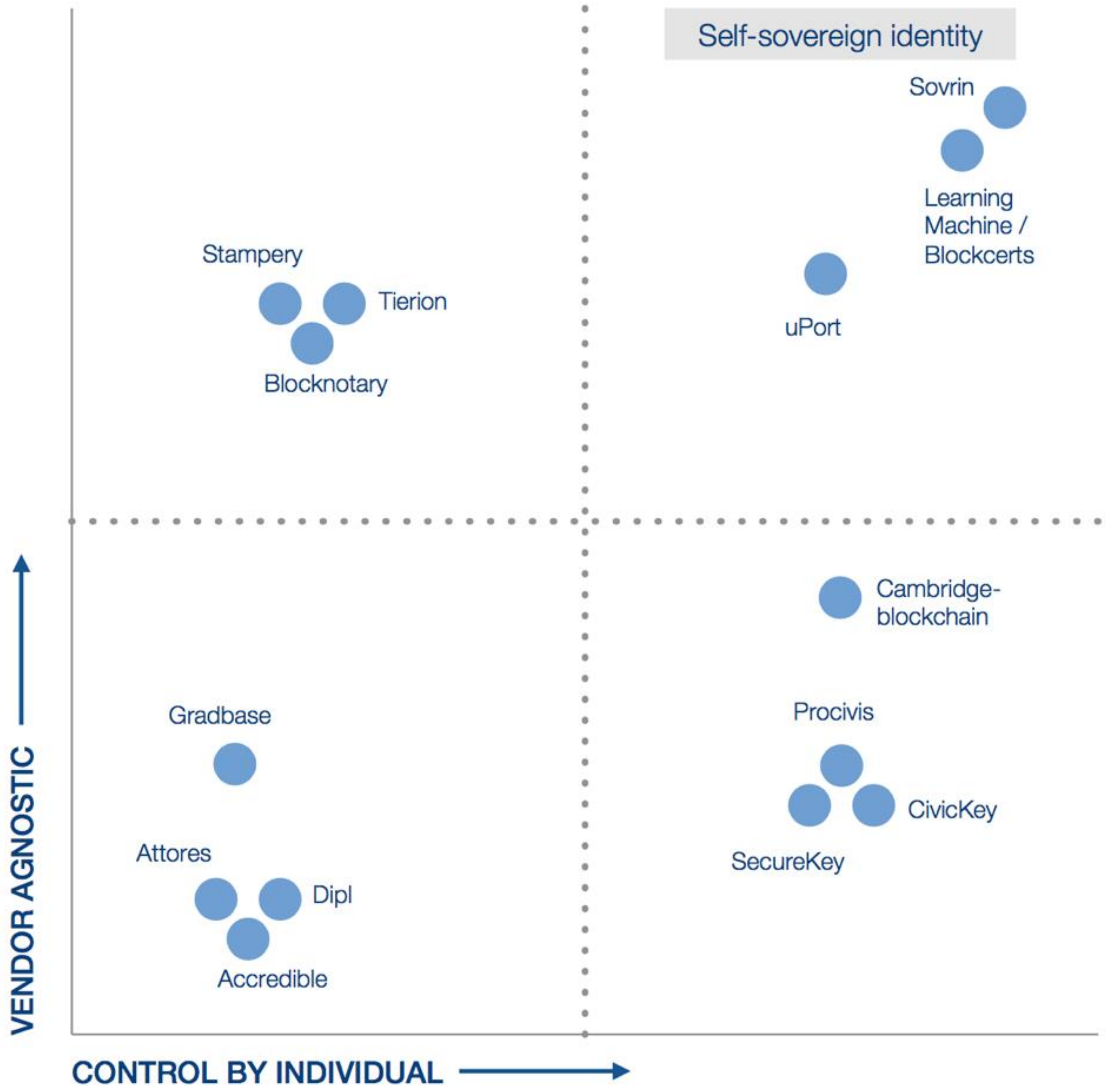
COMMITTED TO IMPROVING THE STATE OF THE WORLD

