High Assurance Consumer Identity

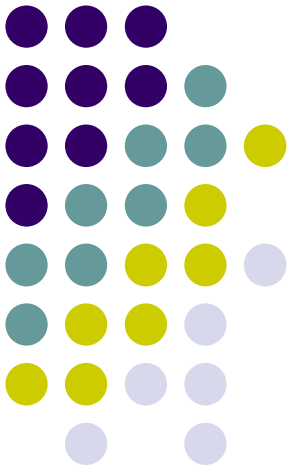
IIW East, Washington DC

September 9-10, 2010

Consumer Identity Workgroup

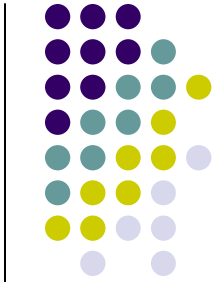
Chair: Bob Pinheiro

consumerid@bobpinheiro.com



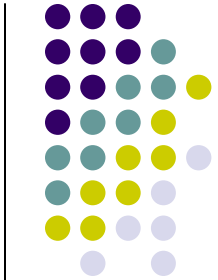
kantara INITIATIVE™

The Problem



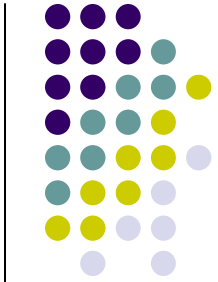
- Consumers are harmed if others can impersonate them for various purposes (financial, medical, etc) when sensitive personal information is stolen or misused to
  - establish **high value, identity-dependent services** such as credit cards, loans, cell phone accounts, etc.
  - obtain **unauthorized access to high value online resources** such as financial accounts, medical records, credit reports, etc
- Service providers are harmed and suffer losses (financial, reputational) if they provide high value services to those who claim a false identity.

Some Basic Assumptions



- High value services require (or should require) the Service Provider to have high assurance of a consumer's identity (or authorization status).
- High assurance ➔ FRAUD PREVENTION
  - Otherwise, just use low assurance, self-asserted identity or other claims
- An identity infrastructure should support high asssurance credentials /claims for high value services / transactions WHILE DISCOURAGING their use for low value services / transactions.

High Value Consumer Apps Where Identity Fraud Is Harmful



- Financial Services
  - New account opening
  - Access to existing online accounts
  - Transaction authorizations; ie, move money out of accts
  - Payments; e.g., credit card, debit, commercial payment services
- Healthcare
  - Access to patient health records or other patient-specfic healthcare portals
  - Impersonation of someone else to obtain medical services (Medical ID Theft)
- Government Interactions
  - Payment and reporting of taxes
  - Motor vehicle issues
- Credit Bureaus
  - Access to free online credit report
- Personal Data Stores
  - Access to personal data stores containing sensitive information
  - Authorized permissions for data access

Can Better Control of Personal Information Help?

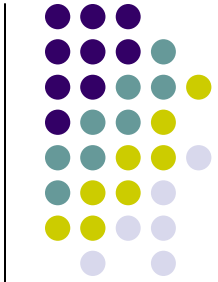
Maybe, BUT

Service Providers offering high value services should not accept self-asserted personal information as "proof" of anything.

Service Providers really need high assurance of various kinds of consumer claims.

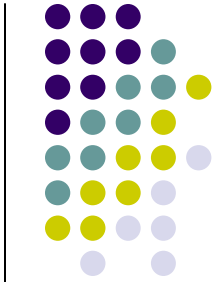
Consumers really need high assurance that false claims made by others using their personal information to obtain high value services will be rejected.

