WG - Consumer Identity

This Work Group operates under the Kantara Initiative IPR Policies - Option Creative Commons Attribution-Share Alike

CHARTER | JOIN THIS GROUP | SUBSCRIBE | MAILMAN ARCHIVE | GOOGLE ARCHIVE

Consumer Identity Work Group News & Updates

Blog stream

Create a blog post to share news and announcements with your team and company.

Introduction

The purpose of the Consumer Identity WG is to help ensure that emerging Internet-based identity infrastructures are designed and implemented in a way that can help prevent consumer identity theft and other identity-related fraud. CIWG does this by proposing specific requirements, recommendations, guidelines, and policy positions that foster the implementation and adoption of high assurance identity-related claims (ie, sets of identifiers or other attributes) that can help prevent identity theft and other types of identity-related fraud affecting consumers and service providers. CIWG also seeks to understand the feasibility issues pertaining to large-scale deployments of these capabilities.

Subject to available resources, CIWG will create reports, whitepapers, and/or other documents that describe how emerging identity technologies, protocols, frameworks, laws and regulations, etc., can be leveraged to: (a) enable a service provider to know, with high assurance, the identities, related attributes, or authorization status of individuals with whom it engages in high-value online transactions, without jeopardizing the privacy interests of those consumers; and (b) enable individual consumers to prevent others from impersonating them in high-value, online transactions.

Some Requirements to Support High Assurance Consumer Claims

As a first step towards this goal, the CIWG Interim Report, released in October 2010, addressed the problem of harmful identity theft and other types of identity-related fraud that affects consumers. The Interim Report highlights several issues that become important when considering how to design and implement an identity infrastructure to support high assurance identity-related claims in a way that consumers will find easy to use, that will maintain their privacy, and that will prevent others from “stealing” their identities in order to conduct activities that can be harmful to the consumer.

In response to the issues raised in the Interim Report, we propose several high-level requirements for an identity infrastructure. These are:

- expand the definition of “high assurance” to include claims other than those consisting strictly of personal identifiers;
- provide consumers with an optional visual representation of these claims to increase usability and ease of claims management;
- eliminate potential service interruptions resulting from unavailability of the identity provider by establishing a way to transmit high assurance claims to a service provider / relying party without requiring that the relying party interact with the identity provider each time;
- provide better consumer privacy protections to prevent identity providers and others from tracking and correlating usage of a consumer’s high assurance identity-related claims;
- provide strong authentication technologies that are usable by consumers;
- deploy the identity infrastructure in a way that satisfies consumer needs for ease of use and portability of credentials;
- establish or support policies to discourage service providers / relying parties from demanding high assurance identity-related claims for access to low value services.

Supporting Technologies

Although an identity infrastructure could satisfy these requirements in more than one way, an identity infrastructure that incorporates the following technologies could serve as a strawman for further discussion and evaluation.

