The Global Identity Foundation
A single global identity for humanity

High Level Requirements
(The key stakeholders perspective on 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.

Introduction

This document describes the key elements of a global identity ecosystem from the point of view of each of the key stakeholders in any transaction. These requirements have been summarized from discussions, roundtables and workshops. *Note that the [ ] denotes the addition of a technical explanation*.

The user wants:

1. To be (actually & directly) in control of their identity.
2. To have a single authoritative source of their identity (the *digital me*) under their physical control.
3. That their "digital me" simply transfers with the changing devices they use, replace, upgrade or add.
4. To work with "everything" they use and interact with.
5. To be able to "walk-up" to any device (including a new device) and just work.
6. To support secondary devices (say a smart-phone, PC or tablet) for everyday working [caching their identity securely into a semi-trusted device].
7. That their identity is not "owned" (or managed) by anyone other than them.
8. Can be used to [bi-directionally] authenticate both devices and services (web sites, applications and systems) that they interact with [my bank is actually my bank].
9. To be as invisible as possible [frictionless].
10. To eliminate the need for passwords.
11. Can provide attributes of their identity under their (exclusive) control.
12. The inability for someone to impersonate "me" simply by knowing their personal attributes.
13. The ability to validate who they are communicating or interacting with [all entity types].
14. To have [automatic] validation that entities I already have a relationship with are actually them.
15. To have a right [an extension of GDPR] to hold my [signed] data for which a 3rd party is authoritative.

> 86% of people want to be in control of their identity, compared to 5% who are happy for a commercial organisation to manage it.
>
> **Source: Survey Monkey: 100 anon. respondents**

The relying party wants:

1. A single, universal, global method of both authenticating entities & understanding identity.
2. A replacement for passwords.
3. A known level of trust in the authentication method(s) used.
4. A known level of trust of the identity attributes themselves.
5. To understand [factor into the risk equation] with what degree of certainly the entity is truly the entity being interacted with. [for people: to understand how the "wetware" is connected to the "firmware".]
6. No need to consume data from, or trust, or be connected with, a central (third-party) server, organization or controlling body. [though you might wish to for high risk transactions]

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

7. To be able to understand the trust levels of all the components in the transaction chain (from the originating person [or entity] to the risk decision point).
8. To be able to understand attributes in context.
9. To be able to enable "entitlement" [rules] for devices, systems, applications and networks. [all entities]
10. The ability to define its own risk tolerance for any transaction.
11. The ability to consume attributes from anywhere [any entity].
12. The ability to negotiate for alternative attributes.
13. The ability to escalate the authentication if required (based on entitlement/risk).
14. The ability to escalate the attributes required [either more or better quality attributes] (based on entitlement rules, transaction value and/or overall risk).
15. To understand the cost of the transaction; and to factor it into any risk equation.
16. To eliminate [minimize] any liability involved in the transaction.

> ***Jericho Forum Commandment #8.***
> "Authentication, authorisation and accountability must interoperate / exchange outside of your locus / area of control."
>
> **Jericho Forum / OpenGroup**

The issuing party wants:

1. To maintain only those attributes for which it is (truly) authoritative.
2. To be able to define the duration for which it considers its attributes authoritative. [lease time]
3. The ability to lodge its "identity proof" [Public Key] in one public place; under its control.
4. No need to register with a central (third-party) server, organization or controlling body.
5. No need for "federation" (in any form) with other entities.

Security wants:

1. A single source of cryptographic-keys that can be leveraged to ensure the security of:
   - Point-to-point communications (web, ftp etc.)
   - Email
   - Files (data at rest) & File transfer (data in transit)
   - Voice & Video communications
   - DRM - Digital Rights Management
2. Usability [frictionless] - invisible to the user [cryptographic keys that automatically store into contact details (or similar) for an entity].
3. One single open standard; allowing the easy leveraging of identity information for increased security; by devices, infrastructure, applications and programs.
4. The ability to request identity attributes with a known level of trust at all levels of infrastructure (Network/SDN, Router, Switch, Server, Application or within an application [identity escalation based on increasing risk]).
5. A unique [cryptographic] relationship to every entity-entity interaction [to eliminate credential theft / credential replay].
6. The ability to securely interact with a device directly [for example IoT over IPv6] without the need for a cloud service or other intermediary (device or service).
7. To support (where needed) post-quantum cryptography.

Conclusion

These high-level requirements need to form the foundation for the Identity 3.0 protocol and architecture; as well as the test(s) by which any reference design and any "technology demonstrator" needs to be judged.