



On a mission to establish trust in the communications industry.

Digital Identity: What Is It Good For?

Enabling Trustworthy Communications
Across Applications and Networks



Pierce Gorman

DISTINGUISHED MEMBER
OF THE TECHNICAL STAFF

Telecom leader with 10+ years shaping industry standards, network architecture, and technology deployment.

Former Systems Architecture Engineer specializing in VoIP and STIR/SHAKEN, active amongst ATIS, FCC NANC CATA, STI-GA, CTIA, USTA, NTCA, NICC, One Consortium, and IETF working groups.

01

Introduction & Call to Action

What is Digital Identity? Why is it an important topic?

02

STIR/SHAKEN

The Good, The Bad, & The Better

03

STIR/SHAKEN Tutorial

Illustrating Conventional Digital Identity

04

The World of Digital Identity Credential Types

05

Global Digital Identity Initiatives

Digital Identity

What is it good for and why should we care?

Like SIP trunks, there's no standard definition for **Digital Identity**

- “Good” Digital Identity requires encoding the results of “good” KYC/KYX, secured with flexible but reliable Trust Frameworks
- Where there is “good” Digital Identity, fraudsters can't hide (the converse is true too)
- Better to promote and protect well-identified communications than to label and traceback to punish perpetrators (But do both. Trust, but **verify**)

I assert,

“Digital Identity is the set of identifiers, attributes, & cryptographic bindings that reliably represent a Subject (person, organization, device, or software agent) in electronic communications.”

Digital Identity

What is it good for and why should we care?

Domains of Identity by Kaliya Young

- **Government:** Birth Certificate (issued to custodian), Licenses
- **Civil Society:** Industry Associations, Unions, State Medical, & Legal Boards
- **Commercial:** Account, Warranties, Discounts, Contracts
- **Employment:** Roles, Authorizations

Activities are Registrations, Transactions, Surveillance

Important Digital Identity Standards Development Organizations

CA/B Forum

Vendor root programs govern public-web PKI.

W3C

Defines the data models (Verifiable Credentials) and web APIs (WebAuthn) that many ecosystems build on.

OpenID + IETF

Provide the protocol plumbing (OAuth-based issuance & presentation, JWT/JOSE crypto, SD-JWT selective disclosure).

ISO/IEC & ICAO

Standardize government-grade credentials (mDL/mDOC, passports).

ETSI/CEN

Align with eIDAS (EU trust services, qualified certs/QSCD).

A Selection of Digital Identity SDO Milestones

9-15-2006	ICAO Doc 9303 (6 th ed.) ePassports baseline. ICAO+1
7-23-2014	EU eIDAS Reg. 910/2014 adopted. EUR-LexElgar Online
7-1-2016	eIDAS provisions begin taking effect
3-4-2019	W3C WebAuthn Level 1 becomes Recommendation. W3C
9-15-2021	ISO/IEC 18013-5 mDL published. ISO+1
5-20-2024	eIDAS 2.0 (Reg. 2024/1183) enters into force
10-7-2024	ISO/IEC TS 18013-7 (mDL over the Internet) 1st ed. (suspended in 2025) AAMVA
4-8-2025	W3C WebAuthn Level 2 (reference milestone). W3C
5-15-2025	W3C VC Data Model 2.0 becomes Recommendations (family of 7 Recs). W3C +2W3C+2
6-23-2025	OID4VP Final Specification public review window closes (path to Final). OpenID Foundation
7-9-2025	OID4VP 1.0 final text proposed. OpenID Foundation
5-29-2025	ISO/IEC TS 18013-7:2025 (revised edition) published
529-2025	IETF SD-JWT in RFC Editor queue (precursor to SD-JWT VC)

STIR/SHAKEN

The Good, The Bad, & The Better

THE GOOD

- Proven foundation for authenticated SIP Signaling at scale
- May someday successfully inhibit number spoofing and illegal robocalls

THE BAD

- Has not materially decreased illegal robocalls (for various reasons)
- The only identity authenticated is that of the service provider that signed the STIR PASSporT

THE BETTER

- Authenticate the caller using **Digital Identity** credentials of the caller (not their service provider)
- **Mutual Authentication** using Digital Identity credentials in a “wallet”


STIR/SHAKEN

Digital Identity Illustrated

STIR: A collection of IETF standards defining:

- SIP IDENTITY Header
- Personal ASsertion Token (PASSporT)
- PASSporT extensions such as “shaken”, “div”, “RCD”, “RPH”
- Secure Telephone Identity (STI) X.509 certificate extensions

SHAKEN: A collection of ATIS/SIP Forum standards defining how to use SIP IDENTITY headers, PASSporTs of various extensions, & the STI X.509 certificate Public Key Infrastructure (PKI) trust framework managing issuance and use of X.509 certs with STI extensions.



SITR/SHAKEN
Authenticates a call
signaled using SIP
(or Out-of-Band)

STIR/SHAKEN: Digital Identity Illustrated

SIP Identity Header

```
INVITE sip:18001234567@example.com:5060 SIP/2.0
Via: SIP/2.0/UDP example.com:5060
From: "Alice" <sip:14045266060@5.6.7.8:5060>;tag=123456789
To: "Bob" <sip:18001234567@1.2.3.4:5060>
Call-ID: 1-12345@5.6.7.8
CSeq: 1 INVITE
Max-Forwards: 70
Identity:
eyJhbGciOiJFUzI1NiIsInBwdCI6InNoYWtlbGlzInR5cCI6InBhc3Nwb3J0IiwieD
VlIjoiaHR0cHM6Ly9jZXJ0aWZpY2F0ZXMuZXhhbXBsZS5jb20vMTIzNDU2Nz
g5LnB1bS99eyJhdHRlc3QiOiJBlwiZGVzdCI6eyJ0bil6WyIxODAwMTIzNDU2
NyJdfSwiaWF0IjoxNTQ4ODU5OTgyLCJvcmlhIjpw7InRuljoiMTQwNDUyNjYw
NjAifSwib3JpZ2lkIjoiaM2E0N2NhMjMtZDdhYi00NDZiLTgyMWQzMzNkNWRI
ZWRiZWQ0In0iS_vqkgCk88ee9rtk89P6a6ru0ncDfSrd1GyK_mJj-10hsLW-
dMF7eCjDYARLR7EZSZwiu0fd4H_QD_9Z5U2bg;info=<https://certificates.ex
ample.com/123456789.pem>alg=ES256;ppt=shaken
```

Base64 Encoding Of
"SHAKEN" PASSport JSON
Web Token (JWT)

IETF RFC 8224

SIP Identity Header "Info"
Parameter

STIR/SHAKEN: Digital Identity Illustrated

“SHAKEN” PASSporT JSON Web Token (JWT)

Header

```
{  
  "alg": "ES256",  
  "ppt": "shaken",  
  "typ": "passport",  
  "x5u": https://certificates.example.com/123456789.pem  
}
```

Payload

```
{  
  "attest": "A",  
  "dest": {  
    "tn": [  
      "18001234567"  
    ]  
  },  
  "iat": 1548859982,  
  "orig": {  
    "tn": "14045266060"  
  },  
  "origid": "3a47ca23-d7ab-446b-821d-33d5deedbed4"  
}
```

