Can We Reconstruct How Identity is Managed on the Internet?

Merritt Maxim

February 29, 2012

Session ID: STAR-202

Session Classification: Intermediate

ca technologies

RSA CONFERENCE 2012

Session abstract

- Session Learning Objectives:
  - Understand the reasons a new Internet identity approach is needed
  - Envision how current government & private federation-based approaches are showing the way to an Internet-scale approach
  - Project into the future of how Internet identity could operate if this approach continues to increase in popularity and what implications this could have for existing and new players
  - Classify the challenges of policy, interoperability, legal, privacy, and others that stand in the way of broader adoption
  - Recommend actions for both individuals and organizations to accelerate the adoption of this new approach

Agenda

- Internet identity problem
- Solution overview
- Overview of current trust frameworks
- Where is there progress?
- What is still missing?
- Trends to monitor
- Conclusion
- Q&A

Think of the Internet Identity Problem as Humpty Dumpty

Now that it is broken, how do we put it back together?

The Internet Identity problem

Simple to understand, hard to solve

How do I securely and accurately link these two?

Is a carbon life form
Has a name & address
Has home phone
Pays taxes
Has utility bills
Has privacy wants
Uses financial institution

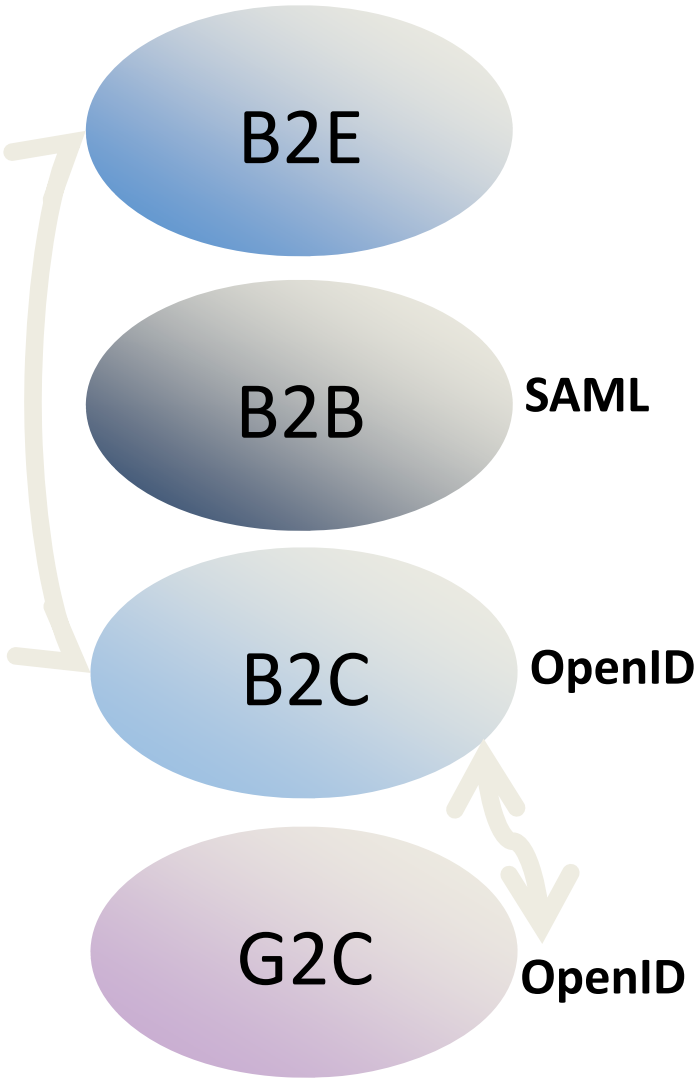
Multiple email addresses
Multiple digital identities
Social media accounts
Highly mobile
Uses multiple devices
Has many online accounts
Has a transaction history

So what?

- Internet identity creates problems such as:
  - Increased risk
  - Identity theft
  - High management costs
  - Poor user experience
- Problem cannot be ignored
  - Increased reliance on internet for commerce