System Initiative on Shaping the Future of Mobility

The Known Traveller
Unlocking the potential of digital identity for secure and seamless travel

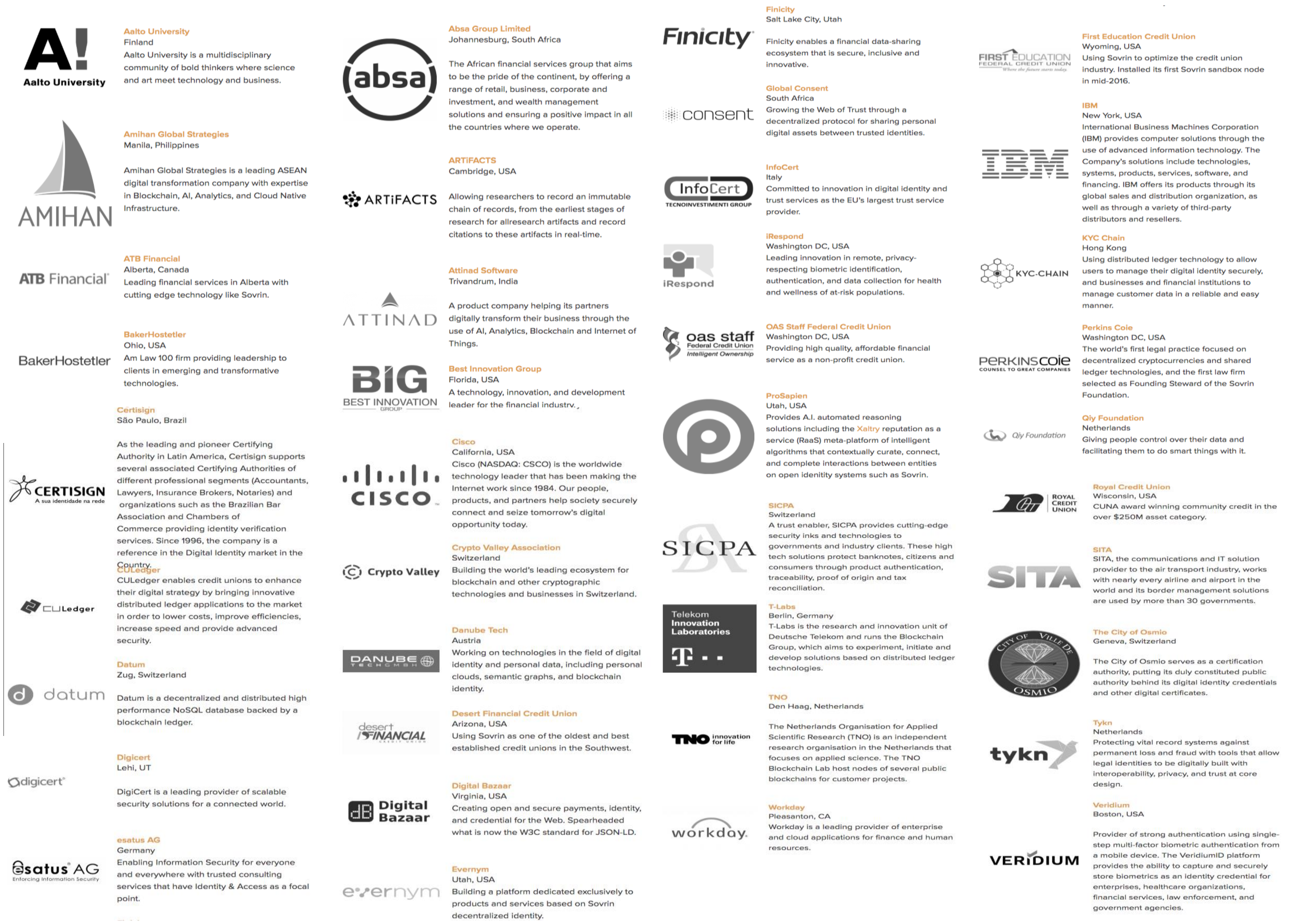
In collaboration with Accenture

January 2018



sovrin

Stewards



Aalto University
Finland
Aalto University is a multidisciplinary community of bold thinkers where science and art meet technology and business.