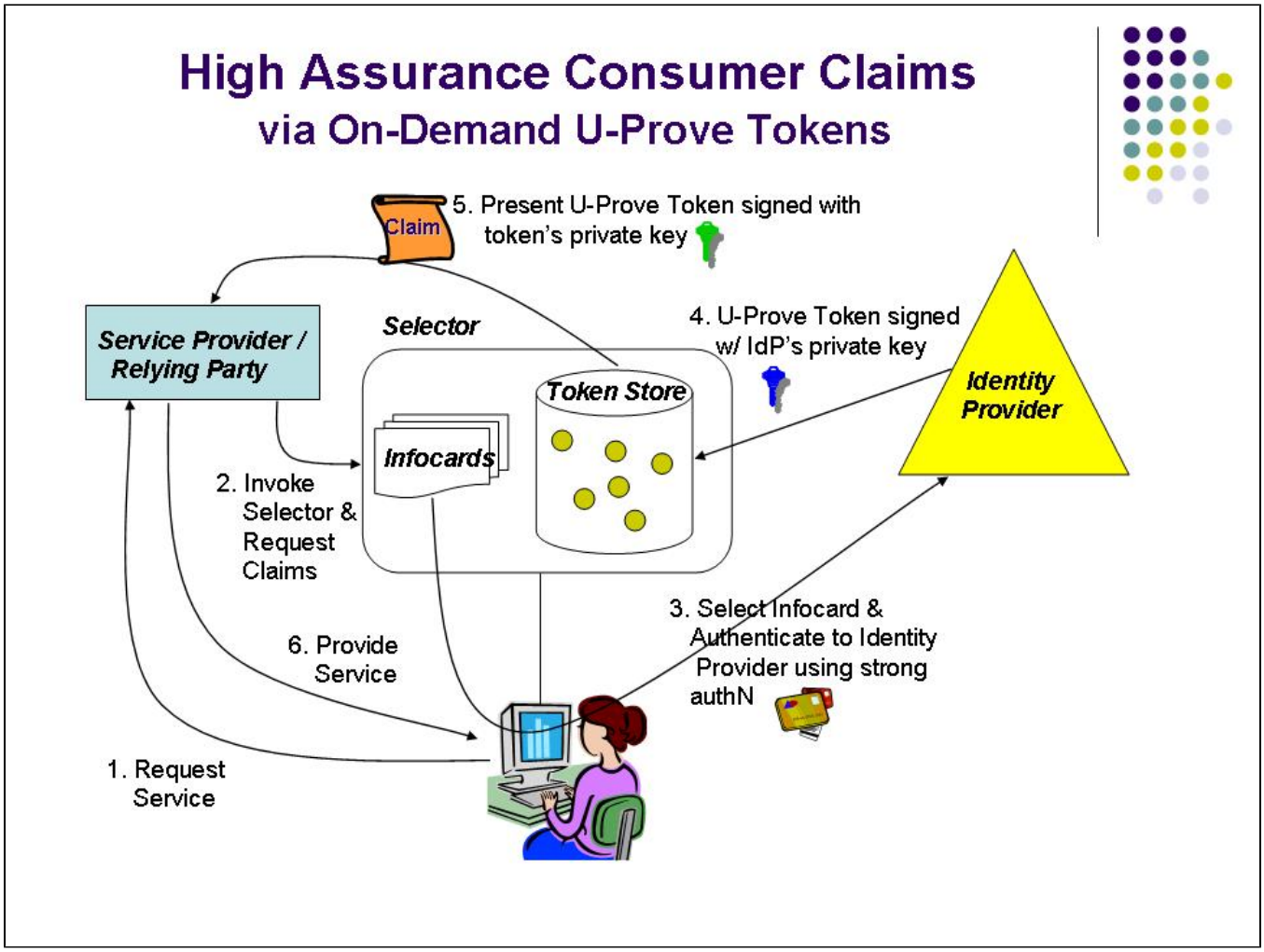
- “Open identity” technologies that support high assurance claims, such as Information Cards or beefed-up OpenIDs (or some analogous credential).
- U-Prove technology that supports both on-demand tokens as well as long-lived tokens. On-demand tokens are used to transmit claims from an identity provider to a relying party (via an active client) in real-time, while long-lived tokens are generated ahead of time and then used when needed to transmit claims without requiring interaction with an identity provider. The use of long-lived tokens would allow service providers to process consumer claims even when a trusted identity provider is unavailable.
- A selector or active client that acts as an online repository or “wallet” to store Information Cards or OpenIDs, as well as to store and manage U-Prove tokens. The selector / active client would also provide consumers with a visual representation of identity-related claims.
- Strong authentication technologies such as public/private keys, one-time passwords, and possibly others that enables identity providers to have high assurance that the claims they issue are in response to a request from the consumer to whom the claim pertains.

