**Some thoughts and observations from a specialist in identity practice**

My average day is spent providing feedback and advice to anyone touching the identity space. I carry out assessments on services, processes, transactions and systems to identify identity-related risk and then advise how this might be mitigated. I do this predominantly, but not exclusively, in the New Zealand context and for government.

The following thoughts and observation apply equally to the draft paper on Vectors of Trust as they do to the NIST Special Publication 800-63-2.

***AUDIENCE***

Who do you want to use this document? What is the goal? Do you want to reduce identity fraud or do you want to reduce identity fraud in the digital channel? And how long do you want to reduce it for?

I work with organisations and individuals. In both cases the identity problem they need to solve is rarely just a digital one. Standards and guidance currently tend to come out of the online space and with that come the following issues:

* They are difficult or impossible to apply to the same service offered via another channel. This can impact customer experience and also mean weaknesses appear in non-digital channels. In the worst case it can result in flawed approaches and the targeting of offline channels for fraud.
* They are written for the technology of the day. As technology changes and evolves gaps quickly appear and they become dated.
* The owner of the risk of a service (whether it be the provider, the relying party or the individual subject) is rarely an IT specialist and struggles with understanding if a risk is mitigated when the solution is supplied in technical terms.

Based on the matrix below, there are insufficient standards and guidance being developed in quadrant 3. My view is, without developing the foundation or fundamental level, all development at the other levels is at risk of being flawed and/or proprietary (i.e. lacking interoperability.)



For example, by my reading NIST is currently running along 1 and 2. VoT draft starts out in 1 and 3 but jumps into 2 at clause 5. ISO/IEC 29003 has moved from 1 and 3 to more firmly in quadrant 3, ISO/IEC 29115 is currently in quadrant 1.

***VOT – THOUGHTS CLAUSE BY CLAUSE***

2.1

The identity model is for a particular scenario where an entity is either acting as an identity provider or using an identity provider and this is not strictly the case, especially at lower levels.

The real-world example jumps immediately to an example for a higher level that does not work in a P1 scenario.

2.2

Second paragraph ‘An important goal for this work is to balance the need for simplicity… with the need for expressiveness’. In that case delete the first paragraph, as it will only be of interest to mathematicians.

I agree with whoever stated earlier in the conversations that Vectors of Trust is not a good description. I have been using the term Expression but don’t doubt we can come up with something better before publication.

3

Aside from issues with the term Credential, here it states credential binding as one of the core components but 3.2 is headed Credential Management. In my view neither is entirely correct. Credential Management involves more than what is needed for this aspect, but Credential Binding is insufficient. We have a ‘thing’ and a linking process and they need to be considered together and separately depending on where in the identity management system you are building, operating, reviewing etc.

3.1

Don’t forget to tie the set of identity attributes to the claimant. Binding occurs at two points firstly when establishing an identity and then when issuing a credential. This harks back to the narrow scope at 2.1

3.2

As mentioned above there are two pieces here the strength of the ‘thing’ (key, token or other rose) and the strength of the binding to the identity subject.

3.3

Thanks for labelling and defining this as it has been a question mark for some time in my FRAGGLE. See later in paper.

4

As an editor for ISO/IEC 29003 – Identity Proofing and having spent many hours with multiple jurisdictions thrashing out levels of proofing – there are four (including the level for no proofing) anyone who wants LoIP 4 or P4 is splitting an unnecessary hair. We have pulled this matter every which way but loose and gone up to 5 & 6 but invariably, and in at least three separate sessions, come back to 0, 1, 2 and 3. The VoT paper describes them in a different way but the number is right.

I would suggest that for P2 the description is too broad as proofing by whatever mechanism has many levels and the level is what is important. At P2 the identity must exist corroboratively i.e. has been used in other contexts.

I like the reference to legal or contractual in P3, however, this is more about the driver for the level not the level itself. At P3 we are essentially talking about official/authoritative identities.

As is often missed, there is no explicit mention of the degree of ownership. As this is the aspect that prevents identity theft, it should not be left to being inferred only.

The C range is all about the strength of the ‘thing’. A relying party should also be aware of the strength of the issuance process and the degree the ‘thing’ has been linked. They are also based on a single delivery channel. See comments on Audience.