Amihan Global Strategies
Manila, Philippines

Amihan Global Strategies is a leading ASEAN digital transformation company with expertise in Blockchain, AI, Analytics, and Cloud Native Infrastructure.

ATB Financial
Alberta, Canada
Leading financial services in Alberta with cutting edge technology like Sovrin.

BakerHostetler
Ohio, USA
Am Law 100 firm providing leadership to clients in emerging and transformative technologies.

Certisign
São Paulo, Brazil

As the leading and pioneer Certifying Authority in Latin America, Certisign supports several associated Certifying Authorities of different professional segments (Accountants, Lawyers, Insurance Brokers, Notaries) and organizations such as the Brazilian Bar Association and Chambers of Commerce providing identity verification services. Since 1996, the company is a reference in the Digital Identity market in the Country.

CULedger
CULedger enables credit unions to enhance their digital strategy by bringing innovative distributed ledger applications to the market in order to lower costs, improve efficiencies, increase speed and provide advanced security.

Datum
Zug, Switzerland

Datum is a decentralized and distributed high performance NoSQL database backed by a blockchain ledger.

Digicert
Lehi, UT

DigiCert is a leading provider of scalable security solutions for a connected world.

esatus AG
Germany
Enabling Information Security for everyone and everywhere with trusted consulting services that have Identity & Access as a focal point.

Absa Group Limited
Johannesburg, South Africa

The African financial services group that aims to be the pride of the continent, by offering a range of retail, business, corporate and investment, and wealth management solutions and ensuring a positive impact in all the countries where we operate.

ARTiFACTS
Cambridge, USA

Allowing researchers to record an immutable chain of records, from the earliest stages of research for allresearch artifacts and record citations to these artifacts in real-time.

Attinad Software
Trivandrum, India

A product company helping its partners digitally transform their business through the use of AI, Analytics, Blockchain and Internet of Things.

Best Innovation Group
Florida, USA
A technology, innovation, and development leader for the financial industry.

Cisco
California, USA
Cisco (NASDAQ: CSCO) is the worldwide technology leader that has been making the Internet work since 1984. Our people, products, and partners help society securely connect and seize tomorrow's digital opportunity today.

Crypto Valley Association
Switzerland
Building the world's leading ecosystem for blockchain and other cryptographic technologies and businesses in Switzerland.

Danube Tech
Austria
Working on technologies in the field of digital identity and personal data, including personal clouds, semantic graphs, and blockchain identity.

Desert Financial Credit Union
Arizona, USA
Using Sovrin as one of the oldest and best established credit unions in the Southwest.

Digital Bazaar
Virginia, USA
Creating open and secure payments, identity, and credential for the Web. Spearheaded what is now the W3C standard for JSON-LD.

Evernym
Utah, USA
Building a platform dedicated exclusively to products and services based on Sovrin decentralized identity.

Finicity
Salt Lake City, Utah

Finicity enables a financial data-sharing ecosystem that is secure, inclusive and innovative.

Global Consent
South Africa
Growing the Web of Trust through a decentralized protocol for sharing personal digital assets between trusted identities.

InfoCert
Italy
Committed to innovation in digital identity and trust services as the EU's largest trust service provider.

iRespond
Washington DC, USA
Leading innovation in remote, privacy-respecting biometric identification, authentication, and data collection for health and wellness of at-risk populations.

OAS Staff Federal Credit Union
Washington DC, USA
Providing high quality, affordable financial service as a non-profit credit union.

ProSapien
Utah, USA
Provides A.I. automated reasoning solutions including the Xaltry reputation as a service (RaaS) meta-platform of intelligent algorithms that contextually curate, connect, and complete interactions between entities on open idenitity systems such as Sovrin.

SICPA
Switzerland
A trust enabler, SICPA provides cutting-edge security inks and technologies to governments and industry clients. These high tech solutions protect banknotes, citizens and consumers through product authentication, traceability, proof of origin and tax reconciliation.

