CIWG Consumer IdentityTopics of Interest

Based on the results of the survey that was taken of WG participant's interest in consumer identity topics, I've summarized these topics, and added (*in italics*) some additional comments and possibilities. Additional comments and suggestions are needed from WG participants to expand on these topics.

We already have a draft set of use cases for consumer identity. Mashing the existing use cases against these additional topics of interest will help to further define and guide the WG's output.

The WG's final output will only be as good as the contributions made by individual volunteer WG participants. If you are a WG participant, please consider adding your own comments, suggestions, etc., to this list. You can either do that below, or you can just post them to the Consumer Identity WG mailing list (wg-consumer-identity@kantarainitiative.org).

1. Strong Authentication Methods

- *PKI (certificates and private keys)*
- *One-time passwords*
- *Other*

2. Privacy

- *Privacy policies of Identity Providers*

3. Business Value of a Consumer Identity

Let's assume we're actually referring here to a consumer's "digital identity." We'll use Wikipedia's definition of "digital identity" as referring to "the aspect of digital technology that is concerned with the mediation of people's experience of their own identity and the identity of other people and things. Digital identity also has another common usage as the digital representation of a set of claims made by one digital subject about itself or another digital subject."

A consumer digital identity refers to a digital identity used by a consumer; ie, an individual seeking to obtain goods or services online.

3.1 Value of a consumer's digital identity to a Service Provider / Relying Party

- *Provide a high-value service to a consumer, dependent on knowing*:
  - *the consumer's "true" identity, with high confidence, or*
  - *other specific personal attributes about the consumer (e.g., over 18 or 21, membership in specific organizations, etc.), or*
  - *that the consumer is authorized to do certain things; e.g., make payments from a certain bank account, etc.*
- *Prevent fraud by preventing false claims of identity or authorization, etc*

3.2 Value of a consumer's digital identity to the Consumer

- *Obtain a high-value service from a Service Provider*
- *Prevent others from using the consumer's identity*

3.3 Value of a consumer's digital identity to the Identity Provider

- *Earn money by providing identity-related assertions to Relying Parties on behalf of the consumer, and/or providing digital identities to consumers*
- *Enhance the value of an associated service by providing identity-related assertions and/or digital identities to consumers*

3.4 Business case for providing stronger protection of consumer identity (js)

- *One of the problems with the current business model is that Relying Parties (Service Providers) who often serve as their own Identity Provider do not incur the full cost of identity theft. While they may be liable for the direct cost of items purchased using a stolen identity, they are not liable for the additional costs incurred by the consumer whose identity has been stolen to reclaim his identity. These include both direct costs (mailing, copying, filing forms) and indirect costs (time expended notifying parties and reconciling records).*
- If we could come up with a way to model these consumer costs, we would gain a better sense of their magnitude.
- We could then work to define a business case (perhaps regulatory language) to add this liability to the party who failed to provide adequate protection to the identity. This would be a more fair allocatoin of cost and may serve as an incentive to RPs and IPs to provide better custodianship of customer identity information and perhaps even incent them to avoid collecting certain high-risk data.

4. "Form Factor" Technologies

- *Consumer digital identity and smart cards/certificates on USB tokens*

- *Consumer digital identity and smart cards/certificates/one-time passwords on mobile devices*

5. Usability Issues

- *Portability of strong authentication methods*
- *Tradeoff between ease-of-use and better security*
- *Consumer acceptance of strong authentication methods and form factors*
- *Personalization and customization of consumer digital identities*
- *Usability of open identity initiatives*
    - *OpenID*
    - *Information Cards*