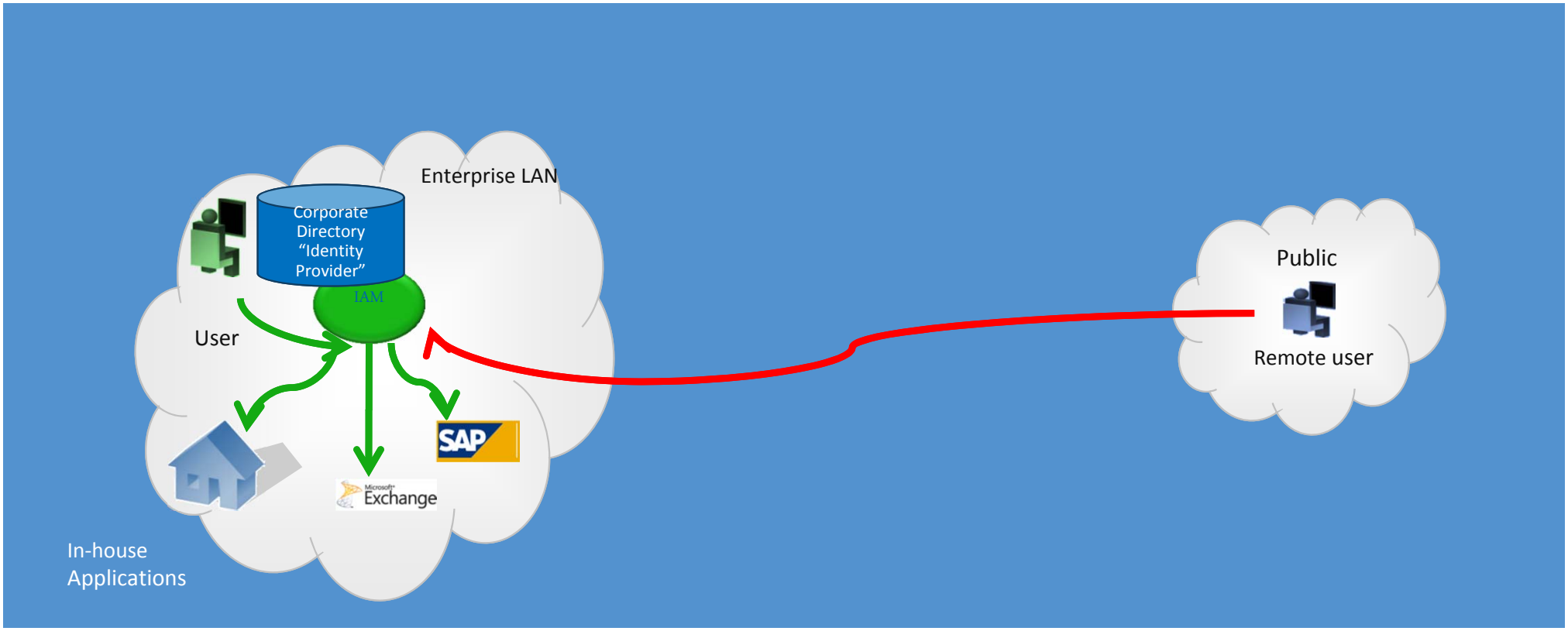
Four conceptual approaches to identity

Identities increasingly crossing these boundaries



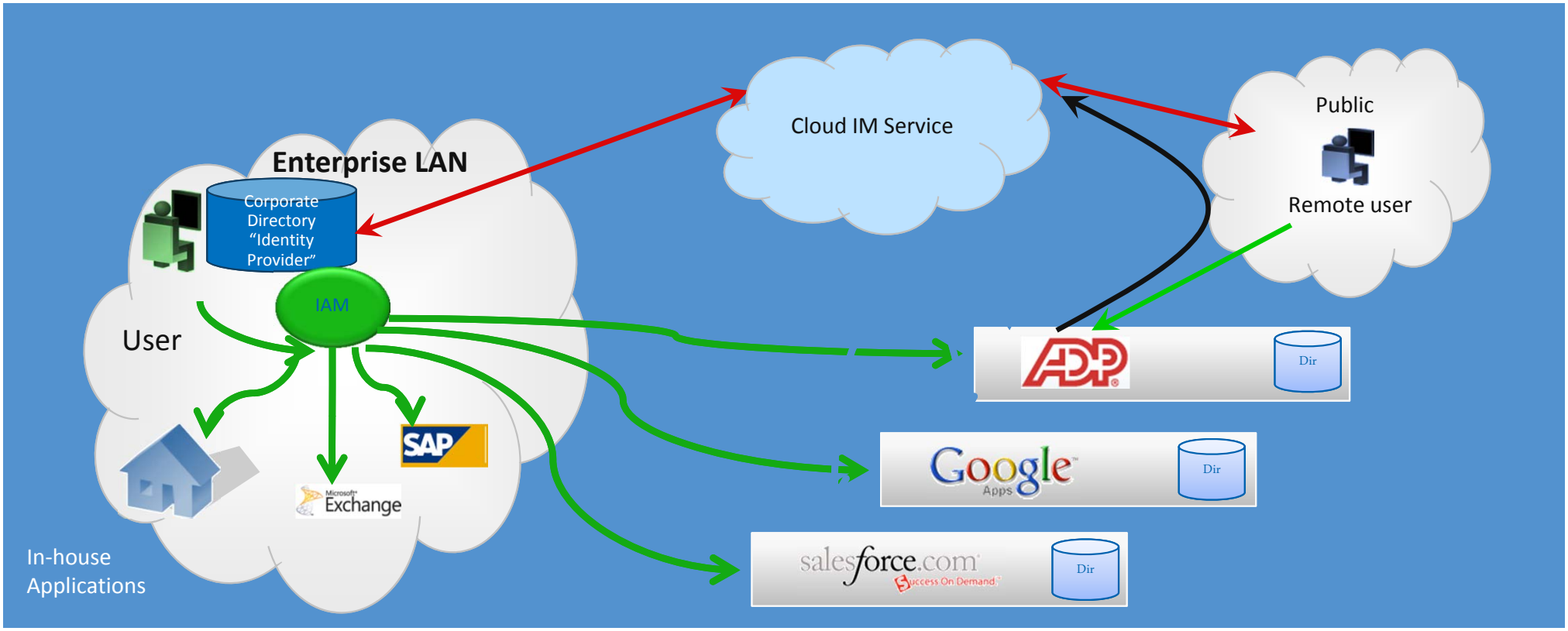
Identity was an easier issue 10+ years ago