“I, the SP, attest I have a relationship with the caller, and they have RTU orig TN”

Called #

Calling #

Signature (not shown)

STIR/SHAKEN: Digital Identity Illustrated

STI X.509 Certificate

-----BEGIN CERTIFICATE-----

MIIC5jCCAougAwIBAgIQUXLKloq4jcYv9SEMioYeGDAKBggqhkJOPQQDAjBnMQSwCQYDVQQGEwJVUzEZMBCGA1UEChMQVHJhbnNOZXh1cywgSW5jLjEPMAOGA1UECXMGU0hBS0VOMSwWkgYDVQQDEYNuUcmFuc05leHVzLCBjb2MwIFNlbnVtFTIBjC3N1aW5nIENBMzAeFw0yMjA1MTcxODQzMjZaFw0yMjExMTMxODQzMjVhMEIxZzAJBgNVBAYTAiVMTQwwCgYDVQQKEWNBVFQxZDZANBgNVBAStBINlbnVtFTJtEUMBIGA1UEAxMLU0hBS0VOIDQwMzYwWTATBgcqhkJOPQIBBggqhkJOPQMBBwNCAAS6jZAWuqTTTNihx3HwoCLW+FyYQNnRtKwZj00mCnolHLFMe7+NGJkD4D37mWsF4WxpjuZbvZn/dqQwyhscs7Q8o4IBPDCCATgwDAYDVR0TAQH/BAIwADAOBgNVHQ8BAf8EBAMCAIAwHQYDVR0OBBYEFet5bm34mhAlpWU0oOxs19nm6kasMB8GA1UdIwQYMBaAFLuW3jESzdOWmYSkNjBgPNdSgX0nMBcGA1UdIAQQMA4wDAYKYIZIAYb/CQEBAzCBpgYDVR0fBIGeMIGbMIGYoDqgOIY2aHR0cHM6Ly9hdXRoZW50aWNhdGutYXBpLmljb25lY3Rpdj5jb20vZG93bmXvYWQvdjEvY3JsolqkWDBWMRQwEgYDVQQHDAUcCmlkZ2V3YXRlcjELMAkGA1UECAwCTkoxEzARBgNVBAMMCINUSStQQSBdUkwxCzAJBgNVBAYTAiVMTQ8wDQYDVQQKDAZTVEktUEEwFgYIKwYBBQUHARoECjAloAYWBdQwMzYwCgYIKoZlZj0EAWIDSQAwwRglhAJGjH1RltjZwCQG566kpy9VB9uoiwn2trtDFflTCvfxAiEApyPhmJzrnOaLLYziBYOVb7ygkgOb97ujfqmFEjOgvrC=

-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----

MIIC8TCCApigAwIBAgIQaeMkSbXPfDSFEKC20T6VZTAKBgqhkJOPQQDAjBkMQswCQYDVQQGEwJVUzEZMBcGA1UEChMQVHJhbnNOZXh1cywgSW5jLjEPMA0GA1UECzMGU0hBS0VOMSkwJwYDVQQDEyBUcmFuc05leHVzLCBjb250IENBMTAeFw0yMTA4MjAwMDAwMDBaFw0zMTA4MTkyMzU5NTIaMGcxCzAJBgNVBAYTAiVTMRkwFwYDVQQKEyBUcmFuc05leHVzLCBjb250MQ8wDQYDVQQLEwZTSEFLRU4xLDAqBgNVBAMTIIRyYW5zTmV4dXMsIEluYy4gU0hBS0VOIElzc3VpbmcgQ0EzMFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAEedxAVLKoKQD8g8QPsb9EqRyITRIDarijlRVn1QsXV3Oh7H5HsWihLITqgbnVM7zF/nXicWwV/kkgvIKOfmCpW6OCAScwgEjMA8GA1UdEwEB/wQFMAMBAf8wDgYDVR0PAQH/BAQDAgAGMB0GA1UdDgQWBBS7lt4xEs3TlpmEpDYwYDZlXUoF9JzAfBgNVHSMEGDAWgBSajEoZn2TEXjO2KYwWyqe4EEsuWzAXBgNVHSAEEDAOMAAGCmCGSAGG/wkBAQMwgaYGA1UdHwSBnjCBmzCBmKA6oDiGNmh0dHBzOi8vYXV0aGVudGljYXRILWFwaS5pY29uZW50aXYuY29tL2Rvd25sb2FkL3YxL2NybkKJapFgwVjEUMBIGA1UEBwwLQnJpZGldd2F0ZXIxZCzAJBgNVBAGMAk5KMRMwEQYDVQQDDApTVEktUEEgQlJMMQswCQYDVQQGEwJVUzEPMA0GA1UECgwGU1RjLVBBMAoGCCqGSM49BAMCA0cAMEQCIGgZROhV4BF/KGMwnKGbSUJ0VMdMavpgljSifXhtc7B3AiA6ODY5dkKtrUbywLLH+ZJX1UnDad6FZwwQVQpUD0oZHA==

-----END CERTIFICATE-----

STIR/SHAKEN: Digital Identity Illustrated

STI X.509 End Entity Certificate

Certificate:

Data:

Signature Algorithm: ecdsa-with-SHA256

Issuer: C=US, O=TransNexus, Inc., OU=SHAKEN, CN=TransNexus, Inc. SHAKEN Issuing CA3

Subject: C=US, O=ATT, OU=SHAKEN, CN=SHAKEN 4036

X509v3 extensions:

X509v3 Basic Constraints: critical

CA:FALSE

X509v3 Key Usage: critical

Digital Signature

X509v3 CRL Distribution Points:

Full Name:

URI:https://authenticate-api.iconectiv.com/download/v1/crl

CRL Issuer:

DirName:L = Bridgewater, ST = NJ, CN = STI-PA CRL, C = US,
O = STI-PA

1.3.6.1.5.5.7.1.26:

0.....4036

TNAuthList OID

Certificate:

Data:

Version: 3 (0x2)

Serial Number:

51:72:ca:22:8a:b8:8d:c6:2f:f5:21:0c:8a:86:1e:18

Signature Algorithm: ecdsa-with-SHA256

Issuer: C=US, O=TransNexus, Inc., OU=SHAKEN, CN=TransNexus, Inc. SHAKEN

Issuing CA3

Validity

Not Before: May 17 18:47:26 2022 GMT

Not After : Nov 13 18:47:25 2022 GMT

Subject: C=US, O=ATT, OU=SHAKEN, CN=SHAKEN 4036

Subject Public Key Info:

Public Key Algorithm: id-ecPublicKey

Public-Key: (256 bit)

pub:

04:ba:8d:90:16:ba:a4:d3:4c:d8:a1:c7:71:f0:a0:

22:d6:f8:5c:98:40:d9:d1:b4:ac:19:8f:4d:26:0a:

7a:25:1c:b1:4c:7b:bf:8d:18:99:03:e0:3d:fb:99:

