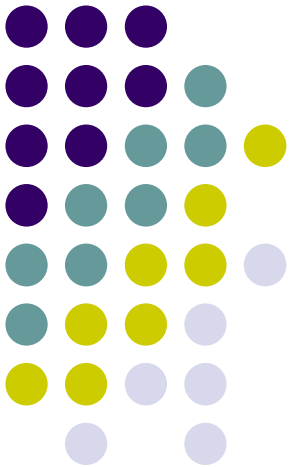
Consumer Identity WG

Chair: Bob Pinheiro



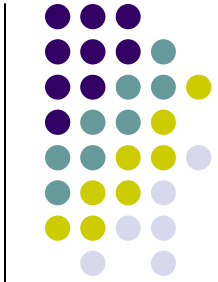
Some Preliminary Questions To Help Define a Funding Proposal for Consumer Identity WG

V0.1

kantara INITIATIVE™

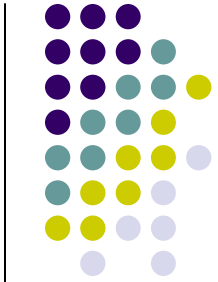
Preliminary Draft March 16, 2010

The Problem



- Consumers are subject to various types of identity fraud (financial, medical, criminal, reputational) if their personal information, financial account information, usernames and passwords, etc., are stolen.
- There is no “identity network” that allows:
  - service providers to know who they are dealing with in high-value consumer transactions,
  - consumers to detect and block others who seek to impersonate them.

Many Issues to Consider

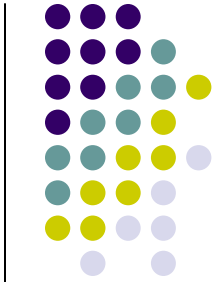


- OpenID, Information Cards may help BUT:
  - Generally no high assurance proofing of consumer's identities by identity providers
  - No widespread deployment of strong authentication methods among consumers
- Consumers largely unaware until they have a problem
- Weak motivation to change:
  - Fraud is part of the "cost of doing business";
  - Don't want to burden consumers with more security;
  - Not my problem; someone else will fix it;
  - Consumers need a good reason to care.

Goal of Consumer Identity WG

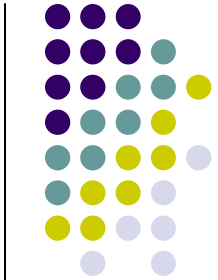
- Goal of CIWG is to help address the basic question “What will it take to realize wide deployment of high assurance digital identities for consumers?”
  - Business/policy drivers for relying parties and identity providers
  - What new services can be enabled by high assurance digital identities for consumers?
  - Role of mobile devices, smartcards, for strong authentication
  - Trust frameworks to enable reliance on trusted consumer credentials by many relying parties
  - Usability, acceptance, privacy impacts of OpenID, Infocards
  - Consumer education and awareness
  - More government involvement needed to jump-start???

What is Value of High Assurance Credentials for Consumers?



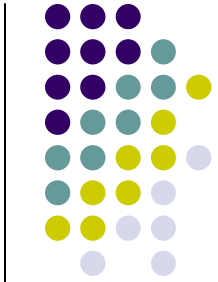
- What's in it for the consumer?
- Is a high assurance credential only needed to prevent fraud?
- If not, what else?
  - Link high assurance credential with verified personal information?
  - SPs might like, but what about privacy?

Some Adoption Issues (1)



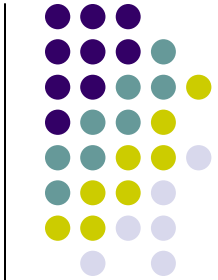
- Does identity proofing mean something different for different types of SPs/RPs?
  - What about attribute assurance?
- Need separate trust frameworks for different “trust communities”?
  - e.g., would credential issued by a healthcare IdP be usable for access to a financial institution?
  - e.g., would credential issued by a financial institution be usable for access to a healthcare provider/e-health record?
- What is “high assurance” for consumers?
  - Always pair strong auth technology with id proofing?
  - What about strong auth technology with no id proofing?

Some Adoption Issues(2)



- Need policy changes by SPs/RPs?
  - Stronger auth vs fraud writeoff?
- What is business case for IdPs?
  - Receive payment from SP/RP for identity assertions?
  - Who pays for issuing strong credentials to consumers?
- OpenID versus Information Cards
  - Almost everything seems to be about OpenID
  - Are OpenID, Infocards merging? ie, active client
  - Separate role for Infocards in consumer space? ie, online payment cards?

Some Adoption Issues(3)



- Different credentials for low assurance versus high assurance apps? Can one credential be “adaptible” for both?
- Are different kinds of strong auth technology more appropriate/usable for different demographic groups; ie, elderly, youth, etc
- Who will educate the public about the value of high assurance identity? FTC? Others?
- Is more government involvement needed to “jump start” greater interest, a la ICAM?