

Briefing: Cloud Vendors – IaaS & PaaS

Why should I be interested?

When implementing an application or service using Infrastructure-as-a-Service (IaaS) or Platform-as-a-Service (PaaS), there should be a set of identity and connectivity options together with a de-perimeterised security model that meets, or preferably exceeds, what could have been achieved using a “traditional” (perimeter) model.

Implementing an identity based “entitlement” solution can deliver both security and flexibility without adding complexity, cost and the need to implement bespoke solutions. The optimal solutionⁱ is to grant access to the layers of the PaaS or IaaS service (from network through to granular data access) using “entitlement” – a set of business-driven access rules based on the identity and attributes of all the entitiesⁱⁱ in the transaction chain. In this way security is enhanced, allowing the business owners to define risk-based decisions about the access to system, application and data.

The quality of the entitlement decision is increased (and thus risk decreased) by the ability to consume strong identity and trusted attributes about the entities involved, from authoritative sources, in a globally consistent manner.

For cloud service providers; being able to use a standard set of identity and entitlement modules that are compliant to global standards will allow customers to simply and easily implement their cloud systems using those services.

Conversely, those building their services on IaaS or PaaS will be able to utilize a set of standard identity modules in the knowledge that displaying the GiD logo as part of their service gives their customers confidence that using their services will be simple, secure and privacy enhancing.

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?

Normally when implementing an IaaS or PaaS service significant planning needs to be undertaken on how the identity of the transacting partner will be undertaken, the level of risk with which the identity can be trusted, and the amount of identity proofing and life-cycle management that will have to be undertaken.

Imagine being able to dispense with most (if not all) of that and instead use a standard set of modules, simply defining a set of entitlement rules that match the requirements set by the business.

Consuming cryptographically signed identity and attributes from all the components in the transaction chain and combining them in a set of entitlement rules that matches the defined business risk, allows maximum flexibility for the business and minimises the need for ongoing maintenance unless the business requirements change.



When building customer facing solutions, the ability to consume identity from any entity that has their identity linked back to their compliant Global Identity Device, means that the identity of all the entities in the transaction chain can be quickly and simply assessed with known levels of assurance; starting with how the user is bound to their device. Should the transaction risk escalate these same standard modules allow further checks to be requested.

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

As a corporate 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.

i Cloud Security Alliance “Guidance v3.0” Domain 12 – “Identity Management, Entitlement & Access Management”
[www.cloudsecurityalliance.org]

ii Entities are defined by the Jericho Forum “Identity Commandments” as Users, Devices, Organizations Code & Agents