T-Labs
Berlin, Germany
T-Labs is the research and innovation unit of Deutsche Telekom and runs the Blockchain Group, which aims to experiment, initiate and develop solutions based on distributed ledger technologies.

TNO
Den Haag, Netherlands

The Netherlands Organisation for Applied Scientific Research (TNO) is an independent research organisation in the Netherlands that focuses on applied science. The TNO Blockchain Lab host nodes of several public blockchains for customer projects.

Workday
Pleasanton, CA
Workday is a leading provider of enterprise and cloud applications for finance and human resources.

First Education Credit Union
Wyoming, USA
Using Sovrin to optimize the credit union industry. Installed its first Sovrin sandbox node in mid-2016.

IBM
New York, USA
International Business Machines Corporation (IBM) provides computer solutions through the use of advanced information technology. The Company's solutions include technologies, systems, products, services, software, and financing. IBM offers its products through its global sales and distribution organization, as well as through a variety of third-party distributors and resellers.

KYC Chain
Hong Kong
Using distributed ledger technology to allow users to manage their digital identity securely, and businesses and financial institutions to manage customer data in a reliable and easy manner.

Perkins Coie
Washington DC, USA
The world's first legal practice focused on decentralized cryptocurrencies and shared ledger technologies, and the first law firm selected as Founding Steward of the Sovrin Foundation.

Qiy Foundation
Netherlands
Giving people control over their data and facilitating them to do smart things with it.

Royal Credit Union
Wisconsin, USA
CUNA award winning community credit in the over $250M asset category.

SITA
SITA, the communications and IT solution provider to the air transport industry, works with nearly every airline and airport in the world and its border management solutions are used by more than 30 governments.

The City of Osmio
Geneva, Switzerland

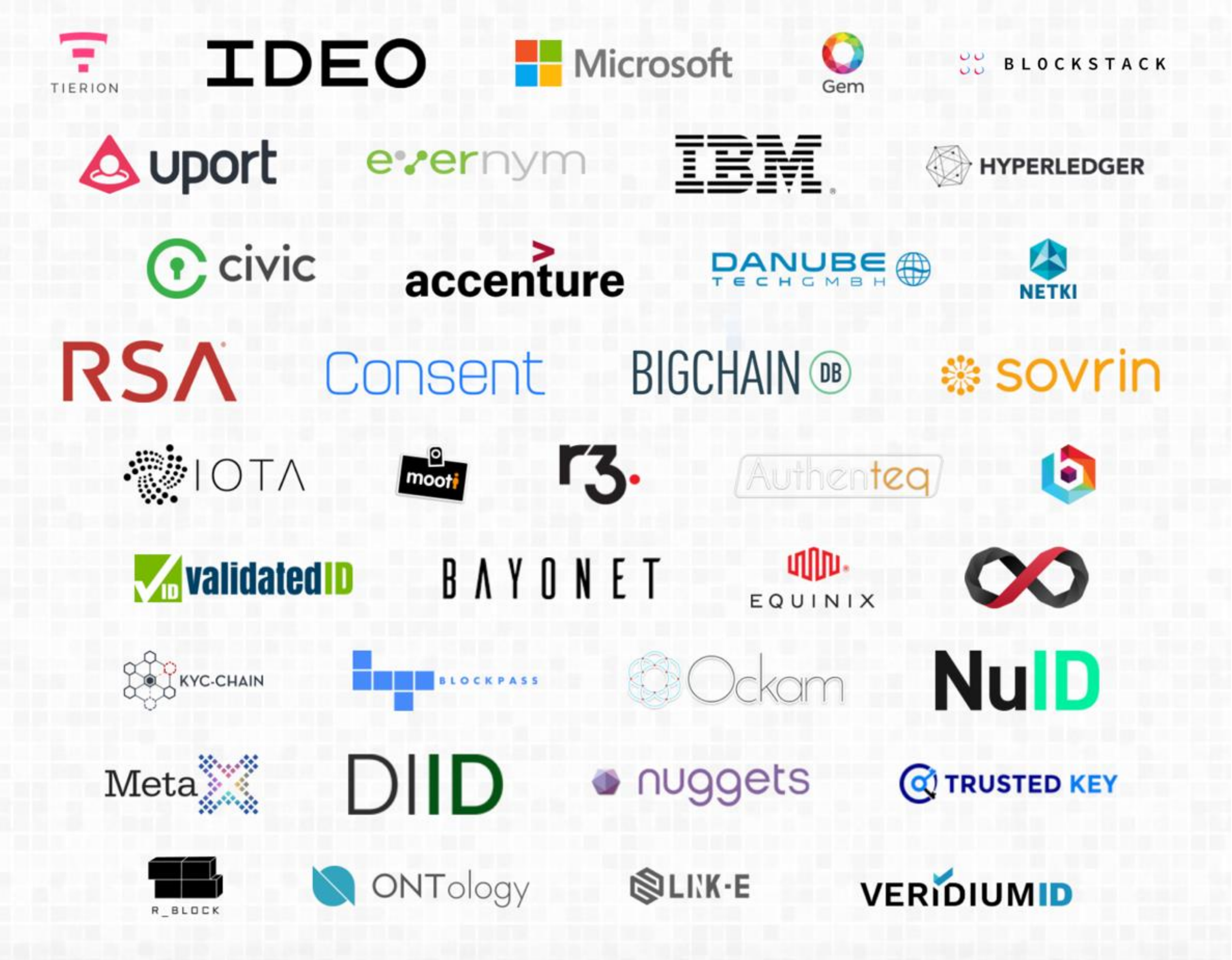
The City of Osmio serves as a certification authority, putting its duly constituted public authority behind its digital identity credentials and other digital certificates.

