

Briefing: Cloud Vendors & SaaS

Why should I be interested?

The advent of Cloud delivered Software-as-a-Service (SaaS) brings new opportunities for businesses, especially in areas of collaboration, as the majority of SaaS services will be located outside of the corporate perimeter; thus enabling business to offer a wide variety of services to staff, mobile staff, business partners and customers without the need to tunnel them back inside their organizational boundary and the inherent security compromises this entails.

Currently SaaS providers have limited options for interfacing with external identity solutions and without bespoke solutions these are generally limited to authentication rather than identity.

Tomorrows SaaS services need to move to providing granular access to all layers of the service they offer, from network, through application and even to granular data access; and to offer this without adding complexity and cost. To achieve this an “entitlement” based solutionⁱ is recommended by the Cloud Security Alliance – a set of business-driven rules based on the identity and attributes of all the entitiesⁱⁱ in the transaction chain.

This entails consuming identity and attributes from a wide variety of sources thus improving security by making risk-based decisions about access to data and services; based on the identity and attributes of all the entities involved in the transaction.

Implementing such a solution realises not only an increase in security, but also provides simplicity and flexibility for customers of SaaS services, allowing them to simply configure many of the services they want to consume without the need to manage users and other entities over which they have little or no control.

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?

Imagine commissioning a new SaaS service and being able to specify a set of business-based rules about who (or what) has access and in which circumstances, with a wide ranges of identity choices and attributes at your command to select from; in the knowledge that by being able to select identity and attributes from their authoritative sources you will not have to on-board or manage the life-cycle of any users, their devices, or organizations which you do not control.

Thus, implementing an e-commerce SaaS service, you can request an authoritative source for delivery address as well as a signed payment assertion from the Credit Card organization together will an assertion of how well the customer was bound to their source of digital identity. Your risk can be managed, for example, by limiting the transaction value based on country, amount and binding quality or any other identity and attributes that you define.



Implementing a business-user to business-application is simply a case of on-boarding the organizational identity and those organizational attributes (relevant to you for defining access) that can be asserted by an individual user and signed by the organization that employs them.

In a pure business to business SaaS application (system to system), individual systems are still entities with organizational persona, exactly the same way a user would be; thus the interfaces, entitlement rule-sets and code are all exactly the same, and are fully interoperable and/or interchangeable.

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 Refer to 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