

Briefing: Banking & Finance Sector

Why should I be interested?

The banking and finance sector are under attack from all kinds of fraud, annual figures for card fraud alone are in the region of 30bn US\$ per annum. The root cause for most of this fraud is the same; there is no current, practical, global, standard method of linking an individual to the card or account with a known level of certainty.

Chip & PIN has improved matters greatly but only guarantees the possessor of the card knows the PIN not that they are the card owner; and still leaves gaps for the criminals to exploit¹ such as distraction thefts, shoulder-surfing, spy cameras on ATM's, social engineering, fake web-sites, and viruses designed to steal banking credentials to name but a few.

Similarly, on-line transactions suffer from fraud, and while American Express SafeKey, MasterCard SecureCode and Verified by Visa work to combat fraud, all suffer from a high level of user password failure leading to weak methods being used to automatically re-set the password.

Banking web sites, suffer from an inability to positively identify the user, with numerous authentication methods in use to confuse the users of such sites and mobile banking apps now adding to the complexity.

PayWave and PayPass contactless cards and the advent of Contactless/NFC payments via cell phones now allow (low value) transactions to whoever possesses the card/phone with few guarantees about the linkage to the account owner.

Correctly implemented, linking a single authoritative source of strong identity with a known and guaranteed linkage between the person and all the devices in use, together with trusted attributes about the transaction has the potential to eliminate most forms of fraud in common use today.

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

¹ <http://www.financialfraudaction.org.uk/Fraud-the-Facts-2012.asp>



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 being able to walk up to an ATM and being able to verify yourself using your own single global identifier that you had previously registered with the bank. Or use that same identifier to authenticate to a banking or credit card app inside your cellular phone, but one that is intelligent enough to recognise and understand the type of device being used and use its inherent features to request further verification (or re-verification) when the transaction risk-profile demands it.

For contactless payments using a smart-phone app, the authentication to the device assures that the person paying is actually the owner of the account, reducing risk and allowing significantly higher transaction values to be permitted.

When paying for a web-based transaction, use that same identifier to make the transaction but assert a one-time signed payment for the amount rather than hand over your credit card number and details that today can then be stolen and exploited.

With no PIN² and no passwords to remember there is nothing to steal, and no password resets required as it's the users device (not the Bank's or Credit Card



companies). Organisations can make the risk decision about whether to proceed with a transaction based on understanding the risk-profile of all the components in the transaction chain, not just a few of them – significantly reducing and in many cases eliminating the opportunity for user error, fraud and criminal activity.

In addition the customer's ability to use the same device to assert their citizenship details ensures banks meet "Know Your Customer" (KYC) regulations, with the guarantee that the same person initially verified under KYC is then the only person operating the account.

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.

² Device dependant