6b:05:e1:6c:69:8e:e6:5b:bd:99:ff:76:a4:30:ca:

1b:1c:b3:b4:3c

ASN1 OID: prime256v1

NIST CURVE: P-256

X509v3 extensions:

X509v3 Basic Constraints: critical

CA:FALSE

X509v3 Key Usage: critical

Digital Signature

X509v3 Subject Key Identifier:

4B:79:6E:6D:F8:9A:10:08:A5:65:34:A0:EC:6C:D7:D9:E6:EA:46:AC

X509v3 Authority Key Identifier:

BB:96:DE:31:12:CD:D3:96:99:84:A4:36:30:60:3C:D7:52:81:7D:27

X509v3 Certificate Policies:

Policy: 2.16.840.1.114569.1.1.3

X509v3 CRL Distribution Points:

Full Name:

URI:https://authenticate-api.iconectiv.com/download/v1/crl

CRL

Issuer:

DirName:L = Bridgewater, ST = NJ, CN = STI-PA CRL, C = US, O = STI-PA

1.3.6.1.5.5.7.1.26:

0.....4036

Signature Algorithm: ecdsa-with-SHA256

Signature Value:

30:46:02:21:00:91:a3:1f:54:48:b6:3c:d9:59:c4:06:e7:ae:

a4:a7:2f:55:07:db:a8:8b:09:f6:b6:bb:43:15:f9:53:0a:f7:

d7:02:21:00:a7:23:e1:98:9c:eb:9c:e6:8b:2d:8c:e2:05:83:

95:6f:bc:a0:92:a3:9b:f7:bb:a3:7e:a9:85:12:33:a0:be:b7

OpenSSL versions:

Library: OpenSSL 3.2.2 4 Jun 2024

Command Line: OpenSSL 3.0.2 15 Mar 2022 (Library: OpenSSL 3.0.2 15 Mar 2022))

The Wide World of Digital Identity Credentials

ISO (& IETF)
X.509

W3C Verifiable
Credentials

GLEIF LEI &
Verifiable LEI
(vLEI)

ISO 18013-5/7
Mobile Driver's
License (mDL) &
mDOCs

The World of Digital Identity Credentials

ISO (& IETF) X.509



Main use **globally** is for the purpose of SSL/TLS connection to web pages.

Web certs are issued by Certification Authorities (CAs) using various entity verification processes




- Domain Validation (DV)
- Organization Validation (OV)
- Extended Validation (EV)

Accreditation via **“Root Programs”**

- Mozilla Root Program (used by Firefox, also forms baseline policy for many others)
- Microsoft Trusted Root Program (Windows, Edge, et al)
- Apple Root Program (macOS, iOS, Safari)
- Google Chrome Root Program (since 2022, separate from Android)

The World of Digital Identity Credentials — X.509

The **Trust Mark** (grey padlock) is the same **regardless** of the validation method

Type	What CA Verifies	Certificate Fields	Issuance Speed / Cost	Browser Trust Mark	Use Cases
Domain Validation (DV)	Only domain control (DNS/email/HTTP)	Subject: domain (CN).	Minutes / low or free.	Gray padlock 	Blogs, personal sites, test servers.
Organization Validation (OV)	Domain + org's legal existence (registry, address, phone).	Subject: domain (CN) + Organization (O), Locality (L), Country (C).	1–3 days / moderate cost.	Gray padlock  (org details only in cert viewer).	Business websites, enterprise portals.
Extended Validation (EV)	Domain + strict vetting of legal entity, physical & operational existence, requester's authority.	Subject: CN + full org details + EV policy OID.	Days–weeks / highest cost.	Gray padlock  (no distinct green bar anymore).	Banks, governments, major e-commerce.

The World of Digital Identity Credentials

World Wide Web Consortium (W3C) Verifiable Credentials (VCs)



W3C Verifiable
Credentials

ChatGPT Prompt:

*“Describe W3C VCs as
though to 3rd grade
students.”*

World Wide Web Consortium

Think of W3C as a big team of librarians & teachers for the internet. Their job is to **make the rules** for the websites, apps, & computers to play together.

Verifiable Credentials

Think of VCs as **digital permission slips or ID cards**, like a library card, a student ID, or a report card. A VC is the same idea, but lives on your mobile device or app instead of paper.

A teacher could give you a digital gold star badge which says, “You finished your reading homework,” and you could show that badge to another teacher, or your parents, and they could easily check that it isn’t a fake badge you drew yourself.

- Easy to share (using your phone)
- Hard to fake (computer math called “cryptography”)
- You get to choose who can see them (like deciding who to show your report card to)

The World of Digital Identity Credentials

W3C Verifiable Credentials



W3C Verifiable
Credentials

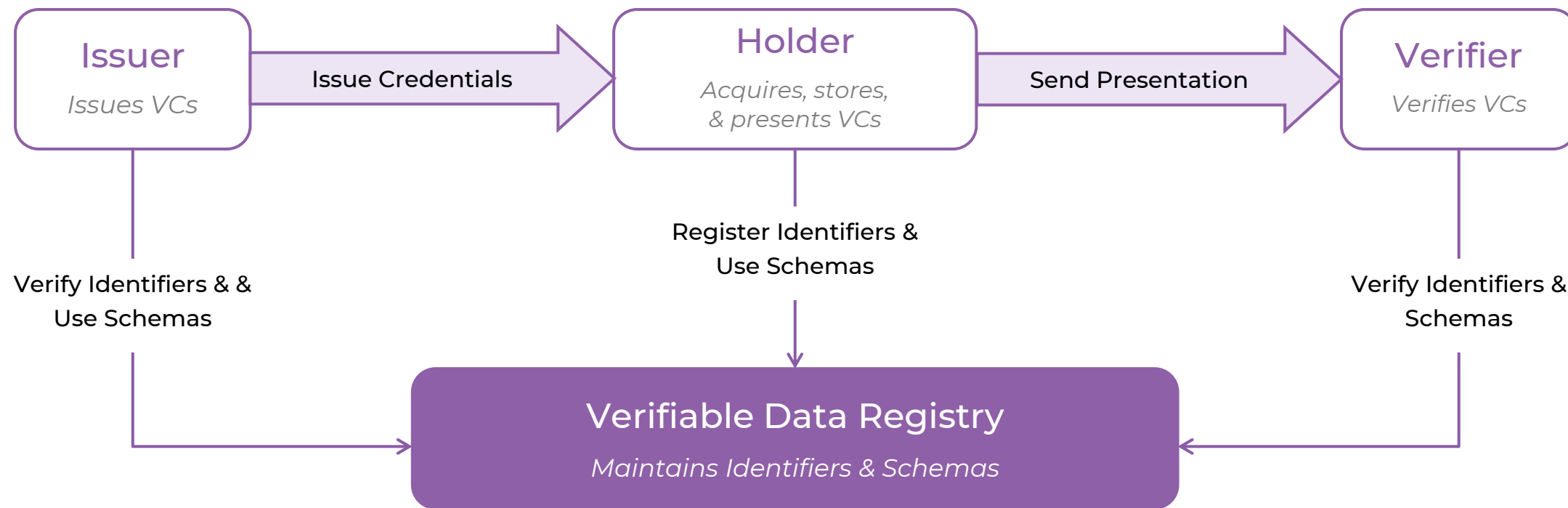
W3C Verifiable Credentials
align well with concepts of
Self-Sovereign Identity (SSI)

Christopher Allen's 10 Principles of SSI

Existence	Users exist independently of systems
Portability	Identities move between systems
Control	Users control their identity
Interoperability	Identities should be widely usable
Access	Users can access their data
Consent	User chooses what to share
Transparency	Systems are understandable and open
Minimalization	Only necessary data is shared
Persistence	Identity lasts over time
Protection	Identity rights are safeguarded

The World of Digital Identity Credentials

W3C Verifiable Credentials



The World of Digital Identity Credentials

W3C Verifiable Credentials

ISSUERS VCs



PUBLIC

Registrations, Licenses, Etc.



