The Global Identity Foundation
A single global identity for humanity

Why Identity 3.0?

(or; what must we do that is fundamentally different?)

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

We all know that Identity in the digital world is broken; passwords (Identity 1.0) are well beyond their sell-by date, while Spam, Fraud, Phishing and Cybercrime succeed by being able to steal identities and impersonate individuals. This fraud, with Identity as its root-cause failing; is an epidemic costing hundreds of billions of dollars per year[2].

Current industry efforts (Identity 2.0) focus on extending the current "silo-based identity systems" and allowing disparate systems to interoperate; but does not scale globally nor address the future needs of a global Internet.

Identity 3.0, based on original work from the Jericho Forum®, is predicated on the need to fundamentally design the underlying Identity ecosystem differently; with key areas that must be addressed if the goal of a single, global, decentralised identity ecosystem is to be created that can achieve a level of trust at intergovernmental levels while being demonstrably privacy enhancing with the concepts of primacy and agency at its heart.

This primer looks at those key differences:

There must be anonymity at the root of identity

Only 100% anonymity at the root of an entity's identity[3] will solve the problems of privacy and primacy; this principle of anonymity will allow entities to operate with a single and consistent root of their identity (enabling Bring Your Own Identity) and facilitate solutions to such problems as anonymous e-Voting and how you get disparate governments to accept each other's digital identities.

Any identity ecosystem must encompass all the entity types

In a global ecosystem Identity must work identically and interchangeably across all five entity types. The creation of a new digital persona as the join of two entity types defines the context associated with that persona and provides a cryptographic "container" for a set of trusted attributes.

Context in turn enables "entitlement"[4] based rules to be specified, enabling technologies such as "Bring Your Own Device", "Digital Rights Management" and the "Internet of Things" to be simply implemented and maintained.

Personas[5] are core to privacy and anonymity

Creating personas[6] from two entities via a one-way cryptographic trust ensures that knowing one persona does not allow identification of the root identity and thus the other personas of that entity.

---

1 Entities are: People, Devices, Organizations, Code & Agents. [Definition: Jericho Forum/Open Group]
2 http://www.mcafee.com/uk/resources/reports/rp-economic-impact-cybercrime2.pdf
3 Jericho Forum "Identity Entitlement and Access Management" Commandments #1 [https://www.opengroup.org/jericho/Jericho%20Forum%20Identity%20Commandments%20v1.0.pdf]
4 For more information on entitlement see Domain 12 of "Security Guidance for Critical Areas of Focus in Cloud Computing V3.0" [https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf]
5 See: "Primer - Personas as a basis for context & trust" for more detail
6 A persona is unique join of two entity types, containing attributes defining the identity of that persona.

Example; your "Citizen Persona" is the cryptographic join of [Entity: Organization] Government and [Entity: Person] Yourself, and contains five attributes signed by Government for which they are authoritative - namely Date of Birth, Place of Birth, Sex at Birth, Name at Birth, Right of Citizenship.

Attributes contained within a persona should be truly authoritative[7] to the issuing entity, with that authoritative entity able to define the validity and expiration of those attributes. This benefits the issuing entity by never having to maintain attributes for which it is non-authoritative, thus eliminating or at least minimising liability.

Once an entity has the cryptographically signed and secured attributes associated with that persona then the pertaining entity is able to unlock and assert individual attributes from that persona (signed by the authoritative organization) as well as asserting attributes from other personas it holds (under the same root) as the transaction[8] requires.

All transactions should be risk-based

Using personas and attributes from authoritative sources negates the need for federation[9]; they also provide context allowing risk-based decisions to be made. The use of authoritative signed attributes asserted under the entities control eliminates most liability concerns and greatly simplifies the Identity model eliminating the need for identity brokers or centralised identity stores, thus making a global ecosystem viable.

Evaluating the quality and provenance of Identity and Attribute information

In any transaction, the entity taking the risk[10] should be able to evaluate the end-to-end risk of that transaction.

By fully understanding the quality and provenance of the identity and pertinent attributes of all the entities in the transaction chain the relying entity is able to ensure that its evaluation criteria matches its risk-appetite

At no point should any intermediate entity in the chain turn "plausibility"[11] into a binary, but instead the entity taking the risk must be capable of evaluating the individual risks in the entire transaction chain.

The quality of the linkage between person and firmware must be understood

The methods of authentication[12] of an entity should be fully understood and form part of any risk equation. Where the entity is a person then it is critical that the level of immutability between person and device is properly understood. This means understanding the method of linkage, the device used and the provenance of that device.

Conclusion

Unlike outdated digital identity systems using passwords, or contemporary federated siloed lock-in systems that collect all attributes about identities in centralized databases, the Global Identity Foundation seeks to design an identity ecosystem that preserves an individual's root anonymity whilst allowing parties in a digital transaction to fully assess their level of risk through cryptographic linking to authoritative sources.

---

7 Authoritative attributes are typically generated, maintained and signed by the entity at their source or origin.

8 A "transaction" could be any interaction between two entities; such as e-commerce, e-banking, system access, file access, data access, network access, email, voice telephony etc.

9 Federation requires trust in the body with which you are federating, not the attributes and identity being consumed; thus it fails to scale, and does not allow the entity taking the risk to properly evaluate the risk.

10 Bearing in mind that most risk is bi-directional, though that bi-directional risk is usually asymmetric.

11 Plausibility: the probability that the entity being authenticated is really that entity; based on understanding 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.

12 Key to evaluating risk is understanding the level and method of "immutable linking" of entity to the digital device.