- Enterprise manages B2E on-premise
- B2C just emerging
- B2B and G2C in infancy
- Implicit trust established between the user and applications



Identity in 2012-Increased complexity

- B2E still managed by enterprise, but highly distributed workforce
- B2C, B2B and G2C much more established
- Trust between user and app no longer a given



So what is a possible solution?

How about trust frameworks….

"Trusted identities and consumer control of personal information are essential to the effectiveness of transactions on the Internet.

Trusted frameworks that provide identity assurance are a critical factor in the success of the digital identity ecosystem."

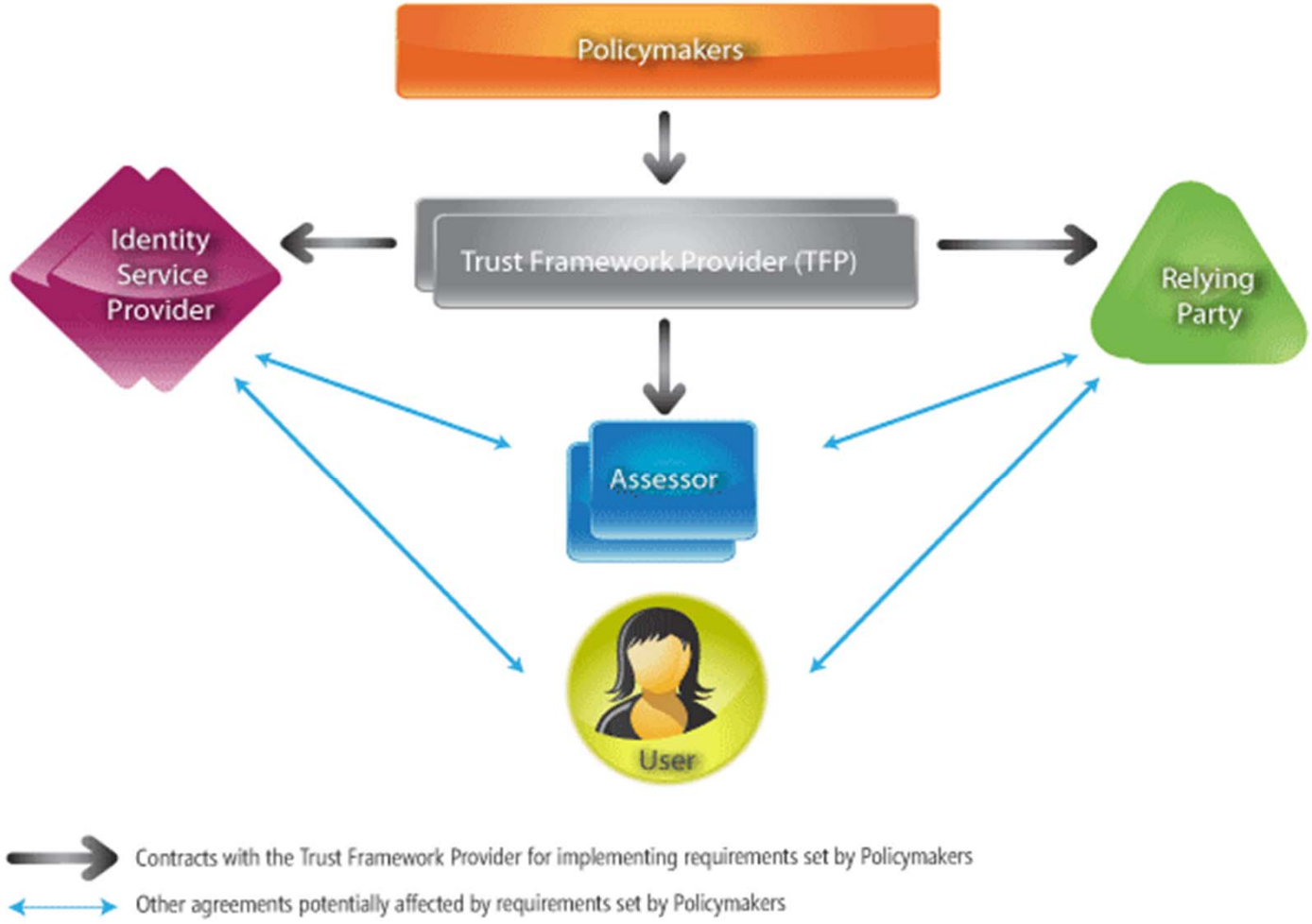
-- Andrew Nash, Senior Director of Identity Services for Google Inc.
OIX Founding Board Member