PRIVATE

Insurance Policies, FICO Score
Coupons, Receipts, Etc.



PERSON

Contact Cards, Prescriptions,
& Authorizations

WALLETS (HOLDERS)



PERSONAL



ORGANIZATIONAL

VERIFIERS



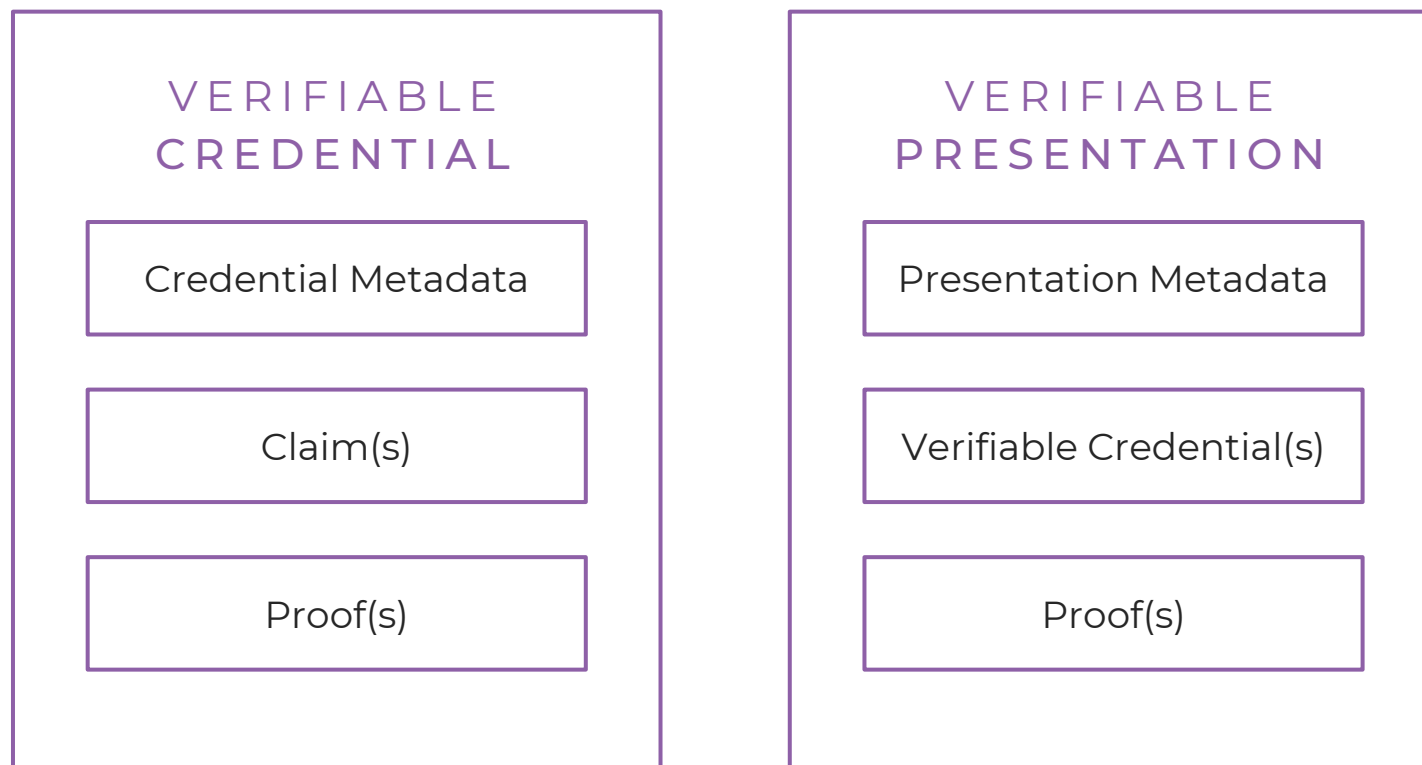
PERSON



APPLICATION

The World of Digital Identity Credentials

W3C Verifiable Credentials



The World of Digital Identity Credentials

METADATA

CLAIMS

W3C Verifiable Credentials & Verifiable Presentation

Example of a Verifiable Credential (JSON-LD)

```
{
  "@context": [
    "https://www.w3.org/ns/credentials/v2",
    "https://www.w3.org/ns/credentials/examples/v2"
  ],
  "id": "http://university.example/credentials/3732",
  "type": ["VerifiableCredential", "ExampleDegreeCredential"],
  "issuer": "https://university.example/issuers/565049",
  "validFrom": "2010-01-01T00:00:00Z",
  "credentialSubject": {
    "id": "did:web:example.com:ebfeb1f712ebc6flc276e12ec21",
    "degree": {
      "type": "ExampleBachelorDegree",
      "name": "Bachelor of Science and Arts"
    }
  }
}
{Proofs not shown}
```

Example of a Verifiable Presentation (VP-JWT)

```
{
  "alg": "ES256",
  "typ": "JWT",
  "kid": "did:example:org:ACME-LEI-5493001KJTIIGC8Y1R12#keys-1"
}
{
  "iss": "did:example:org:ACME-LEI-5493001KJTIIGC8Y1R12",
  "sub": "did:example:org:ACME-LEI-5493001KJTIIGC8Y1R12",
  "aud": "verifier.example.org",
  "jti": "urn-uuid:3c3e9d27-5c76-4f6b-8b5e-3f3c6a6a2a11",
  "iat": 1756300800,
  "nbf": 1756300800,
  "exp": 1756308000,
  "nonce": "2b793b52-2c98-4de1-bc2a-874a4f72cd91",
  "vp": {
    "@context": [
      "https://www.w3.org/ns/credentials/v2"
    ],
    "type": [
      "VerifiablePresentation"
    ],
    "verifiableCredential": [
      "urn:uuid:1f7b3a2e-2d4c-4a7b-b2a9-6f6e7e8a2fd1"
    ]
  }
}
```

The World of Digital Identity Credentials

GLEIF Verifiable LEIs (vLEIs)



GLEIF is the **Global Legal Entity Identifier Foundation** established by the Financial Stability Board of the G20 after the 2008 global financial crisis.

It maintains a database of registered LEIs: ~2.8M and growing.