High Assurance of…….. a consumer's identity



- Needed by Service Provider to prevent fraud when establishing new high value relationships or enrolling in high value accounts
- Requires identity assertion/verified claim from Identity Provider to Service Provider / Relying Party upon Consumer authentication to IdP

High Assurance of…….
authority to access a protected resource

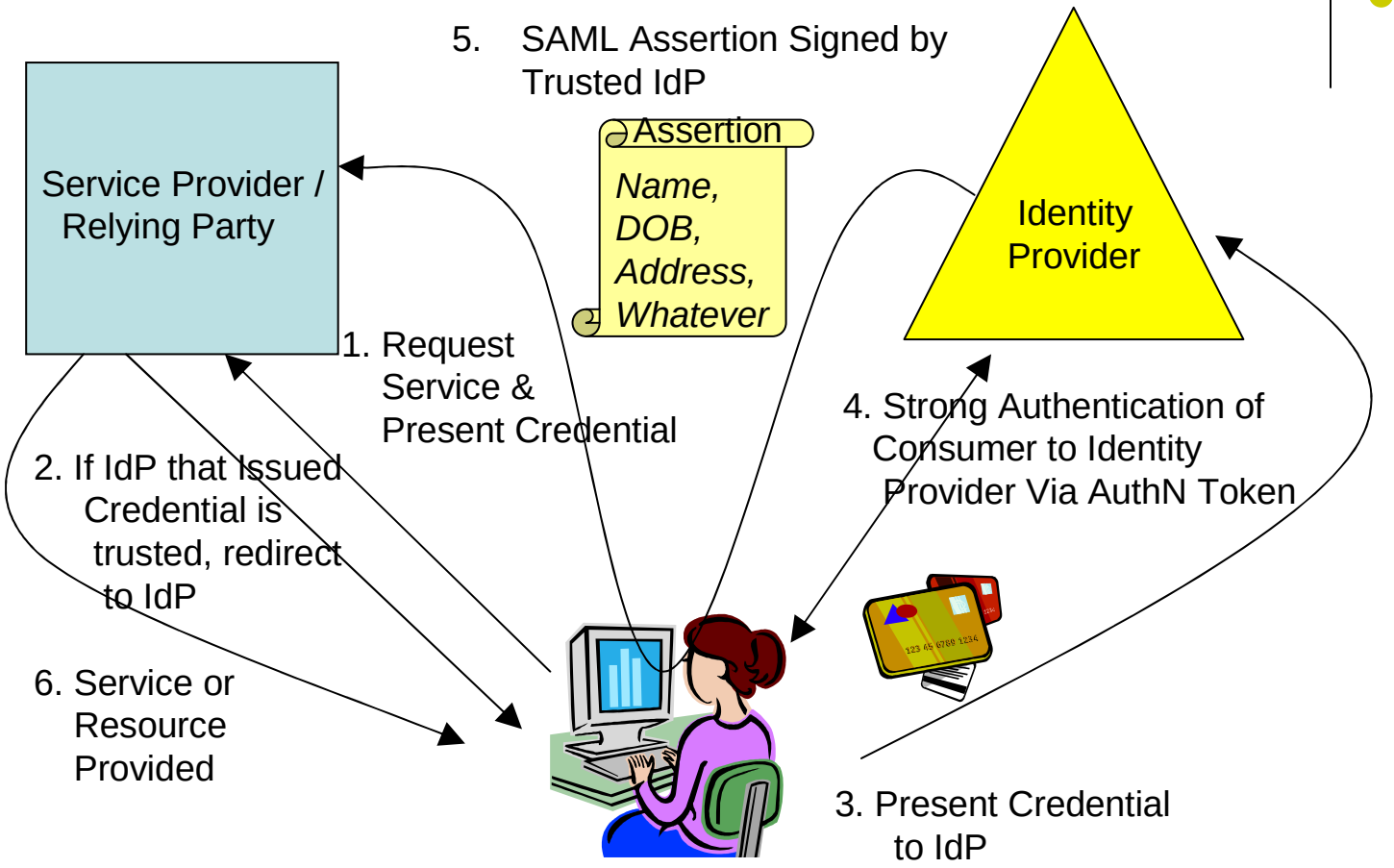


- Needed by Service Provider to prevent fraudulent access to an online account or resource
- Requires EITHER:
  - Assertion/claim from an IdP verifying authN status
  - Strong credential / authN token bound to the resource; e.g.,
    - PKI cert/private key
    - Self-issued Information Card

