The Global Identity Foundation
A single global identity for humanity

Glossary: Identity 3.0 Definitions

The Global Identity Foundation is an organization constituted as a "not-for-profit" foundation working with research sponsors and partners to facilitate the development and enabling the delivery of a viable decentralized global identity ecosystem;

That is truly privacy enhancing

- That scales globally
- That supports all entities[1], not just people, in a distributed global, identity ecosystem
- That is globally acceptable to all parties; to consume identity attributes with a known level of trust.

Background

One of the problems when working in the digital identity space is that every word has been used at least twice! often with very different meanings.

This is a stand-alone document, collating the terms used within the Identity 3.0 body of work.

Agency

The ability to grant another entity the ability to certain aspects (or ***facets***) of one's identity.
For example (1); a parent has agency over certain aspects of their child's identity before they reach legal majority.
For example (2); a PA may be granted agency over certain aspects of their boss's work life, such as book meetings on their behalf (delegated access) or have agency granted to their corporate credit card to book hotels and travel.

Attribute

A characteristic, feature, element, property or inherent part of an **entity**.

Signed attributes: An attribute that is digitally signed by the entity that is **authoritative** for that attribute.

Validation of attributes: The ability to validate the **digital signature** of a signed attribute and also the **attribute lease time**.

Attribute Lease Time

The period of validity, defined by the **issuing entity**, for a persona (and collection of attributes). The **receiving entity** is free to ignore the lease time on any asserted attribute and use its own **entitlement rules;** for example: ignore the lease time and just accept the attribute, or ignore the lease time and insist on real-time validation.

Assertion

The ability of the **pertaining entity** to pass one or more (signed) attributes in support of a transaction; allowing the **receiving party** to validate those attributes in the context of the entity asserting them, vs. the transaction being requested.

See also: ***Self-assertion***

Authentication

The act of proving **sameness** (ideally to an understandable level of certainty).

See: ***Immutable Linkage***

Authentication Factors

The methods (or factors) by which authentication can be asserted:

---

[1] Entities are: People, Devices, Organizations, Code & Agents. [Definition: Jericho Forum/Open Group]

- *Knowledge factors*: Something the entity knows (e.g. a password, partial password, pass phrase, PIN, or challenge response).
- *Ownership factors*: Something the entity has (e.g., digital certificate, security token (hardware or software), implanted device, cell phone etc.)
- *Inherence factors*: Something the entity is (e.g., fingerprint, retinal pattern, DNA sequence, signature, face, voice, unique bioelectric signals, walking gait, or other biometric identifier).

Or the methods by which authentication can be inferred:

- *Observed factors*: Something the entity does or repeats (geo-location, historic/normative transactional profile, browser fingerprinting, device identity, organization identity etc.)

Authoritative (authoritative attributes)

An entity that is authoritative for some aspect or facet (**persona**) of an entities total identity; examples are:

- The Government [Entity: Organization] issues my birth certificate and thus is authoritative for my "***citizen persona***" and attributes within it (date of birth, place of birth, sex at birth, name at birth and citizenship).
- My company [Entity: Organization] is authoritative for my "***work persona***" and the attributes such as "starting date", "grade", "department", "title" etc.
- Volvo [Entity: Organization] is authoritative for their cars [Entity: Device] they make (**Sameness** = VIN Number) with a number of defined attributes (engine, trim level, model etc.). Note that the join between a unique Entity:Device "Volvo XC90 VIN=XXXXX" and Entity:Person "Fred Smith" creates a unique **persona** "Fred Smith's XC90" providing both context, ownership and a unique cryptographic key for that vehicle under Fred's control.

Context

The ability to understand the digital join and who signed the **attributes** (as the **authoritative** source). *For example;* Work **persona** signed by your employer; your date-of-birth signed by government.

Core Identifier

The digital representation of the **core identity**, with a definable level of **immutable linkage** between the two.

Core Identity

The actual entity (or example a person) to which all the **persona**, and hence **attributes**, refer.