The A range is also based on a single delivery channel. See comments on Audience.

5

Again this is limited to a specific channel. It also assumes a single type of implementation – the identity subject provides an identity credential and RP decides based on VoT whether to accept. What about where an organisation tenders their identity verification of customers. It would be determined as part of the agreement prior and the Identity Provider will be expected to fulfil the requirement. The latter is at this time, I believe, the more likely scenario.

Paragraph 2 is spot on and is the problem with LoA.

5.2 – 6.1

Channel and technology specific.

7

See comments for 5 and 5.2 – 6.1.

Overall

If the proposal is to position this as an ubber framework then it needs to be able to apply to a much wider range of identity processes and channels.

As an example I have attached the framework I have been attempting to evolve.

If the intention of this draft VoT is to be something else then this needs to be expressed clearly at the outset to save people trying to apply it where it will not fit.

***FRAGGLE***

The diagram below (which is still evolving) is a framework I have been slowly evolving using a combination of my own observations, conversations in VoT and conversations at ISO. For the time being this is referred to as the FRAGGLE; that is **FRA**mework for **G**athering **G**eneral **L**earnings and **E**piphanies.



The key features of the framework are:

* Clear risk based approach
* Each Lo represents a measurable element of an aspect of identity management.
* Each Lo in rows 3&4 are mutually exclusive and therefore can have their own scale. Note: Based on experience, the individual components of LoCM become important when assessing the capability of an existing system, in that I have rarely met a system where both aspects are of consistent quality.
* The framework allows for different mediums or channels (face-to-face, online, by phone etc.) for delivering identity processes.
* The framework recognises that there are common and specific elements that apply when delivering identity processes across multiple channels.
* The framework recognises that there is a difference between trust in Identity Assurance (LoIA) and trust in System Assurance (LoSA).
* The expressions of LoIA and LoSA can grow as the various Los mature, as long as there is mutual understanding of which Los are included in the expressions.
* It recognises the difference between aspiration (Goal) and reality (Actual).
* Goal and Actual can be applied to both the system and an individual instance of an identity transaction. E.g. where a particular applicant has failed to meet some aspect of the required process, their LoIA (Actual) could be less than the LoIA (Goal) and thereby limit or deny their access to service/s.?
* Capability assessment may be carried out internally. However, if done by independent parties it will provided the foundation for recognised trust marks.

**Risk**

It is all about mitigating risk and there are two aspects where risk appears in the framework and the measures for each differ.

Overall we are looking at the risk that:

* A person isn’t who they claim to be – false or stolen identity (identity proofing)
* A returning customer isn’t that same as the original customer (credential management)

The categories used in the risk assessment phase include financial impact, release of information, injury, embarrassment, distress and reputation etc. These differ from those used in the design and capability assessment of levels phases. These include categories such as existence, theft, manipulation etc.

**Gaps**

As mentioned earlier this is still a work in progress and as such there are a number of gaps that I have identified for more work. These include:

* Refining of terms – Key, Token and Credential. Resolution is needed on the relationship between Key (token) and Credential. NIST defines the difference most clearly however when it comes to ‘practice’ the lines become muddied with Credential Issuance and Management being more often processes of Keys. While the framework is generic the scenarios of ‘keys that are also credentials’, ‘keys that unlock credentials’ and ‘keys that are just keys’ will need to be dealt with.
* All Los need to be defined, labelled and have measurable scales set. See a draft of ISO/IEC 29003 for an example for LoIP. Existing work by ISO and NIST could be used to fill out this framework relatively easily. However there are a number of elements that do not lend themselves to explicit measurement and read more as considerations. There needs to be a way to capture ‘considerations’ within the framework, hence the purple shaded box.
* Guidance similar to PIA methodologies could be developed for the undertaking of Assessments, noting that the rigour of the assessments is a key element of trust. I am working on revising the identity-related risk assessment process we currently use in NZ to align better with this framework having also identified other issues with it. I then intend (time permitting) to look at Capability Assessment. These may or may not then translate into Standards.
* Elements such as those related to a specific implementation, where they cannot be expressed in terms of a reusable scale, may need to be gathered as ‘considerations’. There may need to be an aspect of the framework that can capture this and quantify it in some way.
* An explanation may be needed as to how this framework fits with federation.