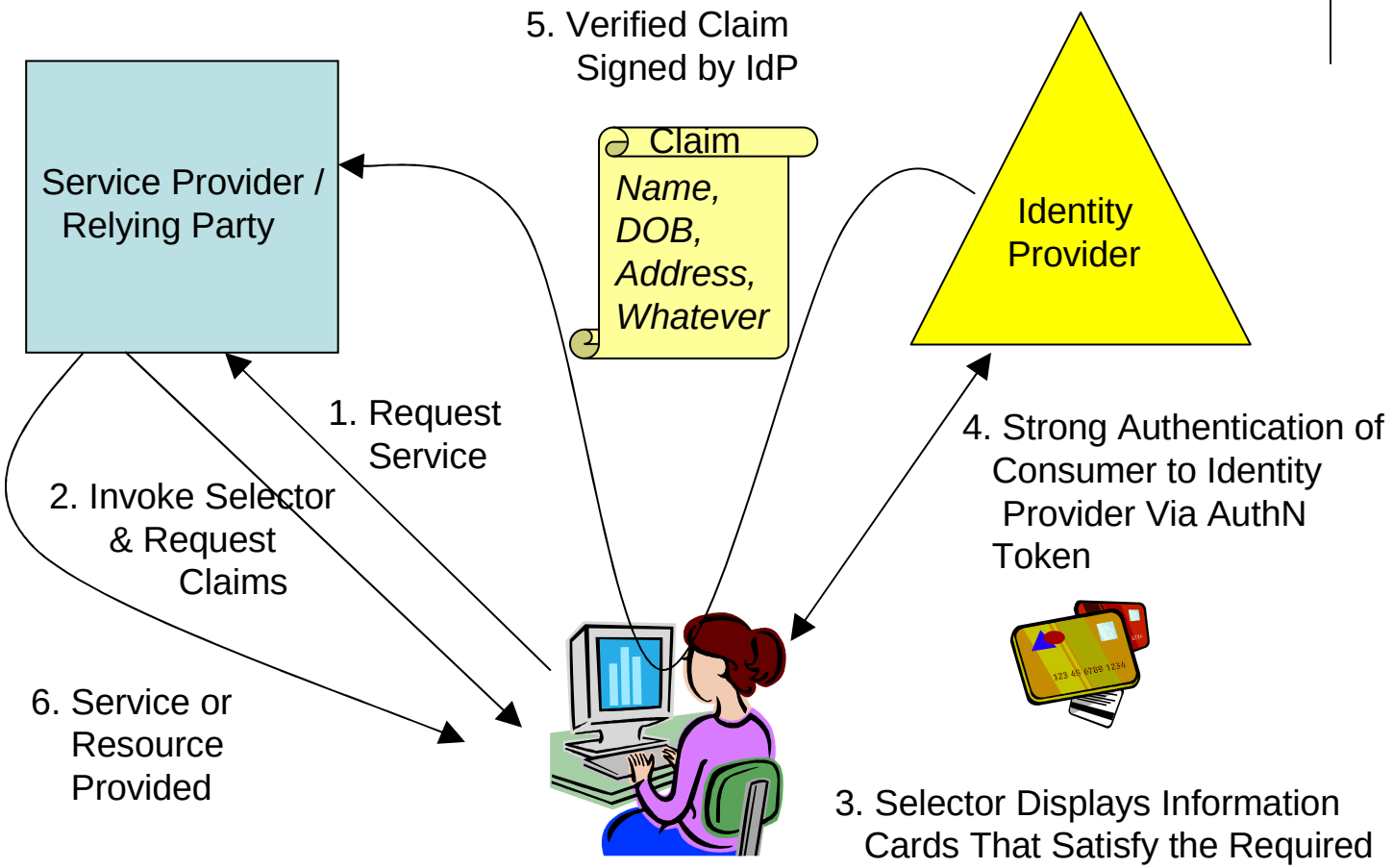
High Assurance of…….. authority to make an online payment

- Needed by online merchants to prevent fraudulent charges to a payment account that can result in a chargeback to merchant. For instance,
  - Credit card / debit card
  - Virtual “one time” credit card
  - Paypal
- Requires:
  - Assertion/claim from a cc issuer to merchant verifying authZ status after consumer authenticates to cc issuer
  - Assertion/claim from cc issuer to merchant containing virtual cc information
  - Strong authN token bound to payment account

Authentication of Consumer Claims (via SAML Assertions)



