Paul Simmonds – Q & A

Q1. Here is your chance for an elevator pitch - what is the Global Identity Foundation?

PS. The Global Identity Foundation provides a vendor and government neutral environment to develop an open, single, extensible and standard for identity. Our goal is an open solution that can be implmented anywhere and by anyone.

The concept behind it is one of "Bring Your Own Identity" (BYOiD), starting with a totally anonymous root to your identity that you can then expand, just as humans do in real life, with personas containing attributes from their authoritative source; in this way you end up with a very powerful solution that puts the owner in control, solves many of the privacy issues and can expand globally.

Q2. The Jericho Forum began work on identity and owning it; is this a follow-on from it?

PS. Yes, the foundational work was laid in the Jericho Forum "Identity Commandments" and the work that then followed; looking at what form a Jericho Forum compliant Identity Ecosystem could take. To our surprise, turning identity "on its head" and starting with an un-trusted root solved most of the problems that have caused previous identity initiatives to fail.

Q3. You are quoted as saying this work radically changed your perspective on Identity, can you tell us a little more?

PS. Yes, I went into the Jericho Forum work on Identity with a preconception around identity, based on 30 years of "this is how we do it with computers", thinking that any solution was based around being in control of the "root" of an identity. The work we did turned my thinking around 180 degrees, as I, and others, realised that only with a totally anonymous root to an Identity can you have an eco-system that will scale globally.

Q4. One of the key issues for identity online is that people have many identities across huge amounts of websites and applications, why is this?

PS. This is an issue of "locus of control" – put simply, the only identity they trust is one they have created validated and that they manage; from that it's a downhill slide to everyone needing to manage their own identity store on not trusting anything they don't create.

Companies try valiantly to authenticate to a single system or put kludges in such as "Reduced Sign-On" – there is no such thing as "Single Sign-On" – but these are "band-aid" solutions not addressing the fundamental issues with authentication – let alone the wider issues with identity.

Q5. Why do they not authenticate me as a user – surely the technology is there to know who I am and recognise me by applications I use regularly?

PS. Yes, there are lots of tricks being used to infer who you are and authenticate accordingly, but these are all custom developments. Do you see SPAM decreasing, or impersonation fraud decreasing or global credit card fraud – currently at about $30bn per annum – decreasing? All these are still rampant because there is no standard way to identify, to a known risk level, all the entities and attributes in a transaction chain.

Q6. We have seen banks roll out authentication tokens which offer strong security; do you think that they are not being encouraged to be used for other applications?

PS. This is back to the problem of "locus of control" – how much to the trust someone else's token. With any current token the only thing you actually prove is the possessor of the token knows the PIN; as the provable linkage between entity and device is generally zero.

This is only marginally better than passwords and the banks augment this with lots of other "magic"; attributes about you as a customer to ensure it's you. This is proprietary and the risk is exclusive to the financial transactions taking place and would not scale to risk calculation in other businesses.

We know that if you were able to assert the trusted identity and attributes of all the components in the transaction chain then the recipient could make a much better risk decision about whether to transact.

Q7. Can there ever be a time when a single login can be securely used across the internet?

PS. Our vision is that you should be able to reuse your single (electronic) identity to log-in to any site you need to, without the need of a username or password, and be able to assert a set of trusted and verifiable attributes to support the transaction you are trying to undertake.

Q8. It has been said by analysts that identity management and access management should be separated, what do you think of this?

PS. Yes, definitely, an identity eco-system should be able to share identity and attributes with access system that needs is and an access management system consume identity and attributes from multiple sources. Unless you separate them you end up repeating the old paradigm of all users needing to be in the one identity system.

This is even more critical when you move to cloud computing and is why this concept is enshrined into the Cloud Security Alliance's "Guidance v3" document.

Q9. It has also been said (by Neira Jones among others) that "identity is the new currency". Do you think that businesses and those who "own" our identities are aware of this "value"?

PS. Yes, on two fronts; first, those companies who can take advantage of the identity and trusted attributes of all the components in a transaction will be able to make larger value transaction with lower risk – opening up new markets and business opportunities while reducing fraud and losses.

Second; people are starting to wake up to the fact that their identity and attributes has a value, not only to their own privacy but also as data to companies; the more accurate the data, the more value that it has. So having attributes of my identity asserted once and from an authoritative source means I maintain my privacy and under my control have more opportunities to realise the value of my information.

Q10. What about biometric authentication, is that the future or is it too easily spoofed by hackers keen to prove their capabilities (such as with the TouchID facility on the new iPhone)?