LEIs are globally unique Legal Entity Identifiers

ChatGPT Prompt:

"Describe GLEIF, LEIs, & vLEIs as though to 3rd grade students."

- **GLEIF** is like the school office that keeps a list of who is who
- An **LEI** is a company's official name tag number. It is a 20-character ID that says, "This exact company is ACME, not some other ACME."
- A **vLEI** is the same name tag number but as a digital badge you can show on the Internet.

The World of Digital Identity Credentials

GLEIF Verifiable LEIs (vLEIs)

Element & Protocol Components of vLEI Architecture

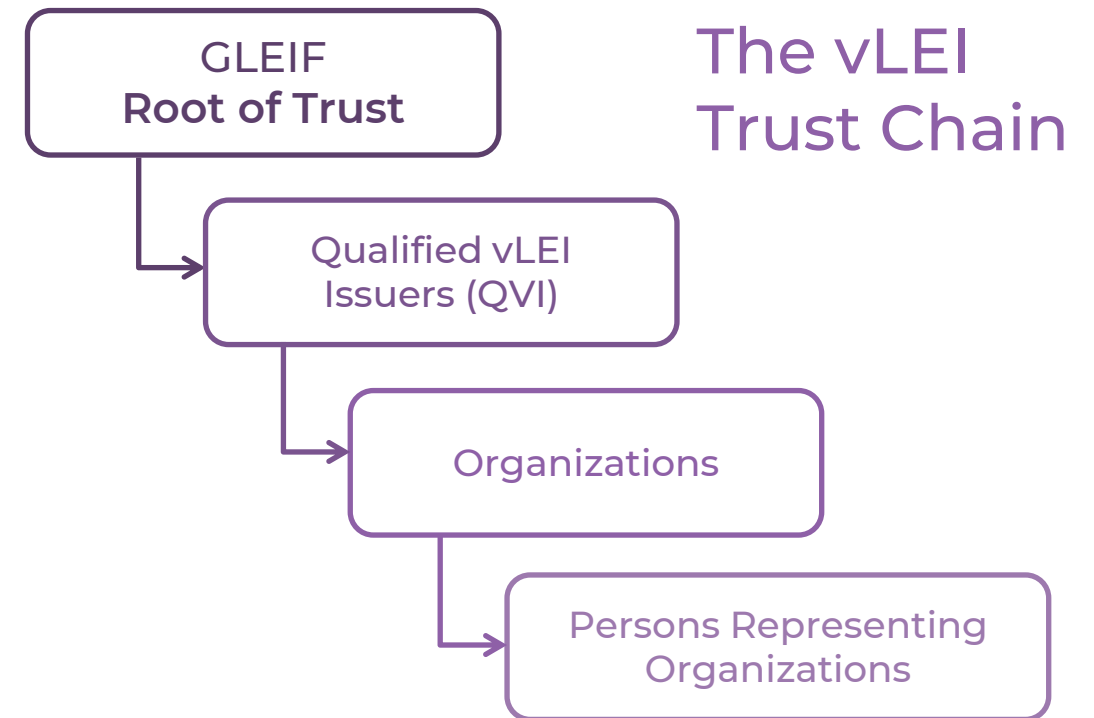
- **KERI** (Key Event Receipt Infrastructure) key event log system
- **ACDC** (Authentic Chained Data Container) variant of W3C VC
- **AID** (Autonomic Identifier) self-certifying ID following KERI protocol
- **CESR** (Composable Event Streaming Representation) similar to CBOR (Concise Binary Object Representation)

The World of Digital Identity Credentials

GLEIF Verifiable LEIs (vLEIs)

- GLEIF is the **Root of Trust**.
- Root **AID** (Autonomic Identifier) to establish the Root of Trust.
- Delegated **AIDs** to issue vLEIs to its trusted network of Qualified **vLEI** Issuers (**QVIs**).
- **QVIs** are qualified to issue Entity & Role vLEI Credentials
- Once a vLEI is issued to an Organization, vLEIs can be issued to Persons who represent Organizations either in official or functional roles.

By combining three concepts – the organization's identity, represented by the LEI, a person's identity and the role that the person plays for the organization, vLEI credentials can be issued.



The World of Digital Identity Credentials

GLEIF Verifiable LEIS (vLEIs)

Example vLEI Authenticated Chained Data Container VC

Generated by ChatGPT




Confidential and Proprietary. ©2025 Numeracle. All Rights Reserved.

```
{
  "v": "ACDC20JSON0001",
  "d": "EFuT9x2l4t7oG7nWg7iYxW3s8Q6c5h2JlKpQmR2aB3C4",
  "i": "did:keri:EFacmeIssuerAID1234567890",
  "s": "EFschemaECRvlabcd efghiJKL",
  "a": {
    "lei": "5493001KJTIIGC8YIR12",
    "entityName": "ACME Trading Corporation",
    "subject": {
      "id": "did:keri:EFpersonAID0987654321",
      "givenName": "Pat",
      "familyName": "Lee"
    },
    "role": {
      "type": "EngagementContextRole",
      "label": "Authorized Representative",
      "authority": "Acts on behalf of ACME within the engagement below"
    },
    "engagement": {
      "id": "urn:uuid:8f9c2f3a-1b62-4d8a-9e57-5c9e5f4b51a2",
      "counterparty": { "name": "Example Bank S.A.", "lei": "529900T8BM49AURSDO55" },
      "scope": "Onboarding, periodic KYC/AML updates, and signing API agreements",
      "jurisdiction": "EU",
      "validFrom": "2025-08-25T15:00:00Z",
      "validUntil": "2026-08-25T15:00:00Z",
      "constraints": {
        "maxTransactionLimit": "EUR 100000",
        "channels": ["Web", "API"],
        "revocableBy": ["ACME Compliance", "Example Bank S.A."]
      }
    }
  },
  "role": {
    "type": "EngagementContextRole",
    "label": "Authorized Representative",
    "authority": "Acts on behalf of ACME within the engagement below"
  },
  "engagement": {
    "id": "urn:uuid:8f9c2f3a-1b62-4d8a-9e57-5c9e5f4b51a2",
    "counterparty": { "name": "Example Bank S.A.", "lei": "529900T8BM49AURSDO55" },
    "scope": "Onboarding, periodic KYC/AML updates, and signing API agreements",
    "jurisdiction": "EU",
    "validFrom": "2025-08-25T15:00:00Z",
    "validUntil": "2026-08-25T15:00:00Z",
    "constraints": {
      "maxTransactionLimit": "EUR 100000",
      "channels": ["Web", "API"],
      "revocableBy": ["ACME Compliance", "Example Bank S.A."]
    }
  }
}
```

(ACDC illustration abbreviated)

The World of Digital Identity Credentials

Mobile Driver's License (mDL) & mDOCs



ISO 18013-5/7
Mobile Driver's
License (mDL) &
mDOCs

Parallel approach
to **W3C VCs**

ISO 18013-5/7: Specifications define mDOCs for government-issued credentials

mDL: Mobile Driver's License, a specific mDOC profile

Tech Standards: CBOR structures and COSE Mobile Security Object (MSO)

