

**Any ID is good**

...in a rapidly changing (meta)world

Andrey Kolesnikov  
IoT Association

# ID basics

What are identifiers?

What is the ID for?

Properties of identifiers

- Shared vocabulary

- Syntax and Semantics

- Governance

- Assignment and resolution

Humans and Objects with identifiers

Syntax	Letters and numbers (ASCII, Unicode). Structured and unstructured (prefix, symbols separation, character count or flat)
Semantics	Humans can understand or apprehend; or, only machine readable
Governance	Managed within organization, association, government or global governance
Assignment	Assigned within a domain or global assignment
Resolution	Local resolution into local IT system or global resolution into local or global IT system

# Old and new ID standards

URI RFC3986(7) - billions

UUID RFC4122 - trillions

Domain names - millions

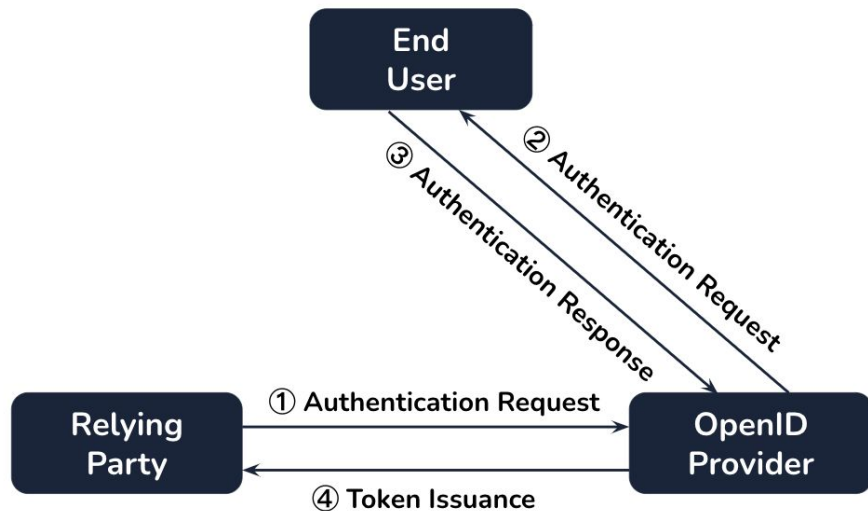
--

[OpenID connect](#)

Decentralized Identifiers ([DIDs](#))

Federated infrastructure IDs

# OpenID



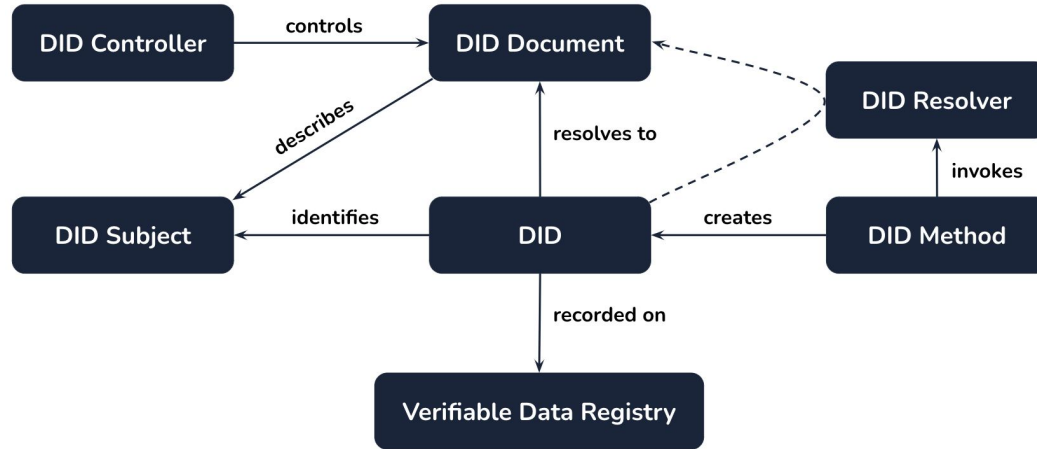
Step 1 - user attempts to start a session with a client application (i.e., a relying party) and is redirected to the OpenID provider for authentication.

Step 2, the OpenID provider prompts for user authentication and shows the end user which user attributes the relying party is requesting.

Step 3, the end user authenticates to the OpenID provider and grants or rejects access to the requested user attributes.