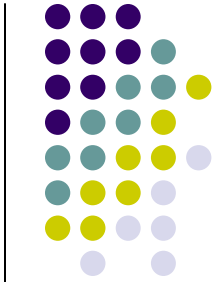
Authentication of Consumer Claims
(via Managed Information Card)



National Strategy for Trusted Identities in Cyberspace

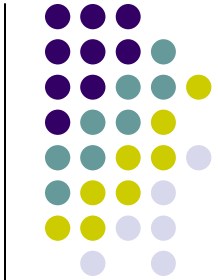
- US federal government's NSTIC initiative seeks to facilitate the creation of an identity "ecosystem" that can help to "*raise the level of trust associated with the identities of individuals, organizations, services, and devices involved in certain types of online transactions.*"
- CIWG seeks to help ensure that such an infrastructure can enable high assurance identity or other claims necessary to reduce fraudulent high value consumer transactions, in a way that
  - protects consumer privacy,
  - discourages demand for high assurance identity claims for low value transactions,
  - enables consumers to detect, and prevent, someone else from impersonating them in high value transactions.

Consumer Identity WG Goals



- Investigate open issues and provide specific recommendations to help ensure that an identity infrastructure enables
  - Service Providers / Relying Parties to authenticate, with high assurance, relevant claims about consumers to whom they provide high-value services, while protecting the consumer's privacy
  - Consumers to easily provide the minimal set of verified claims needed by SPs/RPs to enroll in, and use, high-value services
  - Consumers to prevent others from fraudulently impersonating them online in high value transactions
- Determine feasibility and understand what must happen in order to "roll out" this identity infrastructure and achieve widespread adoption by consumers.

Feasibility Depends On



- Whether **Service Providers / Relying Parties** will place a premium on minimizing fraud in connection with high-value services by demanding relevant high assurance consumer claims.
- Whether **Consumers** will perceive digital credentials and authentication methods needed for authentication of high assurance consumer claims as being easy to use.
- Whether **Identity Providers** that provide high assurance consumer claims can develop a business justification for doing so.
- Whether consumer **Privacy** can be protected
- Whether **Liability Issues** can be adequately addressed.

Open Issues in High Assurance Consumer Identity

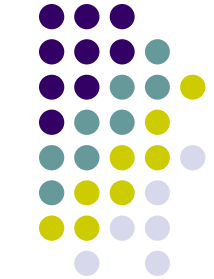
Definition of "High Assurance"

- Current trust frameworks associate "high assurance" with knowledge of an individual's identity; *identity proofing*
- Need to redefine high assurance in terms of strong authentication coupled with rigorous verification of claims by an IdP.
- "High assurance" should also pertain to claims other than identity; ie, authorization to access a resource, claims based on other attributes such as age, membership, etc.

Open Issues in High Assurance Consumer Identity
Trust Frameworks and Claims

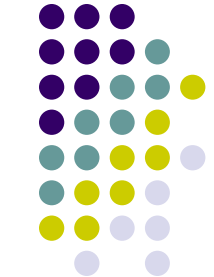
- Will different trust communities require different trust frameworks for supporting high value services offered by service providers in those communities?
  - Open Identity Exchange (OIX) is defining trust frameworks for different “trust communities” such as OCLC library, telecom, personal data stores, PBS public media
  - What about communities such as financial, healthcare, government, where high assurance is also important?
  - How will these trust frameworks be the same/different?
- Will different sets of claims be required by Service Providers operating in different trust communities?

Open Issues in High Assurance Consumer Identity
Credentials & Tokens



- Distinguish “credentials” from “authentication tokens”
  - A credential presents a claim made by a consumer; e.g., personally identifiable information, a userID, X.509 certificate, Information Card, OpenID
  - An authentication token authenticates a credential; e.g., a password, shared secret, one-time password, X.509 private key, biometric
- Will separate credentials be needed by consumers for use within different trust communities?
- Who will provide high assurance credentials and tokens to consumers?
  - A consortium within each trust community?
  - Individual Identity Providers within each trust community?
  - State Motor Vehicle Bureaus?
  - Commercial Identity Providers; ie, Yahoo, Paypal, etc?