Presentation Methods: NFC, BLE, QR code, or mDOC-over-HTTP

Wallets: Being built to support both W3C VCs and mDOCs

Global Digital Identity Initiatives

EUROPEAN UNION



eIDAS 2.0 (European Digital Identity Framework Regulation (2024/1183))

- EUDI Wallet EU-wide for identity, attributes, & signing
- Developed via LSPs & Commission implementation prototype aligned with ARF, with national wallets expected to conform
- Wallets for individuals and organizations
- Goal to reach 80% of EU citizens by 2030 (~360M users)

INDIA



Aadhaar (Foundation in Hindi)

- Centralized, registry-based national ID system
- Uses APIs and PKI Artifacts:
 - Online Authentication (biometrics/OTP)
 - Paperless offline e-KYC (ZIP with signed XML)
 - Digitally signed secure QR code

UAE



UAE Pass

- OAUTH/OIDC flows, digital signatures & e-seal, & document verification ("UAE Verify")
- Unknown if it will support W3C VCs

BELGIUM



Itsme

- Supports OpenID Connect login
- Piloting VC flows with EUDI Wallet LSPs

UNITED STATES



Per-State mDL Programs

TSA is currently accepting mobile wallets/mDLS:

AR, AZ, CA, CO, GA, HI, IA, LA, MD, MT, NM, NY, OH, PR, UT, VA, & WV

Q&A

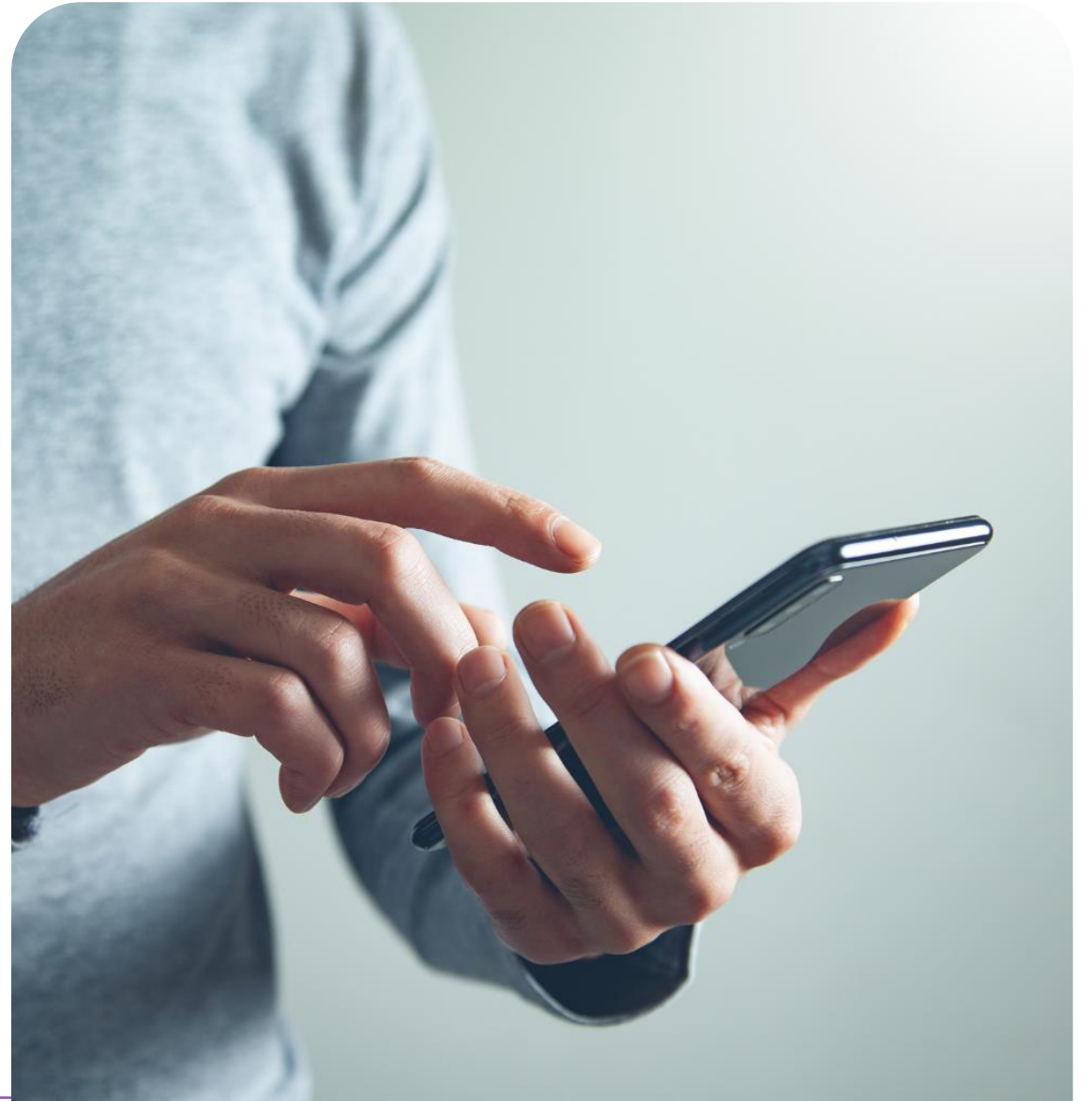
Join the ATIS Digital Identity
Working Group