Digital Persona

The digital join of two entities; one that is **authoritative**[2] - the **issuing entity** which signs the attributes and the **pertaining entity** - the entity to which those attributes refer. [see also: ***Persona***]

A cryptographic join of two entities[3];

- Creating a separate, unique and (cryptographically) identifiable persona
- Containing a collection of **authoritative attributes**
- With attributes (cryptographically) signed by the **issuing entity**
- With attributes (cryptographically) assertable by the **pertaining entity** or **originating entity**
- Where the cryptographic join may be via an entities **core identifier**, but more likely will be via a persona belonging to that entity[4]

A digital persona allows the **relying entity** to put **context** around an asserted **attribute** from a particular persona; e.g. an "I am over 18" assertion is signed by the UK Government.

Personas come in three **persona types**;

- Self-asserted - A persona and attributes that the **pertaining entity** has self asserted and self-signed.
- Inferred - A **persona** that you assign and maintain based on information you have inferred

[2] A self-asserted persona is the join between the same entity

[3] Where one entity may be a null entity (in, for example, a self-asserted persona)

[4] Where the persona could be the core identifier, rather than a persona

- Entity-signed - signed by an **issuing entity** - the authoritative source for those attributes and that persona

Digital Signature

A digital code which is attached to an attribute, allowing the **receiving party** to verify its authenticity.

Entitlement (entitlement rules)

A set of rules (or an algorithm) which if met entitles two entities to transact. If using an algorithm, the "entitlement process" could include a "negotiation" between the **pertaining entity** and the **receiving party** about **attributes** each considered suitable to meet the entitlement criteria.

Entity (and entity types)

A thing with distinct and independent existence. There are five entity types: People, Devices, Organizations, Code and Agents. Any entity type may interact with any other (in that way they are functionally identical) but the interaction of two entities to create a **persona** gives **context**.

Facet (of an identity)

An exposed slice of an entity's total Identity. See also: ***Persona***.

Identity

A collection of **attributes** about the entity, grouped together in peronas which are linked together by **sameness**. All (in the digital world) with an understood (and communicable) level of **immutable linkage** between the entity and its sameness.

Identification

The process by which a set of **assertions** or **attributes** allow matching to a particular unique entity (**sameness**).

Note: Identification may be initiated as part of a transaction, but can also be triggered by an asynchronous event; for example, a person walking past a public camera linked to a facial recognition system.

See also: **Verification, Validation** & **Sameness**

Immutable Linkage (or Immutable Binding)

The linkage between the entity and the digital ecosystem. The authentication/linkage method must always be communicated to the other party in the transaction chain. Key to trust in the ecosystem is the **receiving party** being able to understand the level of immutability with which the linkage is made; this usually means understanding the method (usually hardware type/model) used.

Issuing Entity

The entity that is authoritative for a set of **attributes** given in a **persona** to the entity to which they pertain. The issuing entity is responsible for maintaining the attributes over time, including automated renewal, setting an appropriate **[attribute] lease time**, and providing an interface where the entity can automatically renew its lease and any receiving party can check (in real time) the validity of those attributes.

Lease Time

See: ***Attribute Lease Time***

Originating Entity

The entity originating a set of attributes - this could be the **pertining entity** (if those attributes pertain the that entity) but could be an entity:agent; originating attributes on-behalf (with agency) of another entity.

Persona

A collection of **attributes** that describes or places an **entity** in a particular contextual setting (a particular "facet" of an overall identity). [see also "Digital Persona"]

Persona Lease Time

See: ***Attribute Lease Time***

Persona Types

There are three persona types; Self-asserted, Inferred & Entity-signed.
See: **Digital Persona**

Pertaining Entity

The entity to which a **persona** and associated set of (signed) attributes pertain (refer) or belong.

PI

Shorthand for "Personal Information"; this has specific legal connotations when handling such information under the EU GDPR or other privacy legislation. See also: **SPI**

Plausibility

The probability that the entity being authenticated is really that entity; based on understanding both the authentication method used (which defines the strength of the authentication method [the level of **immutable linkage** between the entity and the device]) and the possibility of the device itself being subverted to give a false authentication assertion (understanding the model or hardware being used to provide the immutability, and potentially the chain of custody or provenance of the hardware).

