The Global Identity Foundation
A single global identity for humanity

Why identity ecosystems fail
(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

Attempts to develop an identity ecosystem that is truly interoperable and can be trusted by multiple disparate parties, to date, have failed spectacularly and expensively; quietly die; or stagger on, adding yet another identity system into the mix. It is therefore important to understand why Identity Ecosystems fail.

Fail #1 - Reliance on a "Locus of Control"[2]

Needing to trust a third-party ecosystem (and its operator) that contains identity attributes and/or authentication information for which that system is not truly authoritative.

The lack of trust in those systems (why would you trust a US system holding Chinese citizen information?) results in a proliferation of disparate identity systems; most holding non-authoritative information.

Design criteria: *Identity systems should only hold authoritative identity information.*
Design criteria: *Minimise the reliance on identity systems holding non-authoritative identity information.*

Fail #2 - A lack of anonymity at the root of an entity's identity[3]

Without anonymity at the root of an identity, privacy cannot be assured and neither can the ability to connect disparate personas and attributes in a privacy enhancing manner.

Entities (particularly "people") need to be assured that "their" identity attributes are under their control, ensuring privacy, connecting disparate assertions, enabling e-voting and facilitating the entity to have both primacy and agency over the various attributes of their identity.

Design criteria: *Ensure anonymity at the root of an entities identity to provide an assurance of privacy, and;*
Design criteria: *Enable the entity to issue a [cryptographically] provable assertion of attributes from multiple disparate authoritative sources thus providing enhanced levels of context.*

Fail #3 - Maintaining or using attributes that are non-authoritative

There is an inherent lack of trust in any attributes consumed from a non-authoritative source.

Thus, organizations insist on their own identity validation (usually paper documents) storing attributes which change (or can be revoked) over time, in yet another (non-authoritative) identity silo.

Whether storing those attributes themselves or consuming them from 3rd party sources (which may provide a level of indemnification), most non-authoritative attributes go stale over time, or can be unknowingly incorrect, resulting in flawed risk calculations.

Design criteria: *Only maintain identity attributes for which you are the definitive authoritative source.*
Design criteria: *Insist on only accepting identity attributes from the definitive authoritative source.*

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

[2] Definition: "Locus of Control" - a control point (which could be a single server or infrastructure) that must be trusted and/or referred to; in order for the ecosystem to work.

[3] Also see: "Primer - Anonymity at the root of an Identity" for an expanded explanation

Fail #4 - Federating identity systems

If A trusts B; and B trusts C - does A trust C? [n=2] - In general federation breaks down at n=3.

The trust in a direct relationship (n=1) can be evaluated; based on the attribute(s) and how truly authoritative they are. The more attributes are disintermediated through one or more third-parties so the level of trust reduces.

Design criteria: *Only consume identity attributes asserted directly (n=1) by the authoritative source.*

Fail #5 - Fixation on "my product" solving all your problems

Myopic vision by companies solving one problem, and thinking it can expand to solving identity in general.

Trust is enhanced when you can consume authoritative attributes and assertions from any device, system or source. It fails when you are limited to a single source of (someone else's) "truth" over which you have no control.

Design criteria: *Ensure any product that is authoritative in their area can contribute to the overall risk calculation.*

Fail #6 - A lack of context in risk calculations

Not understanding the context in which an attribute is asserted restricts the richness of any risk decision.

When asserted attributes can be understood in context, then a better risk calculation can be performed. Where any non-authoritative party is in the chain, then context is usually lost or severely reduced.

Design criteria: *Full contextual information must be communicated to enable a better risk calculation.*

Fail #7 - The ecosystem only supports people (not all entities)

Without encompassing all entities, understanding persona and context are exponentially more difficult.

Persona and context are evaluated by understanding the join between entity types (see: primer on personas), thus without the support of all entity types there is no simple way to factor context into a risk decision.

Design criteria: *Any ecosystem must encompass all five entity types and the concepts of persona and context.*

Fail #8 - Not understanding the level of immutable linkage to the Entity[4]

Not being able to understand the certainty with which the entity making the assertions is actually the entity.

When making an "entitlement" decision the relying party needs to understand the degree of certainty with which the entity asserting information is actually said entity [the level of immutability]. While this is easier with device entities, with people this can be incredibly hard, especially if there is a reliance on trusting (but not owning, controlling or having detailed understanding of) the hardware and software in the transaction chain.

Design criteria: *Assertions must include the method and level of immutability of the entity to the assertion.*

Fail #9 - Turning a variable into a binary

Trust levels are not binary, but most authentication systems turn a variable (maybe the entity) into a binary.

When a third-party system turns "maybe Fred Smith" with a known level of immutable binding, into a binary "IS Fred Smith" - the entity taking the risk is unable to factor the level of immutability in their risk equation.

Design criteria: *A variable must never be represented as a binary; and all identity, attributes and context must be sent to the relying-party (entity) taking the risk to evaluate.*

Fail #10 - Reduced privacy by consolidating attributes from disparate personas

Allowing an entity (commercial or government) to maintain, collect or control multiple disparate attributes, places the "identity" of an entity at risk of misuse by the holder, hackers, criminals and corrupt governments.

Collating attributes of people (and other entities) into an identity repository makes it liable to abuse (malicious or accidental). It also allows the controller to make contextual links for commercial or nefarious purposes.

Design criteria: *Minimise the attributes held to only those for which the organization is truly authoritative.*

[4] Also see: "Primer - Trust and Immutability" for an expanded explanation