Coming Soon

www.numeracle.com

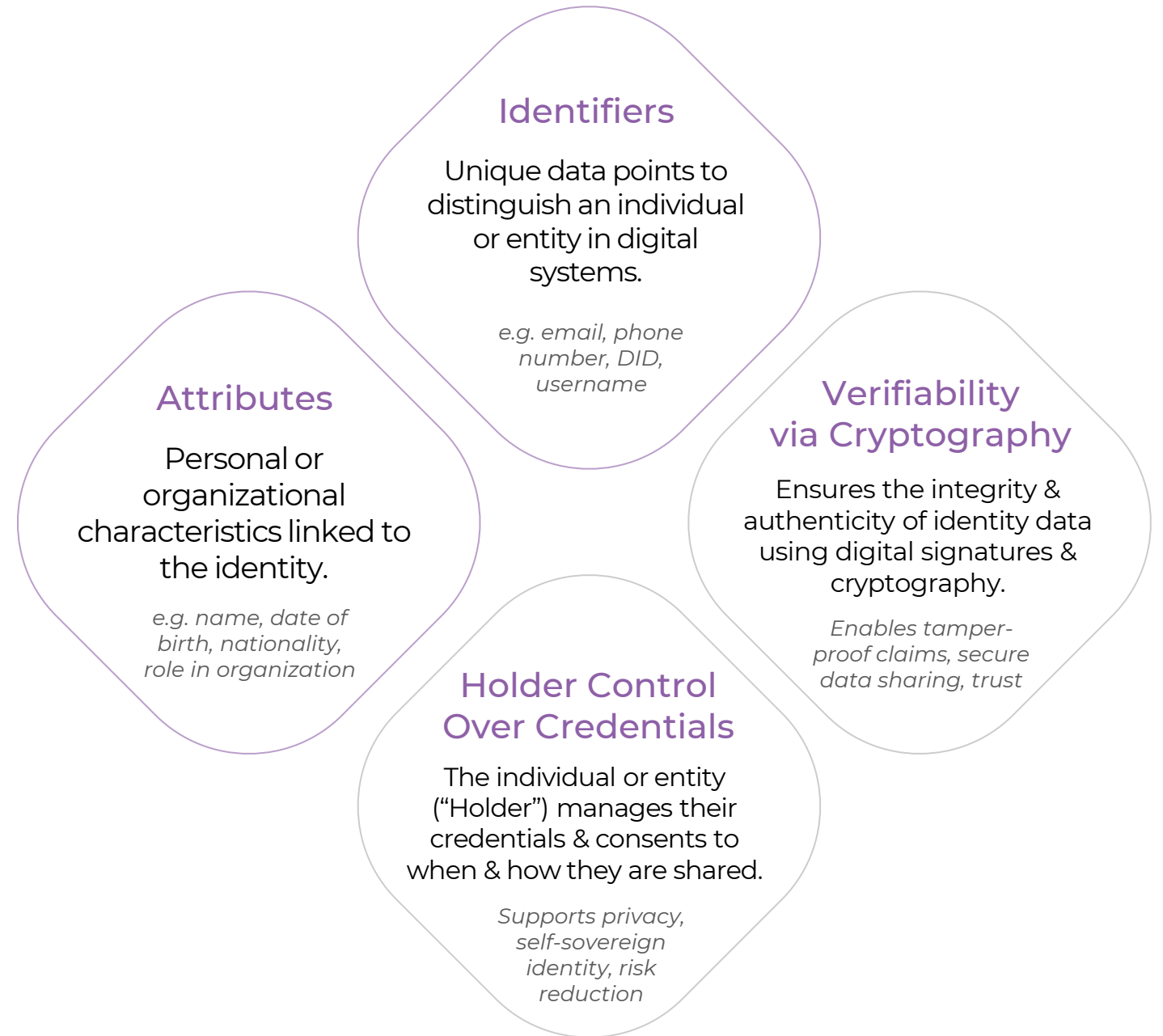
Appendix

[Learn More](#)

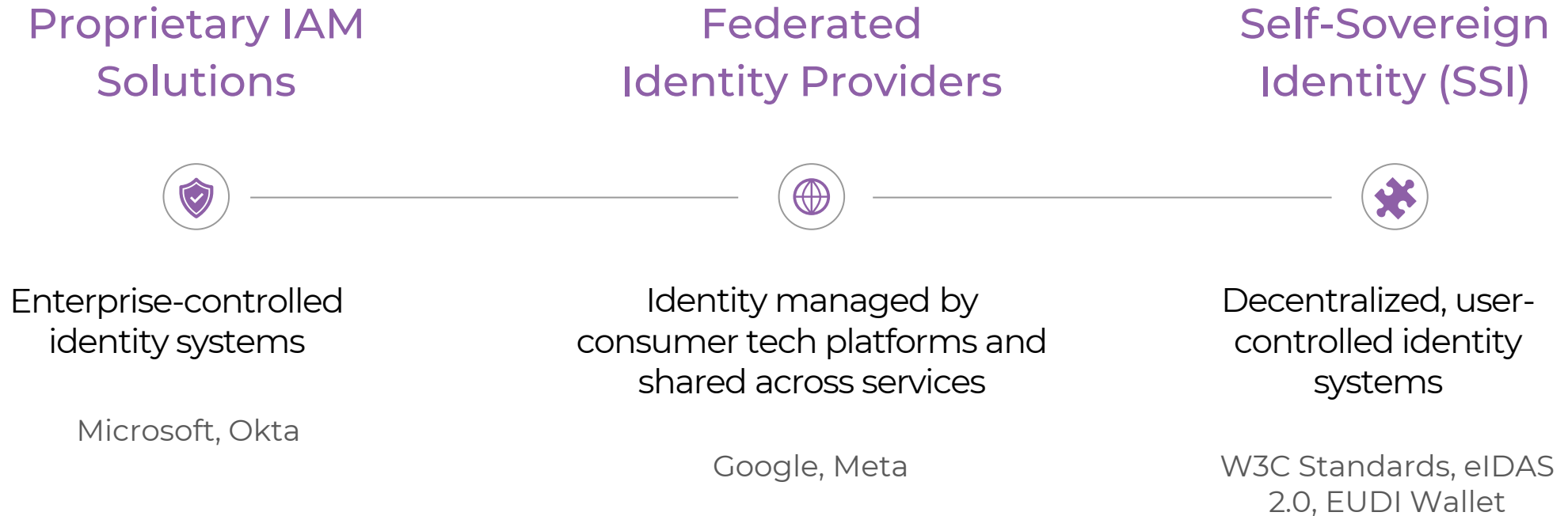


What is Digital Identity?

There is **no** official or standard definition.



