

Briefing: Phone & Mobile Sector

Why should I be interested?

The mobile and smart-phone world is at the centre of the Bring-your-own-device (BYOD) revolution; with many perceiving the smart-phone as the hub device that will marry personal identity, payments and access into a single device. Correctly implemented in a consistent, open and global manner, identity is the key to this happening in a way that is both secure and privacy enhancing.

The future smart-phone needs to understand who has picked it up, and in what context; enabling the device to control access to the data held within the device, be able to assert information about the device and its current user, as well as enhancing the user experience by better understanding the context in which the user wishes to operate.

The phone industry is already exploring many of these aspects, such as;

- Phones having multiple persona based identities allowing the mixing of personal and professional sources of data, such as e-mail and contacts, e.g. Blackberry's "Balance".
- Extending the use of trusted execution environments at the hardware level such as Intel's IPT and ARM TrustZone or the TPM chip found on corporate grade laptops and tablets.
- Future phone operating systems using a hypervisor layer to provide secure virtual persona's or special hardware for secure containers such as the Samsung KNOX platform.
- Implementing enhanced security to attract wider corporate acceptability for BYOD.
- Mobile wallet and other functions moving to mobile devices but limited in the transaction value; with better security and identity critical to enable higher value transactions.

Correctly implemented, the smart-phone will likely be the delivery mechanism of choice for identity functions, such as re-mixing of identity attributes, caching cryptographic assertions and providing a universal access device; with secure (high value) payments, access control to buildings, user log-on to computers, access to your house, car and many more applications that are viable once this device is linked to a source of strong identity.

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 that picking up your phone causes it to automatically authenticate you and validate any of your personas on that device (personal, corporate etc.) against the your (single) Bring-Your-Own Identity (BYOiD); with each separate persona having distinct rules for authentication. So simple device possession may unlock the personal persona whereas unlocking a corporate persona may require that the device has seen a biometric verification in the last 30 minutes, or even in real-time.

Giving the phone to a friend to make a call would automatically lock the corporate persona, and thus data, email and contacts (a rule defined by the corporation) but the personal email, contact and photos can remain unlocked in a rule defined by the individual who owns the personal persona.

As both the corporate and personal persona have their own individual cryptographic certificates, data on the device can be separately encrypted together with rules about how long data can be cached, thus enabling a BYOD environment that is both flexible and secure, with the security transparent to the user of the device.



With the phone linked to a source of strong identity and able to assert that it's currently in possession of a particular person (to a defined level of trust); higher value transactions can be enabled; with the third-party having full visibility of how the user to device linkage was made, as well understanding the capability of the authentication device, thus enabling a far richer risk calculation to take place around the transaction.

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.