

Briefing: Privacy

Why should I be interested?

Any identity ecosystem needs to strike a balance between usability, trust and privacy. The insatiable move to all things digital in a joined-up world puts the privacy of the individual at risk.

Strong identity is crucial if there is to be trust of individuals and entities on the Internet; strong authentication of that identity is also essential if those digital identities are to be kept secure and free from hacking and impersonation.

To maintain privacy, attributes of an identity should ideally only be held once by the authoritative source for that attributes, and be cryptographically secure, so only the identity that owns the attributes can assert them. This minimises the proliferation of attributes and minimises the risk of attribute aggregation – the ability to infer a unique entity from the collection of enough attributes about that entity.

For individuals, there are two key principles to ensuring privacy; first, the entity must be in total control of their own identity (agency & primacy) and second; entities must be able to segregate their digital lives into persona, ensuring that attributes linked to those persona are unique to a single persona – again minimising any risk of attribute aggregation.

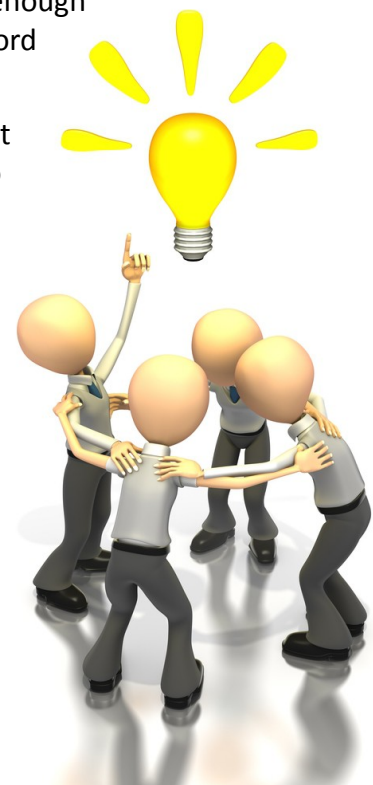
An increased level of trust also brings the potential for increased privacy; much of the current need to continuously re-enter details about ourselves is due to the requirement of third-parties to perform identity proofing to a standard they deem necessary to minimise their risk to an acceptable level (ignoring their need to gather marketing data), or to have enough information unique to that individual to be able to perform password and/or account resets.

By having an identity ecosystem with significantly higher levels of trust of the entities, and their attributes, and the ability of those entities to assert attributes about themselves from authoritative and trusted sources, so the information gathering need for third-parties is substantially reduced and in most cases eliminated.

Why should I get involved?

The Global Identity Foundation is a non-for-profit, vendor neutral organisation combining the identity requirements of numerous sectors of industry, as well as other interested parties, to define a consistent set of use cases for identity and from that a single set of requirements.

Building on the work of the Jericho Forum and many others, our aim is to further prove and expand the current draft identity ecosystem to a viable solution set of capabilities that would be implementable by anyone, anywhere, as an open-standard.



In this way, vendors can implement their piece of the identity puzzle, being able to rely on others to play their part, saving both money and time, with users able to bring their own single global identity (BYOiD) to all aspects of their digital lives; while users can be assured that using this single standard all the components will interact correctly while protecting their privacy and leaving them in control.

What does a future with global identity look like?

As an individual, imagine being able to take your single identity device (BYOiD), in a form factor that you chose to suit your lifestyle, that you anonymously purchased and use it to create a number of digital persona of your choosing.

The individual persona that you choose to link your digital identity to, in general will be the authoritative sources for attributes about yourself – for example a citizen persona will be the authoritative source for date-of-birth, place of birth, sex and citizenship – but nothing more.

Linking that same device to your credit card provider will provide a credit card persona with only your credit card details.

Identity proofing only takes place when a persona needs it, and only for those attributes for which the persona needs to be the authoritative source.

Using cryptographic one-way links ensures that while you can make assertions of your attributes from multiple personas, there is no way – starting from an individual persona – to go “back up your identity tree” and deduce either the individual entity or any other personas linked to that individual.



Imagine being able create an anonymous voting persona and enable voting from anywhere in the world. However in places in the world where voting is mandatory imagine still being able to prove you voted.

Privacy is inherent to the identity ecosystem being proposed, a design that starts with a totally anonymous root and places the control for linking that “Core Identity” to its various persona of its choosing.

What can I contribute, and what do I get back in return?

As a member of the Global Identity Foundation you have access to all aspects of the process, from the scenario workshops being held globally which will define the generic use cases; the distillation of those use cases into a set of identity ecosystem design requirements; all based around the concept of a user being able to have a single global identity (and identifier).

We envisage organizations will want their experts in the areas relevant to them to be actively involved, both to submit their requirements and influence the design, as well as to have advanced knowledge of how their products may want to evolve in the future or understand new products or offerings that they could develop.

About the Global Identity Foundation

The Global Identity Foundation is a not-for profit foundation constituted to first oversee the development and then maintain the core technology for the solution developed, together with its ongoing evolution.