The Global Identity Foundation
A single global identity for humanity

Anonymity at the root of an Identity
(A primer on key aspects of Identity 3.0)

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

On first encounter, the concept of anonymity as the starting point for trust seems counterintuitive; the headline statement means that people, particularly those in law enforcement, do not read beyond that headline. However in the majority of cases, the ability to deliver contextual and trusted attributes along with privacy safeguards has the ability to deliver a significantly more trustworthy Internet.

The basis for anonymity at the root of an identity

This is how humans operate! Notwithstanding a universal DNA database; when we are born we are effectively anonymous - and over time we add "personas"; groups of identity attributes that place us in a particular role or context. Examples of "personal" personas are: family, school, sport, profession, sexual persuasion, qualifications, citizen, tax payer, education, address, driving etc.

How many of these personas, or more correctly, attributes of those personas, we choose to expose or share in a particular context is under our control and is a function of our personal risk assessment, based on our level of trust in the third party (and the attributes they may share with us) and/or the environment.

So, while there will be some people (such as a long-term partner) who know most of your personas, ultimately YOU, as the "root" of your own identity, are the only entity who knows all your own personas and their attributes.

Note that currently, in the digital world, we leverage this ability to provide multiple disparate attributes (some of which may be semi-secret) to prove "sameness"; that we are the same entity that set up the computer account; typically when performing account recovery / password reset, or "proving" our identity on the telephone.

Digital identity

We can replicate the concept of an anonymous root with multiple personas into the digital world; but now we can leverage cryptography to improve four aspects:

1. Utilise an anonymous cryptographic root owned by the entity, allowing the creation of digital personas to sit under this common cryptographic root; thus enabling only that entity to assert multiple disparate attributes from its various personas.
   The party receiving the assertions is able to cryptographically verify:
   - That these asserted attributes have a common, single root; while that root can remain anonymous.
   - That each individual attribute is signed by the entity that is authoritative for that attribute.
2. Provide a cryptographic foundation for a persona to be created and digitally signed by the entity that is authoritative for those attributes. For example;
   - Government : Citizen Persona
   - Local authority : Address Persona
   - Visa : Issuing Bank : Credit Card Persona
   - ACME Company : Employee Persona

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

3. Utilise a one-way trust to ensure that an entity issuing, or knowing, one persona is unable to go back up to the root and come down into all the other personas of that entity.
4. Create an ecosystem, whereby you may know many of an entities attributes, but you are unable to assert them as a signed collective set, or assert them pretending to be that entity.

The benefit of this approach it that its privacy enhancing, allowing only attributes required in a particular context to be exposed.

Anonymity vs. Sameness

In many transactions all the relying party cares about is that the entity belongs to its attributes, credit cards have signatures, driving licences have photos; there is no actual interest in "who" the entity actually is, except to potentially tie together multiple disparate assertions; the name on the drivers licence (photo & over 18) matches the name on the credit card (ability to pay) and the name on the casino membership card.

In contrast, most computer systems only care about "sameness" - you are the same entity today that first enrolled for this account, and will be the next time you connect; again there is no interest in "who" the entity actually is.

Anonymity and immutability

In the physical world the originating entity is likely present and thus the level of immutability between credentials and entity (e.g. photo) can be evaluated; but over the Internet there is usually a need to understand the level of trust that can be placed in the entity at the centre of the transaction (the level of immutability).

Cryptographically proving an entity is easier when the entity is a device or an organization rather than a person; with people the level of immutability is the certainty by which the biological entity is linked to the device/firmware they are using and understanding the device, registration method and the potential for subverting the device or spoofing the person registered on that device.

The receiving entity

Has a set of (entitlement) rules by which it is happy to transact. They are able to validate each of the attributes it needs for this calculation to their authoritative sources, and can (if they choose) layer on historic and normative transaction information [have they done this before? was it all OK?].

If the entity is a person, the attribute assertion(s) should also contain information about the level of immutability between person and device; thus the transactional risk can be accurately matched within allowable risk appetite.

The originating entity

Can make a (risk-based) decision about whether to transact using the attributes from its various personas that are being requested and how anonymous / privacy-enhancing they are (such as "are you over 21" vs. "date-of-birth").

Understanding the attributes being requested; and matching the reasonableness of this request to the context of the transaction allows the entity to make a risk-based decision to either continue or abort the transaction.

Governments & law enforcement

Can leverage a global identity ecosystem to mandate that providers insist on traceability to a real person [a Government, signed, "Citizen persona"] when creating an account; thus stopping fake profiles, account impersonation, "sock puppets" and allow the tracing of "trolls". Service providers can be mandated to implement an age rule when dealing with minors; e.g. to disallow grooming.

However the originating entity is able to maintain its anonymity by being able to understand the assertions being requested and choosing not to subscribe to services that mandate such requests.