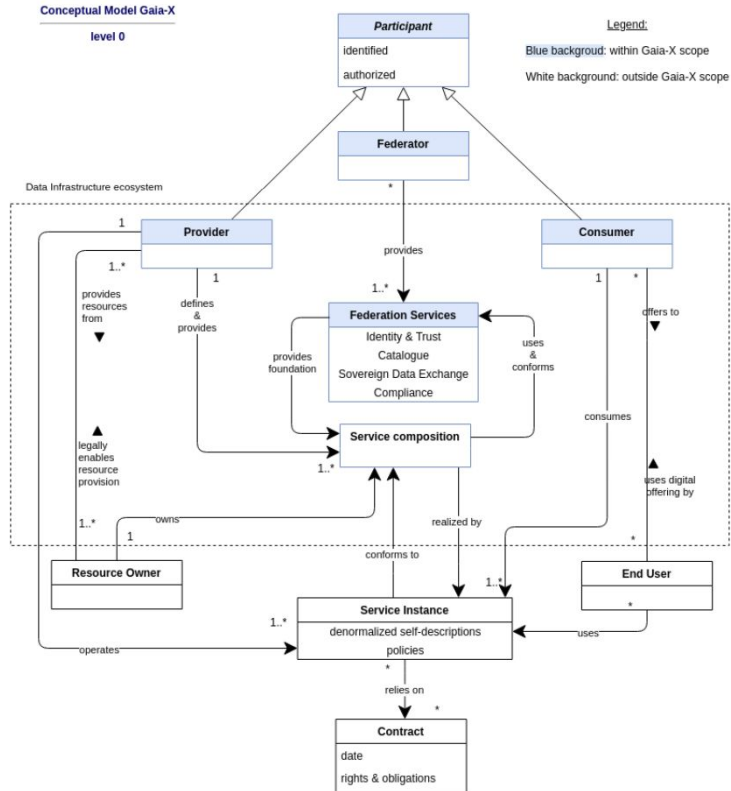
Step 4, the end user is redirected back to the relying party by the OpenID provider.

# Decentralized identifiers (DIDs)



DID, which is created via a DID method and recorded on a verifiable data registry (e.g. a distributed ledger, a decentralized network, etc.), identifies a DID subject (e.g. a person, organization, thing, data model and abstract entity)

# GAIA-X federated infrastructure



IDs must be unique in the context of [GAIA-X](#). This is achieved by combination of a schema and the protocol-specific ID

Controlled by the identity system of a participant, no central repository

Any participant's identity system can generate identifiers

Identifiers can be referenced without publishing the identifier beforehand in a separate system

Identifiers shall be derived from an identity system without any separate attribute needed. The identifier shall provide a clear reference to the identity system technology used (OpenID Connect and DID). Any scheme for identifiers must permit future extensions to the scheme

Lifetime of an Identifier is permanent

No Reuse

An identifier shall not impede resolution. For identifiers that have corresponding URLs or other resource access protocols, there must be some feasible mechanism to translate an identifier to an address of the resource

The identifier shall be comparable in the raw form. A transformation must not be needed to compare two identifiers and tell whether they are the same

Identifiers should not contain more information than necessary (including personal identifiable information)

# XXI Century (meta) IDs

## Industrial and human IDs

Not driven by unique entities such as ICANN

Good for humans, machines and information entities

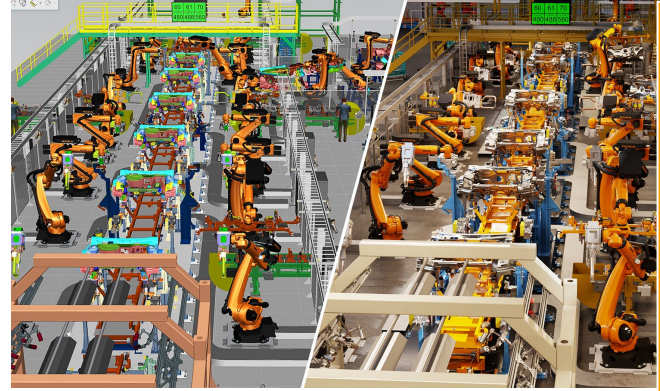
--

Metaverse IDs: decentralized blockchain approach vs. trusted parties authority, [saga continues](#)

Web3: decentralized by default

---

No business for domain names at large, however DNS will be in place to resolve your meta-cats in meta-siloes until stakeholders come to an agreement for meta-ICANN (which is unlikely, IMHO)



# Conclusion

Many ID systems have emerged

Reason: Real-world / Virtual-world  
identification and interoperability

3 main ID properties: Registration,  
resolution, discovery

Can be centralized or distributed

Thank you!

Andrey Kolesnikov

[dagnazza@gmail.com](mailto:dagnazza@gmail.com)