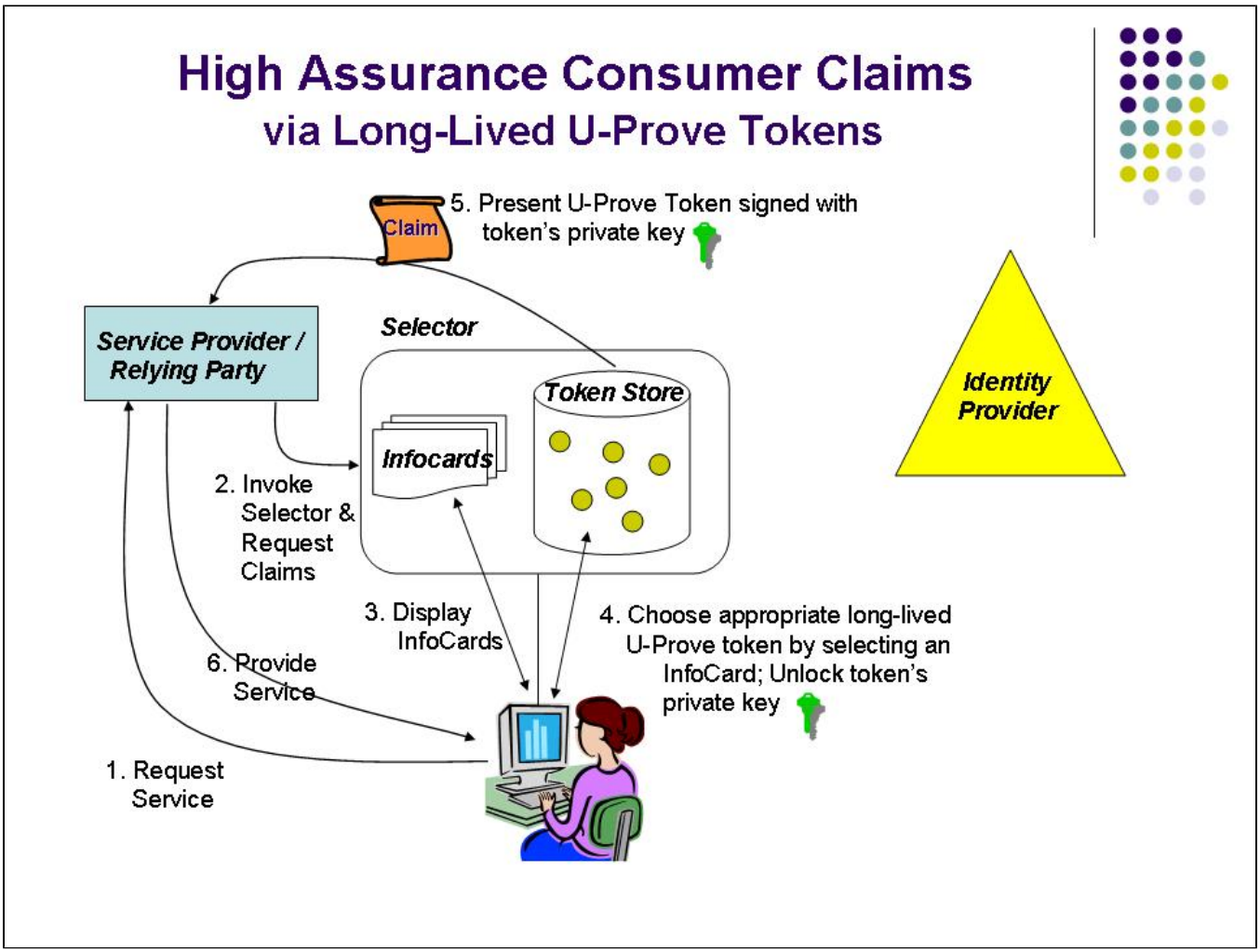
- Smartcards and PC-based Trusted Platform Modules for the deployment of selectors / active clients and other authentication technologies, as well as for the private keys that allow consumers to make use of U-Prove tokens to transmit trusted claims to relying parties. Smartcards implemented in smartphones, USB dongles, or other mobile devices may be more usable from a consumer standpoint for online transactions than smartcards implemented as physical cards that require a card reader in order to be used.

Subject to availability of resources, it is CIWG's goal to further refine the above requirements, as well as to provide more specific or detailed recommendations for various technology alternatives.

High Assurance Consumer Claims with U-Prove Tokens

The following two diagrams illustrate how consumer identity-related claims can be used with either on-demand or long-lived U-Prove tokens. It is assumed that trust between service providers / relying parties and the identity providers that issue verified claims is based upon the adoption by these parties of an appropriate trust framework.





Chair:

Bob Pinheiro,
Robert Pinheiro Consulting [Feb 2010]

Roles of Leadership

- Read the roles for Leadership

Teleconferences:

- Dial-in Details
- Skype: +99051000000481
- US Dial-In: +1-805-309-2350
- Conference ID: 613-2898

Recently Updated

DG - PImDL - Home
Sep 23, 2021 • updated by Armin Kathrein • view change

DG PImDL - How-to articles
Sep 23, 2021 • updated by Armin Kathrein • view change

DG PImDL - Meeting notes
Sep 23, 2021 • updated by Armin Kathrein • view change

DG PImDL - Quarterly reports
Sep 23, 2021 • updated by Armin Kathrein • view change

DG PImDL - Chair Info
Sep 23, 2021 • updated by Armin Kathrein • view change

DG PImDL - Participant Roster

Sep 23, 2021 • updated by Armin Kathrein • view change

DG PImDL - Meetings and Minutes
Sep 23, 2021 • updated by Armin Kathrein • view change

DG PImDL - Charter
Sep 23, 2021 • updated by Armin Kathrein • view change

DG PImDL - Participant Roster
Sep 02, 2021 • updated by Lynzie Adams • view change

DG PImDL - Participant Roster
Apr 19, 2021 • updated by Elizabeth Day • view change

2021-04-14 Meeting notes (draft)
Apr 12, 2021 • updated by John Wunderlich • view change

PIMDL_20201028.pdf
Apr 12, 2021 • attached by John Wunderlich

2021-04-07 Meeting notes
Apr 07, 2021 • updated by John Wunderlich • view change

PIMDL_20201028.pdf
Apr 07, 2021 • attached by John Wunderlich

DG PImDL - Participant Roster
Apr 07, 2021 • updated by Colin Wallis • view change