The Many Faces of Digital Identity



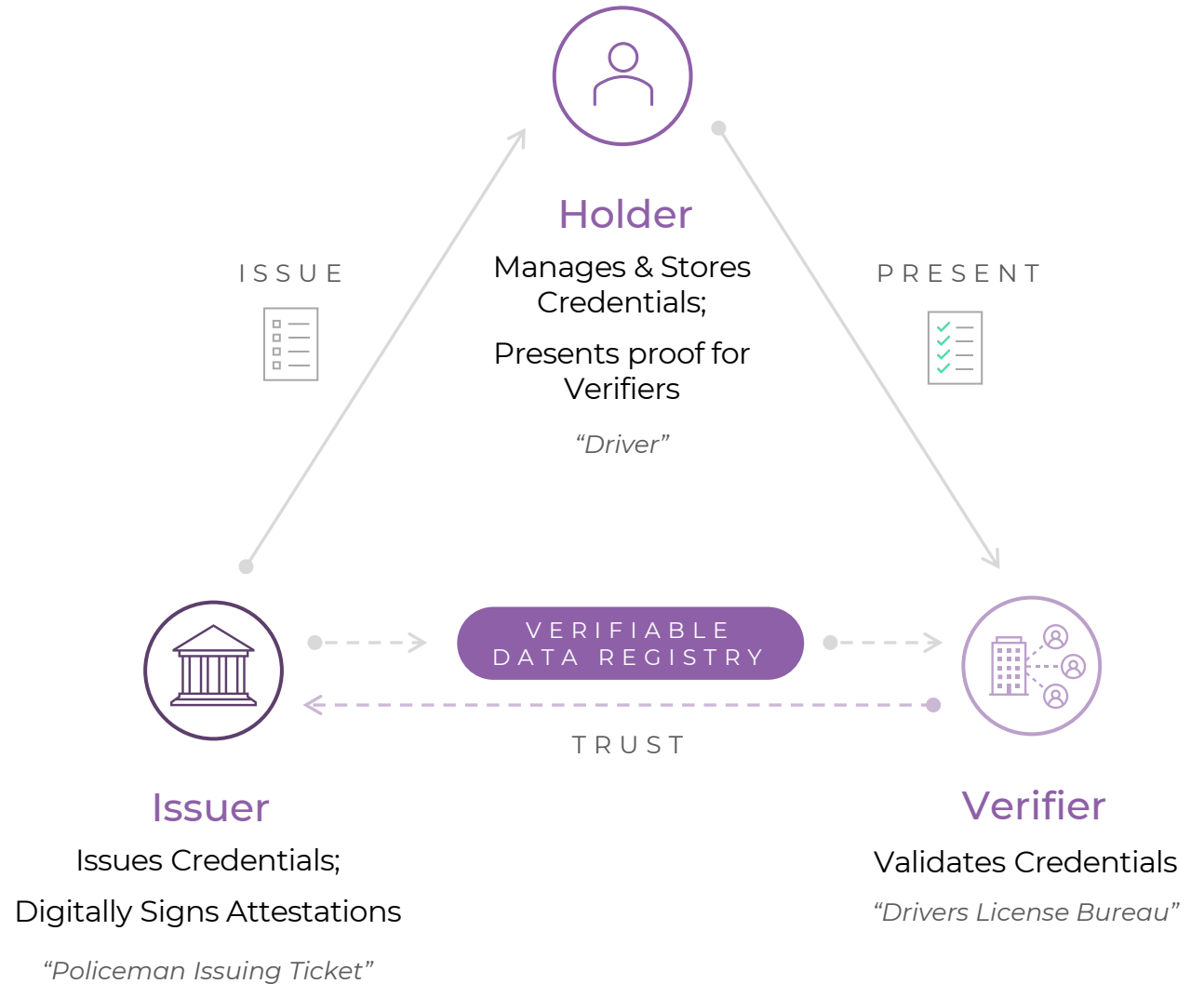
Digital Credentials Ecosystem

Verifiability via Digital Signatures

Where do credentials come from?

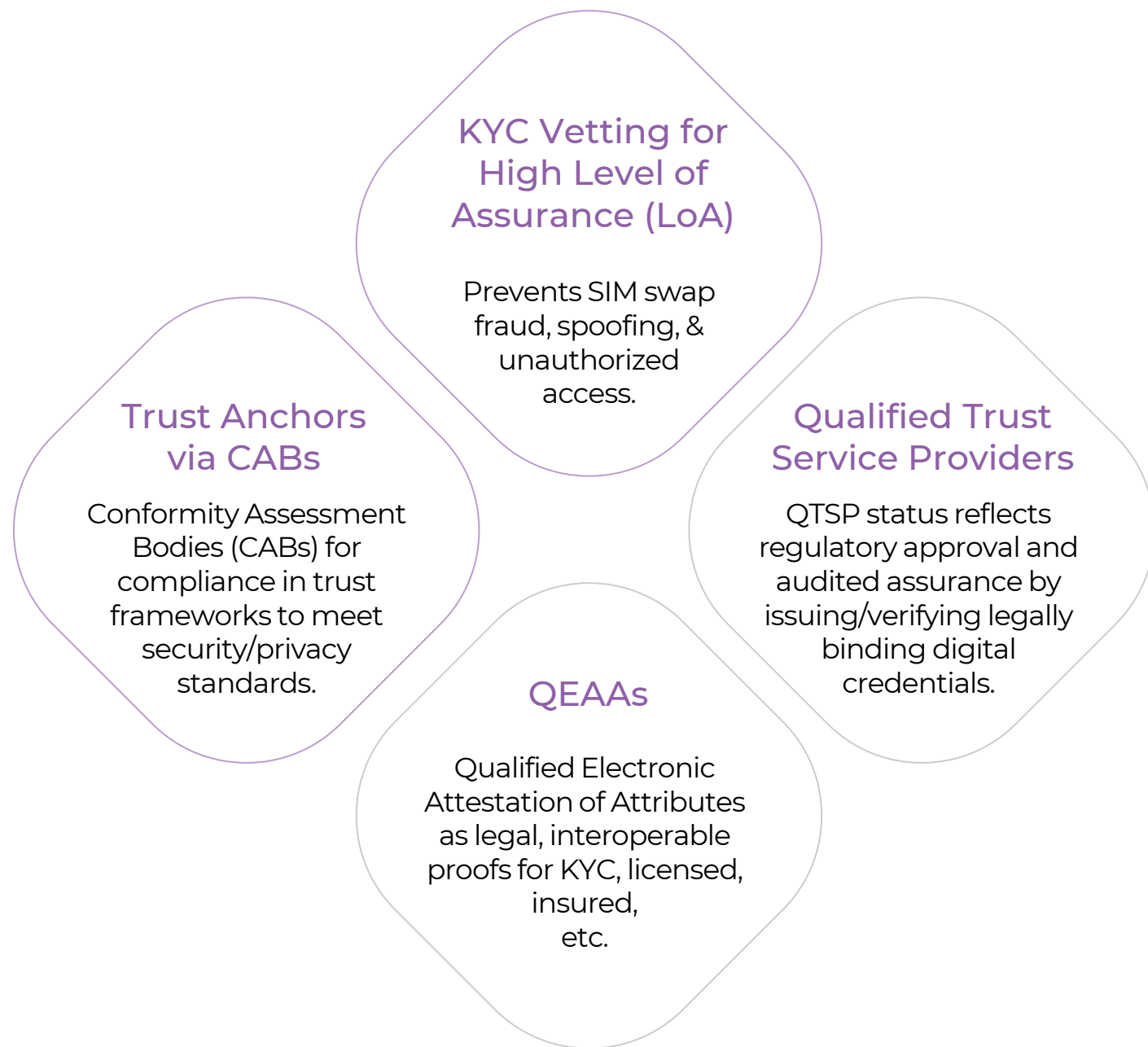
Who is trustworthy?

How do you know you can trust them?



Trust Frameworks & Assurance

Interoperability, compliance, and a high level of assurance for identity interactions.



Digital Identity in Communications

The foundation to **trusted** communications, enabling authentication, accountability, and security to ensure every interaction, whether from a business or individual, is **verifiable** and **legitimate**.

Trustable Caller Identity

SITR/SHAKEN for Voice

A framework to digitally sign & verify caller identity in VoIP networks through digital call signatures.

Secure SMS

Rich Communications Services (RCS)

RCS with verified sender identity for secure and authenticated feature-rich messaging with brand trust indicators.

Applicable Channels

A2A, A2P, B2B, B2C, C2C

Consistent verification across interaction types to protect both users and brand in omnichannel communications.

Security Goals

Ensuring identity is **established**, **protected**, and **verifiable**

Authentication of All Actors

- Critical for STIR/SHAKEN, RCS verification, & identity validation
- Combats impersonation, spoofing, unauthorized access

Encryption for Confidentiality

- Protect data in identity exchanges from unauthorized access
- Privacy-by-design in identity exchanges

End-to-End Trust Across Digital Ecosystems & Networks

- Enables interoperable trust and cross-carrier caller identity authentication
- Chains of trust from the identity source through every layer in the communication stack



Summary

Digital Identity is Multifaceted