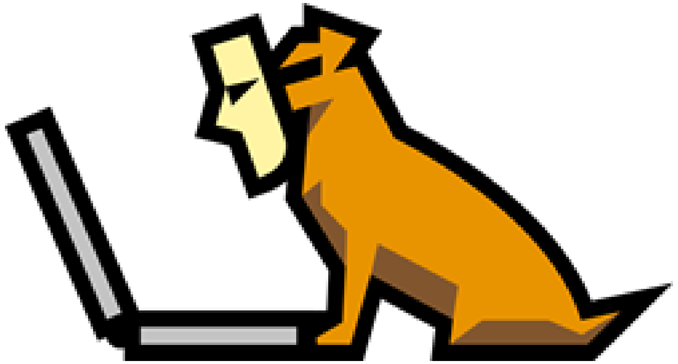
Tykn
Netherlands
Protecting vital record systems against permanent loss and fraud with tools that allow legal identities to be digitally built with interoperability, privacy, and trust at core design.

Veridium
Boston, USA

Provider of strong authentication using single-step multi-factor biometric authentication from a mobile device. The VeridiumID platform provides the ability to capture and securely store biometrics as an identity credential for enterprises, healthcare organizations, financial services, law enforcement, and government agencies.

DIF


TIERION
IDEO
Microsoft
Gem
BLOCKSTACK
uport
evernym
IBM
HYPERLEDGER
civic
accenture
DANUBE TECH GMBH
NETKI
RSA
Consent
BIGCHAIN DB
sovrin
IOTA
mooti
r3.
Authenteq
ID validatedID
BAYONET
EQUINIX
KYC-CHAIN
BLOCKPASS
Ockam
NuID
MetaX
DIID
nuggets
TRUSTED KEY
R_BLOCK
ONTology
LINK-E
VERIDIUMID



Internet Identity Workshop

IIW 27 23-25 October 2018
Computer History Museum
Mountain View, CA

Microsoft Conference Dinner	Google	WIRELINE Tuesday Dinner
vmware Barista	CULedger Projectors	aws Power and Tables
sovrin Premiere Lunch	IEEE Lunch	IBM Tuesday Reception
WIRELINE Demo Hour	digi.me Tech Fair	evernym Breakfast
VERIDIUM HANDS ON SECURITY Gifting	((IBO)) Gifting	