Some definitions

(courtesy Kantara Initiative)

Party	Description
Trust Framework Provider	Sets the rules for operation of the trust framework; Accredits assessors
Relying Party	Controls a resource that users wish to access Determines attributes required for access to resources
Identity Provider	Verifies identity of Subjects as specified in the trust framework
Credential Provider	Issues credentials that meet criteria for content and technical specifications as specified in the trust framework; Verifies validity of credentials when requested by Relying Party
Attribute Provider	Verifies attributes associated with Subjects as specified in the trust framework

What is a trust framework?



http://openidentityexchange.org/what-is-a-trust-framework

- Examples of Trust Frameworks-Phone networks, credit card payment networks

Trust Framework
Example 1-Kantara Initiative

- Joint initiative founded in 2009 by:
  - Liberty Alliance, Concordia Project, Internet Society, Information Card Foundation and XDI.org
- Not a standards-body-cooperates with OASIS & IETF
- Only Approved US Government Trust Framework Provider (TFP) with certified Levels of Assurance (LoA) 1, 2 and 3 non-crypto (non-PKI)
- Currently working on user managed access (UMA) model

— http://www.kantarainitiative.org/

Trust Framework
Example 2-Open Identity Exchange (OIX)

- Launched at RSA 2010
  - Executive members-AT&T, Booz Allen, CA Technologies, Equifax, Google, Symantec, Verizon
  - Created partially out of US Government need to accept identities issued by 3rd parties
- Goal: Build trust in the exchange of identity credentials online
- Offer frameworks with different level of assurance (LOA)
  - LOAs based on NIST 800-63
- www.openidentityexchange.org

Trust Framework Example 3

National Strategy for Trusted Identities in Cyberspace (NSTIC)

- Announced April 2011
- Envisions an Identity Ecosystem—a user-centric online environment, a set of technologies, policies, and agreed upon standards that securely supports transactions ranging from anonymous to fully authenticated and from low to high value.
- Managed through NIST/Commerce Department
- Privacy Act of 1974 is underlying legislative framework
  - Allows for identity providers outside government.
- Established National Program Office (NPO)
  - Announced $10M program to fund 6-8 pilots in 2012

— http://www.nist.gov/nstic/

US Government Identity Assurance Levels

Level 1	Level 2	Level 3	Level 4
Little or no confidence in asserted identity No identity proofing required, and some confidence the same claimant is accessing the protected transaction or Data	Some confidence in asserted identity Provides single factor remote authentication using a wide range of available authentication technologies	High confidence in asserted identity Provides multi-factor remote authentication using“soft” cryptographic tokens, “hard” cryptographic tokens, and one-time password tokens	Very high confidence in asserted identity Provides multi-factor remote authentication using “hard” cryptographic tokens

Source-http://www.cio.gov/Documents/OMBReqforAcceptingExternally_IssuedIdCred10-6-2011.pdf

Benefits of Trust Frameworks

- Standardized identity interactions
  - Early progress
  - US Govt NIH PubMed program projects ~$3M in savings/5 yrs
- Simplified end-user experience
  - Reduced cost of supporting end-users
- Reduced the friction of logins, registrations, purchases, and other online activities
- Increased confidence in online identity infrastructure
- Increased confidence in regulatory compliance