Primacy

The ability of an entity to have control over **facets** or **personas** of their total identity.

For example (1): to refuse a request for certain identity **attributes**, identity **facet**, or **persona** [in a form that neither confirms nor denies its existence].

For example (2): While knowing a person's date of birth & address; primacy implies you are unable to **assert** those **attributes** (spoof or impersonate) as being that person. Primacy implies that only the owner of that **persona** can **assert** (signed) **attributes** from that **persona**.

Privacy

The ability of an entity to keep secret (or at least minimize) information about **facets** of their overall identity. Note: there is an acceptance here that to operate in a digital society total privacy is not a feasible concept, but that there are certain **facets** or **personas** (especially SPI) an entity will keep highly restricted or may try never to reveal..

Receiving party (or Receiving entity)

The entity that receives a set of (signed) assertions from a **pertaining entity** or **originating entity** as part of a transaction which facilitates being able to make an **entitlement** decision about whether to transact[5].

Relying party (or Relying entity)

See: **Receiving party**
Note: "Relying party" implies a hierarchical, one-way trust relationship, whereas in most transactions the trust and risk is (or should be) bidirectional but usually asymmetric.

Sameness

Being identifiable as a unique entity - the same entity at first interaction, today, and tomorrow. Ideally the **receiving party** will be able to understand the level of **immutable linkage** between entity and **authentication** method used. In the non-digital realm humans use faces to identify that you are the same person they first met, are today, and will be tomorrow.

[5] Remembering that in any transaction, risk is bidirectional but usually asymmetric.

Schema

A defined set of attributes that a particular persona contains. There are four persona and schema types:

1. **Signed Public [SIGNED]** - Is a common persona, signed by the authoritative source for the attributes it contains. Because of the need for interoperability it is defined once globally. Examples: Citizen, Postal Address, Bank.
2. **Signed Private [PRIVATE]** - Is a common persona, signed by the authoritative source for the attributes it contains. It is defined (and maintained) and it is unique to the organization that created it. Potentially this could be a "club" of organisations for example: "OneWorld (Airline) Alliance" or "SAFE-BioPharma".
3. **Self Asserted [SELFASSERTED]** - Is a common persona (see 1.) but signed by the **pertaining entity**. Examples: Postal Address, Alias [how the entity wants to be known in a particular context].
4. **Derived [DERIVED]** - A derived persona contains attributes, conforming to a common class, populated in real time (or at run time). Example: Device [the signed trust attributes of the Anti-virus on a device, interrogated directly from the device by an ID3 app]

Self-assertion

The process by which an entity signs its own **attributes** within a **persona** it creates and therefore owns and is responsible to manage.

Signed Attributes

See ***attributes***.

SPI

Shorthand for "Sensitive Personal Information"; this has specific legal connotations when handling such information under the EU GDPR or other privacy legislation. See also: **PI**

Validation

There are three primary types of validation:

1. The process by which an entity's **attributes** are checked to see if they exist; thus providing a level of assurance that the attribute being asserted is valid. For example, by checking databases such as postal address files, telephone records or basic credit data.
2. The process of checking the (digital) signature of presented **attributes** or assertion to ensure that the signing entity is the authoritative source [or at a minimum a source that is acceptable to the **receiving party**]. For example, the presented "I am over 18" assertion is signed by a government entity.
3. The process of comparing something unique to the entity with information held by the relying party. For example, a stored photograph vs. a (requested) real-time snapshot; or a cryptographic assertion leveraging the existing cryptographic relationship (digital **persona**).

See also: **Verification**

Verification

The process by which an entity's **attributes** or **assertions** meet the conditions (or **entitlement** rules) defined for a transaction to occur.

For example, **validation** matches a stored photograph to a (requested) real-time snapshot, which in turn provides verification that said entity is the owner of the asserted bank account.

See also: **Validation**