PS. Yes and no; as a security professional the only place I want my biometric information stored is within a device that I have 100% control over. However biometrics will be key to understanding the level of immutable binding between person and device, and therefore the associated risk factor.

We advocate that any identity ecosystem should be capable of accepting any level of binding from zero (no-binding) to 99.99% (probably DNA level binding) and everything in-between, communicating that binding level to the transacting parties to use in their risk calculations.

Q11. Does the future of authentication and identity lie with the application/website or user?

PS. The only thing that scales globally beyond companies and countries is user-centric identity. Mobile devices, applications and websites should simply be consumers and processors of that identity.

Q12. Where would you like the Foundation to be in twelve months time?

PS. In twelve months I'd like to see that we have successfully communicated why turning identity on its head is a viable solution and have a critical mass of global companies working together with us in a neutral environment to refine a solution that meets their needs, and the needs of users everywhere.

Q13. Why a global not-for-profit foundation?

PS. Quite simply for this to be successful this needs to be a global initiative with all the key global players collaborating with no preconceptions or industry bias in the same neutral and safe environment – the work must not be constrained by the aspirations of any national government, or the profit motive of any one corporation.

Anyone should be able to implement the solution, or leverage the Identity from the solution within their products thus prohibiting monopolization of the technology.

The aim is a single solution, acceptable to all individuals, at a cost all citizens of Earth can afford.

Q14. Why will you success where others have failed?

PS. First by being inclusive and gathering global experts together, funding their involvement if it is required to ensure global applicability and global involvement.

Second; by being a single, independent organization, looking to maintain the purity of a clearly and concisely articulated goal, and delivering a pragmatic solution, while operating by consensus to ensure no one person or organisation can dominate.

And finally; by ensuring an open solution/standard is produced that can be used anywhere and by anyone.

Q15. So what will a future with a BYOiD look like?

For people; accessing a site, an application or using an item of hardware with the GiD Logo on it will let them know that they can interface safely and securely, and most importantly, simply, easily and with privacy under their control – all without needing to create another account, or manage yet another username and password.

On the other side, vendors can add the GiD interface free of charge into products, web-sites, apps, and devices in the knowledge that it will enable a standard set of interfaces, allowing a more informed transactional risk decision to be made, interfacing with other entities in a standard manner, using code and methods maintained by an industry-neutral body.

As we get asked more questions this FAQ will be updated.
Last Updated December 2013

About Paul Simmonds

Paul is the CEO of the Global Identity Foundation, and previously was the Global Chief Information Security Officer (CISO) for AstraZeneca, Global CISO for ICI, Head of Information Security with a high security web hosting provider and Global Information Security Manager at Motorola.

Paul is a co-founder and was Chairman of the Jericho Forum, established in 2003, and regarded as one of the leading think-tanks on Information Security. He's been awarded both "Chief Security Officer of the Year" and "Best Security Implementation" at the SC Magazine Awards and is twice listed as one of (the US publication) Network World's "most powerful people in networking[1]".

Paul sits on the global advisory board of a number of global companies, as well as the Executive Advisory Board of ISSA UK. Paul is also one of the three global editors of the Cloud Security Alliance "Guidance - Version 3" document.

Paul's varied career has included Electronic Countermeasures, Theatre & TV Lighting, designing North Sea Oil control systems, network management for JET (Nuclear Fusion Research) and setting up a number of commercial radio stations.

Paul's linked-in profile is: http://uk.linkedin.com/in/psimmonds

About The Global Identity Foundation

Building on work from the Jericho Forum and others; the Global Identity Foundation provides a vendor and government neutral environment to develop an open, single, extensible and standard for Identity.

Our belief is that for competitors to work together, with no preconceptions or industry bias, there needs to be a neutral and safe environment that operates with a global remit constituted as a not-for-profit organisation.

Our aim is to get all the right people, the key global players, academics and other experts, into the same neutral environment, sponsored either by their respective companies, or if necessary directly by the Global Identity Foundation with the aim of delivering a pragmatic and viable solution designed to work globally, and that will equally be accepted by Governments, corporations and the citizens of the globe.

To be successful this needs to be a global initiative, not constrained by the aspirations of national governments, or the aspirations of any one corporation.

Our goal is an open solution/standard that can be used anywhere and by anyone; with anyone able to implement the solution, or leverage the Identity from the solution within their products thus prohibiting monopolization of the technology.

The Global Identity Foundation's website is at: http://www.globalidentiyfoundation.org

Acknowledgement: With thanks to Dan Raywood who provided some of the initial questions

[1] http://www.networkworld.com/power/2005/122605-power50.html?page=6#simmonds
http://www.networkworld.com/power/2004/12270450most.html?page=4