Progress to date

US Government Trust Framework Program

US ICAM LOA 1 Trust Framework operational March 2010

Enables Federal Agency websites to accept OpenID credentials

Trust Framework Providers:

- InCommon Federation – Level of Assurance 1 *(provisionally approved)*
- Kantara Initiative – Level of Assurance 1, 2, and non-PKI 3 *(provisionally approved)*
- Open Identity Exchange – Level of Assurance 1 *(provisionally approved)*

Approved Identity Schemes (Levels 1, 2 and non-PKI 3):

- Identity Metasystem Interoperability (IMI) 1.0 Profile
- OpenID 2.0 Profile
- SAML 2.0 Web Browser Single Sign-On Profile

Approved Identity Providers	
Yahoo OpenID	Wave Systems, OpenID 2.0, LoA 1
PayPal OpenID 2.0, LoA 1	PayPal IMI 1.0, LoA 1
VeriSign OpenID 2.0, LoA 1	Equifax IMI 1.0, LoA 1
Google OpenID 2.0, LoA 1	

Why not use governments as sole online verifier?

- Consumers expect choice
  - 1 size fits all is not likely solution
- Practical problem
  - 200M+ people have dual citizenship (Economist)
- Private sector has skills and expertise
- Risk (perceived or real) of government monit online behavior can inhibit adoption
- Solution should be open and flexible
- This issue is geographic dependent
  - In some countries, citizens are ok with this model
  - Not all governments have the same capabilities

Identity Trend to monitor

Google Street Identity/LMNOP Project

- Experimenting with authorizing access to verified street addresses
- Relying party sends postcard to end-user's home with 1-time code
- User goes online and enters code
- Relatively low cost, relatively secure
- Uses cases can get more elegant (and complex)
  - User can authorize IdP to issue physical address "attribute" to RP
  - RP can contact mobile operator to verify address attribute

— www.streetidentity.com

Identity Trend to monitor
User-managed access (UMA)

- Evolution of OAuth user-centric model to enhance user control over user attribute/claim usage and RP compliance requirements
- Protocol for users to manage what attributes to share
- Managed through Kantara's UMA Working Group
- Contributed to the IETF for consideration
- Planning interoperability testing and increased OpenID Connect integration in 2012
- Initial implementations
  - Newcastle University (UK) Smartam.org
  - Fraunhofer AISEC photo-sharing project
    - User-defined Photo sharing service

What is still missing?

- **For everyone**
  - Use of standards to promote interoperability
  - Linking strong credentials/authentication to identity
  - Risk analysis
  - Processes to automate trust establishment
  - Portability between web and mobile environments
- **For user**
  - Choice, privacy, portability of identity between communities
- **For IdPs and RPs**
  - Limitation on liability
    - As RP, what legal or contractual protection is there in event of fraud?
      - Orgs may wait until there is a body of case law before proceeding.
  - Confidence of good behavior by RPs
  - Defined metrics for Level of Protection (LOP)

Apply

If you are a…	Consider the following in 90+ days…
Relying Party	• Understand strengths and weaknesses of each framework. • Conduct risk assessment of your environment • (NIST 800-37 is good basis) • Select appropriate level of assurance you expect from IdP • "Is accepting an ID from ID provider X acceptable?"

Identity Providers
Credential Providers
	• Complete internal assessment of your security procedures
	• Publicize your due diligence
	• Consider something like SAS-70 audit
	• W/o these-few relying parties will want to work with you
	• If partnering with attribute providers:
	  • Determine "freshness of underlying attributes
	  • Understand any liability issues associated with using 3rd party attributes

Attribute Provider	• Provide details on freshness of attributes • Work on partnering with IdPs

In conclusion

- Session Learning Objectives:
  - Trust Frameworks are one proven approach to address the Internet Identity problem
  - Current government & private federation-based approaches are showing the way to an Internet-scale approach
    - Kantara, OIX, NSTIC are proven this now
  - Project into the future of how Internet identity could operate if this approach continues to increase in popularity and what implications this could have for existing and new players
  - Policy, interoperability, legal, privacy challenges remain
    - Still many challenges to be addressed, but off to a good start
  - There are concrete actions that individuals and organizations can begin taking to take advantage of these new approaches.

Thank you

- Tracking/stalking me:
  - Merritt.maxim@ca.com
  - www.twitter.com/merrittmaxim
  - http://www.linkedin.com/pub/merritt-maxim/0/315/526
  - Blog
  - http://community.ca.com/blogs/iam/default.aspx