Suggested Model of Trust

Goals

- Score the responsibilities of an Identity Provider (IDP) equally along the axes that matter to the Consumer being authenticated and to the Relying Party (RP).
- Allow commercial services to evolve to meet market needs for shared services that meet your model of trust.
- Support the development of Open Standards for any of the pathways between the IDP and the RP and between the Consumer and their Chosen IDP
- Ensure the qualities of Security, Identity, Privacy, and a Consistent User of a RP’s Service

The Four Vectors that Constitute Level of Trust

Level of Assurance

MEASURES IDENTITY

Level of Assurance (which could also be called Level of Establishment in order to have LOE be a different acronym than LOA) is the measure of the certainty of the validity of the User to which the account is
given. It can be measured before the account is granted (as in Identity Proofing) and then continually as the account is used (as in identity analytics for persistent vetting).

The valuation of “assurance” may be different within any particular realm of human identity – a scoring of the assurance of an account in a social setting may be based on usage and social contacts, but also include the degrees of separation from the Account Holder to another User they are interacting with. There are 8 realms of identity to consider, including legal, social, professional, etc.

Level of Protection

**Measures Security**

*Level of Protection* measures the lengths to which security operations have made the end-to-end system impenetrable and the credential retain original validity. It is the domain of Cybersecurity expert evaluation.

Level of Authentication

**Measures Consistency of the User**

*Level of Authentication* is the measure of confidence that the current User of the Service or Transaction is the original person to whom a credential was issued. This measure has been the focus of most Internet use cases so far, with mechanisms such as Touch ID from Apple introducing alternatives to passwords for authenticating users. This focus is largely because the repeated account creation process of self-attested attribute entry has been accepted as sufficient, even though the *Level of Assurance/Establishment* that services require is not met.

Level of Control

**Measures Privacy**

Adherence to privacy principles, obtaining consent, privacy policies, and consumer control of attributes are all measurable within *Level of Control*. It is a measure of the Consumer’s protection, which could be trustmarked, measured, or assessed. In any environment where Consumer control is very low, Consumers may respond with their own protection measures of privacy – pseudonyms, deliberate error, etc. Returning control over identity to the Consumer will help increase accuracy as well as privacy.

**An Example of Valuing Vectors Differently within a Particular Framework**

Consider the example of a social network with an API ecosystem where Service Providers (e.g. Apps) in the ecosystem rely on the identity provided by one or more social account IDPs. Each particular Service Provider within the ecosystem may have different requirements in these 4 areas of Trust in their transaction.

A Shared Economy Service and its Users may have a specific mix of the 4 Levels above that truly matter to their interaction and the transaction. The Service Provider assesses their risk exposure for the transactions that they want to enable online. *Excluding* ability to pay, which is not an identity issue, and
utilizing a None, Low, Medium, and High ranking system for simplicity, the mix may look something like the following:

- **Low Level of Assurance/Establishment**, based on a social-account scoring that indicates whether the account is new or fraudulent, and a reputation system
- **Medium Level of Authentication**, because the Shared Economy Service Provider needs to know that the assured account is not being reasonably used by another party
- **Medium Level of Protection**, because the credentials do not require high protection end-to-end
- **High Level of Control**, because Consumers truly do not want to be tracked utilizing a Shared Economy Service that can be anonymous, provided that reputation and payment keep the transaction solidly reliable and safe

Since these parties operate in a social framework, the scoring and valuation of items like Reputation and Social-Account Reality Score is the province of the Social Trust Framework provider. The Trust Measurement System should support their ability to provide scores that are meaningful to their parties.

**Note on Ability to Pay**

The level of risk in payment for a service and the absorption of that risk throughout the system are well covered in today's credit card transactions. It may, therefore, not be a scored item in the new NIST 800-63-2 guidance. It can be left to scoring of the credit and ACH providers.

**Suggestions on “Levels” that Matter to RPs but can be understood by Consumers**

**Gradations**

It is sensible to have four to five gradations publicly available to Service Providers and that the gradations are able to be understood and fulfilled by Consumers.

One or two additional levels of Security and Top-Secret security clearance should be available above and beyond the base gradations, but not typically publicly available for online interactions. For instance, an administrator may have to prove Security cleared Level of Trust in order to perform system-wide operations.

**Naming**

Naming of Levels of Trust must be understandable to the widest population of potential users. Naming could be left to the domain/framework in order to support flexible differences between calculation methods, particularly in the 8 domains of identity.

**Capabilities for Add-On Layers on Top**

The framework must provide for the extensibility of additional “Levels of Y” that may apply in a particular identity domain. Scoring another level and normalizing it into the calculation can be performed by the Framework Provider as an additional feature that they assure within their domain.