Open Issues in High Assurance Consumer Identity
Digital Wallets / Selectors / Active Clients



- Should selectors / active clients be the default mode of deployment for high assurance online consumer credentials?
- Will consumers be able to keep and manage their various credentials using a single selector / active client?
- What are the issues and tradeoffs determining whether selectors / active clients should be deployed:
  - on the consumer's PC or laptop or cell phone
  - "in the cloud"
  - on a portable physical device; ie, USB dongle
- Who will provide and setup these selectors / active clients on behalf of consumers?
  - Browser makers (as plug-ins)?
  - Identity Providers?
  - Consumers themselves?

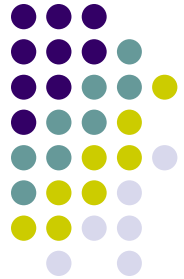
Open Issues in High Assurance Consumer Identity
Digital Wallets / Selectors / Active Clients

- What is the trust relationship between cloud-based selectors and Identity Providers?
  - Does the consumer use an authN token to authenticate to the selector for access to a credential, followed by an authentication assertion from the selector to the IdP for issuance of a verified claim,
    => IdP trusts Selector
  - Does the consumer authenticate separately to the selector and to the IdP
    => No trust relationship
- Trust relationship between cloud-based selector and Relying Party?

Open Issues in High Assurance Consumer Identity
Portability of Authentication Tokens

- For credentials residing in cloud-based selectors / active clients, or on a consumer-owned device, where will authentication tokens needed to authenticate to Identity Providers reside in order to maintain portability?
  - Also on the mobile device?
  - USB dongle?
  - Somewhere else?

Open Issues in High Assurance Consumer Identity
Does a High Assurance Claim Always Involve an Identity Provider?



- Yes, whenever a identity assertion or claim Is needed:
  - Subject is unknown to SP and seeks to establish a new high value, long-term relationship or account
  - Subject is unknown to SP, seeks no long-term relationship but wants a high value, identity-dependent service
- The need for such claims is likely to be infrequent.

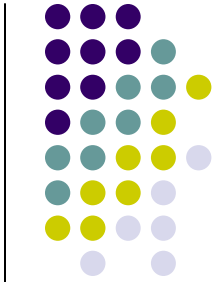
Open Issues in High Assurance Consumer Identity
Does a High Assurance Claim Always Involve an Identity Provider?

- Once a relationship/account is established, an authorization claim is needed to access or use the service.
  - Authorization claim/assertion from IdP based on authentication of consumer to the IdP via authN token **OR**
  - Localized challenge/response interaction between Service Provider and Consumer to demonstrate control of authN token.
- Since authZ claims are likely to be frequent, can the claim be authenticated without involving an IdP?
  - via PKI certificate or self-issued Information Card

Open Issues in High Assurance Consumer Identity
Prevention of Identity Theft Based on Stolen PII

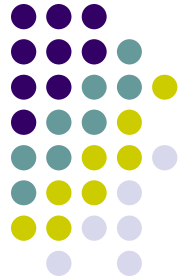
- Previous assumption is that all SP/RPs should rely on a high assurance identity claim/assertion from a trusted IdP when establishing high-value, identity dependent relationships. BUT this won't happen for a while if, ever.
- In the meantime, if an IdP within some trust community has issued you a credential/token, how can you prevent someone who has stolen your PII from claiming your identity?
  - Is there a way to discover if someone is using your PII?
- Possible role for Credit Reporting Agencies to notify credential holders when a SP requests a credit check based on PII for identification.

Open Issues in High Assurance Consumer Identity Privacy



- What are privacy requirements regarding consumer information retained by, or gathered by, entities within the trust framework (IdPs, SPs/RPs)?
- How can high assurance identity assertions be limited to certain types of high value applications involving financial transactions, access to healthcare records, etc?
  - Don’t want to create a system whereby every Service Provider demands to know your identity

Open Issues in High Assurance Consumer Identity
Stakeholder Roles



Who are the stakeholders and how would they benefit from this?

- Service Providers / Relying Parties
- Financial and healthcare consortia
- Identity theft prevention and assistance organizations, as well as other consumer advocacy organizations
- Identity Providers
- Strong authentication vendors
- US Federal Trade Commission & other government agencies